Cisco Identity Services Engine Administrator Guide, Release 3.1

First Published: 2021-08-03

Last Modified: 2024-07-15

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1

New and Changed Information 1

New and Changed Information 1

CHAPTER 2

Overview of Cisco ISE 13

Introduction to Cisco ISE 13

Cisco ISE Features 14

Cisco ISE Administrators 15

Force CLI Administrator to Use External Identity Store 15

Create a New Administrator 16

Cisco ISE Administrator Groups 17

Create an Admin Group 24

Administrative Access to Cisco ISE 25

Role-Based Admin Access Control in Cisco ISE 25

Role-Based Permissions 26

RBAC Policies 26

Default Menu Access Permissions 26

Configure Menu Access Permissions 144

Prerequisites for Granting Data Access Permissions 144

Default Data Access Permissions 145

Configure Data Access Permissions 155

Read-Only Admin Policy 155

Customize Menu Access for the Read-Only Administrator 156

CHAPTER 3

Licensing 157

Cisco ISE Licenses 157

Tier Licenses 159

    Device Administration Licenses 160
    Evaluation Licenses 160
  Cisco ISE Smart Licensing 160
    Register and Activate Smart Licenses 161
    Manage Smart Licensing in Cisco ISE 162
    Troubleshooting: Unregistered License Usage 163
  Smart Licensing for Air-Gapped Networks 164
    Configure Smart Software Manager On-Prem for Smart Licensing 164
    Specific License Reservation 165
      Enable Specific License Reservation 168
      Update Specific License Reservation 169
      Return Specific License Reservation 170

CHAPTER 4 **Deployment of Cisco ISE** 171
  Cisco ISE Deployment Terminology 171
  Personas in Distributed Cisco ISE Deployments 172
  Configure a Cisco ISE Node 172
    Configure a Primary Policy Administration Node 173
    Register a Secondary Cisco ISE Node 173
  Support for Multiple Deployment Scenarios 175
  Cisco ISE Distributed Deployment 175
    Cisco ISE Deployment Setup 175
    Data Replication from Primary to Secondary Cisco ISE Nodes 175
    Cisco ISE Node Deregistration 176
    Node Status in a Cisco ISE Deployment 176
    Guidelines for Setting Up a Distributed Deployment 177
    Menu Options Available on Primary and Secondary Nodes 178
  Deployment and Node Settings 179
    Deployment Nodes List Window 179
    General Node Settings 180
    Profiling Node Settings 185
  Logging Settings 187
    Remote Logging Target Settings 187
    Configure Logging Categories 189

Admin Access Settings 189
  Administrator Password Policy Settings 190
  Session Timeout and Session Information Settings 191
Administration Node 192
  High Availability for Administrative Node 192
  High-Availability Health Check Nodes 194
  Health Check Nodes 195
  Automatic Failover to the Secondary PAN 195
  Sample Scenarios when Automatic Failover is Avoided 196
  Functionalities Affected by the PAN Automatic Failover Feature 196
  Configure Primary PAN for Automatic Failover 198
  Manually Promote Secondary PAN to Primary 199
  Reusing a Node of an Existing Cisco ISE Deployment as a Primary PAN for a New Cisco ISE Deployment 199
  Restoring Service to the Primary PAN 200
Support for Automatic Failover for the Administration Node 200
Policy Service Node 200
  High Availability in Policy Service Nodes 200
  Load Balancer to Distribute Requests Evenly Among PSNs 201
  Session Failover in Policy Service Nodes 201
  Number of Nodes in a Policy Service Node Group 201
  Light Data Distribution 201
  RADIUS Session Directory 202
  Endpoint Owner Directory 202
Monitoring Node 203
  Manually Modify the MnT Role 203
  Syslog over Cisco ISE Messaging Service 204
  Automatic Failover in MnT Nodes 205
Monitoring Database 207
  Back Up and Restore the Monitoring Database 207
  Monitoring Database Purge 207
  Guidelines for Purging the Monitoring Database 207
  Operational Data Purging 208
  Purge Older Operational Data 208

Configure MnT Nodes for Automatic Failover 209
Cisco pxGrid Node 210
  Deploy Cisco pxGrid Node 211
  Configure Cisco pxGrid Settings 212
  Generate Cisco pxGrid Certificate 213
  Control Permissions for Cisco pxGrid Clients 214
  pxGrid Operations and Services Use Cases 215
Cisco pxGrid Cloud Overview 216
  Enable pxGrid Cloud Service in Cisco ISE 217
  Connect Cisco ISE to Cisco pxGrid Cloud 218
  Disable pxGrid Cloud Service on Cisco ISE 218
  Configure a pxGrid Cloud Policy 219
  Cisco pxGrid Cloud Clients 219
  High Availability for pxGrid Nodes 220
  Log Files Specific to pxGrid Cloud Service 221
  Configure Debug Log Level for pxGrid Cloud Service 222
View Nodes in a Deployment 223
Download Endpoint Statistical Data from MnT Nodes 223
Database Crash or File Corruption Issues 223
Device Configuration for Monitoring 224
Synchronize Primary and Secondary Cisco ISE Nodes 224
Change Node Personas and Services 224
Effects of Modifying Nodes in Cisco ISE 225
Create a Policy Service Node Group 225
Remove a Node from Deployment 226
Shut Down a Cisco ISE Node 227
Scenarios In Which Need to Reregister a Node 227
Change the Hostname or IP Address of a Standalone Cisco ISE Node 228

CHAPTER 5 **Basic Setup** 231
Administration Portal 232
  Interactive Help 238
  Cisco ISE Home Dashboards 238
  Configuring Home Dashboards 239

Context Visibility Views 240
  Attributes in Context Visibility 242
  The Application Dashboard 243
  The Hardware Dashboard 244
Dashlets 246
Filtering Displayed Data in a View 247
Create Custom Filters 249
Filter Data by Conditions Using the Advanced Filter 249
Filter Data by Field Attributes Using the Quick Filter 249
Endpoint Actions in Dashlet Views 249
Cisco ISE Dashboard 250
Cisco ISE Internationalization and Localization 252
  Supported Languages 253
  End-User Web Portal Localization 253
  Support for UTF-8 Character Data Entry 254
    UTF-8 Credential Authentication 254
    UTF-8 Policies and Posture Assessment 254
    UTF-8 Support for Messages Sent to Supplicant 254
    Reports and Alerts UTF-8 Support 254
    UTF-8 Character Support in the Portals 255
    UTF-8 Support Outside the Cisco ISE User Interface 257
    Support for Importing and Exporting UTF-8 Values 258
    UTF-8 Support on REST 258
    UTF-8 Support for Identity Stores Authorization Data 258
MAC Address Normalization 258
Cisco ISE Deployment Upgrade 259
Administrator Access Console 259
  Administrator Login Browser Support 259
  Administrator Lockout Because of Login Attempts 260
Configure Proxy Settings in Cisco ISE 260
Ports Used by the Administration Portal 261
Set Up the Cisco ISE Application Programming Interface Gateway 261
Enable API Service 262
  Enable External Active Directory Access for API Services 267

External RESTful Services Software Development Kit 267

Specify System Time and Network Time Protocol Server Settings 267

Change the System Time Zone 269

Configure SMTP Server to Support Notifications 269

Enable Secure Unlock Client Mechanism 270

Federal Information Processing Standards Mode Support 272

  Enable Federal Information Processing Standards Mode in Cisco ISE 273

    Configure Cisco ISE for Administrator Common Access Card Authentication 273

Secure SSH Key Exchange Using Diffie-Hellman Algorithm 276

Configure Cisco ISE to Send Secure Syslog 276

  Configure Secure Syslog Remote Logging Target 277

    Remote Logging Target Settings 277

  Enable Logging Categories to Send Auditable Events to the Secure Syslog Target 279

    Configure Logging Categories 279

  Disable TCP Syslog and UDP Syslog Collectors 280

Default Secure Syslog Collector 280

Offline Maintenance 281

Configure Endpoint Login Credentials 282

Changing the Host Name in Cisco ISE 282

Certificate Management in Cisco ISE 283

  Configure Certificates in Cisco ISE to Enable Secure Access 283

  Certificate Usage 284

  Certificate Matching in Cisco ISE 286

  Validity of X.509 Certificates 286

  Enable Public Key Infrastructure in Cisco ISE 287

  Wildcard Certificates 288

    Wildcard Certificate Support in Cisco ISE 288

    Wildcard Certificates for HTTPS and Extensible Authentication Protocol Communication 289

    Fully Qualified Domain Name in URL Redirection 289

    Advantages of Using Wildcard Certificates 290

    Disadvantages of Using Wildcard Certificates 291

    Wildcard Certificate Compatibility 291

  Certificate Hierarchy 292

  System Certificates 292

- View System Certificates 293
- Import a System Certificate 294
- System Certificate Import Settings 295
- Generate a Self-Signed Certificate 296
- Self-Signed Certificate Settings 297
- Edit a System Certificate 299
- Delete a System Certificate 300
- Export a System Certificate 301

Trusted Certificates Store 301
- Certificates in Trusted Certificates Store 302
- List of Trusted Certificates 303
- Trusted Certificate Naming Constraints 304
- View Trusted Certificates 305
- Change the Status of a Certificate in Trusted Certificates Store 305
- Add a Certificate to Trusted Certificates Store 305
- Edit a Trusted Certificate 306
- Trusted Certificate Settings 306
- Delete a Trusted Certificate 308
- Export a Certificate from Trusted Certificates Store 308
- Import a Root Certificate into the Trusted Certificate Store 309
- Trusted Certificate Import Settings 309
- Certificate Chain Import 310
- Install Trusted Certificates for Cisco ISE Inter Node Communication 311

Default Trusted Certificates in Cisco ISE 311

Stale System and Trusted Certificates 314

Certificate-Signing Requests 315
- Create a Certificate-Signing Request and Submit it to a Certificate Authority 315
- Bind a CA-Signed Certificate to a Certificate Signing Request 316
- Export a Certificate-Signing Request 317
- Certificate-Signing Request Settings 317

Set Up Certificates for Portal Use 322
- Reassign Default Portal Certificate Group Tag to CA-Signed Certificate 322
- Associate Portal Certificate Tag Before You Register a Node 323

User and Endpoint Certificate Renewal 324

        Dictionary Attributes Used in Policy Conditions for Certificate Renewal **324**
        CWA Redirect to a Renew Certificate **325**
        Configure Cisco ISE to Allow Users to a Renew Certificate **325**
        Update the Allowed Protocol Configuration **325**
        Create an Authorization Policy Profile for CWA Redirection **326**
        Enable BYOD Settings in Guest Portal **326**
        Certificate Renewal Fails for Apple iOS Devices **326**
        Certificate Periodic Check Settings **326**
    Extract a Certificate and Private Key from a .pfx File **327**
Cisco ISE CA Service **328**
    Cisco ISE Certificate Fingerprinting **328**
        Create a Policy with SHA-256 Fingerprint **329**
        Create and Map an Authentication Policy with SHA-256 Fingerprint **330**
        Create an Authorization Policy **330**
        Verify PRRT Logs **331**
    Cisco ISE CA Certificates Provisioned on Administration and Policy Service Nodes **331**
    Requirements for CA to Interoperate with Cisco ISE **332**
    Cisco ISE CA Chain Regeneration **333**
    Cisco ISE Messaging Certificate Support with External CA **334**
    Elliptical Curve Cryptography Certificates Support **334**
    Cisco ISE Certificate Authority Certificates **336**
        Edit a Cisco ISE CA Certificate **336**
        Export a Cisco ISE CA Certificate **336**
        Import a Cisco ISE CA Certificate **337**
    Certificate Templates **337**
        Certificate Template Name Extension **337**
        Use Certificate Template Name in Authorization Policy Conditions **338**
        Deploy Cisco ISE CA Certificates for pxGrid Controller **338**
        MAC Randomization for BYOD **339**
    Simple Certificate Enrollment Protocol Profiles **339**
    Issued Certificates **340**
    Issued and Revoked Certificates **340**
    Backup and Restoration of Cisco ISE CA Certificates and Keys **341**
        Export Cisco ISE CA Certificates and Keys **341**

    - Import Cisco ISE CA Certificates and Keys 342
  - Generate Root CA and Subordinate CAs on the Primary PAN and PSN 343
  - Configure Cisco ISE Root CA as Subordinate CA of an External PKI 343
  - Configure Cisco ISE to Use Certificates for Authenticating Personal Devices 344
    - Add Users to Employee User Group 345
    - Create a Certificate Authentication Profile for TLS-Based Authentication 345
    - Create an Identity Source Sequence for TLS-Based Authentication 346
    - Configure Certificate Authority Settings 346
    - Create a CA Template 347
    - Internal CA Settings 349
    - Create a Native Supplicant Profile to be Used in Client-Provisioning Policy 349
    - Download Agent Resources from Cisco for Windows and MAC OS X Operating Systems 350
    - Create Client-Provisioning Policy Rules for Apple iOS, Android, and MAC OS X Devices 350
    - Configure the Dot1X Authentication Policy Rule for TLS-Based Authentication 351
    - Create Authorization Profiles for Central Web Authentication and Supplicant-Provisioning Flows 352
    - Create Authorization Policy Rules 352
    - CA Service Policy Reference 353
    - Client-Provisioning Policy Rules for Certificate Services 353
    - Authorization Profiles for Certificate Services 354
    - Authorization Policy Rules for Certificate Services 355
  - Cisco ISE CA Issues Certificates to ASA VPN Users 356
    - VPN Connection Certificate-Provisioning Flow 356
    - Configure Cisco ISE CA to Issue Certificates to ASA VPN Users 357
  - Revoke an Endpoint Certificate 360
- OCSP Services 360
  - Cisco ISE CA Service Online Certificate Status Protocol Responder 361
  - OCSP Certificate Status Values 361
  - Update of OCSP Responder Certificates 362
  - OCSP High Availability 362
  - OCSP Failures 362
  - Add OCSP Client Profiles 363
  - OCSP Client Profile Settings 363
  - OCSP Statistics Counters 366

Configure Admin Access Policies 367
Administrator Access Settings 367
  Configure Maximum Number of Concurrent Administrative Sessions and Login Banners 368
  Allow Administrative Access to Cisco ISE from Select IP Addresses 368
  Allow Access to MnT Nodes in Cisco ISE 369
  Configure a Password Policy for Administrator Accounts 370
  Configure Account Disable Policy for Administrator Accounts 371
  Configure Lock or Suspend Settings for Administrator Accounts 371
  Configure Session Timeout for Administrators 372
  Terminate an Active Administrative Session 372
  Change Administrator Name 372
  Admin Access Settings 373
    Administrator Password Policy Settings 373
    Session Timeout and Session Information Settings 375

CHAPTER 6 **Maintain and Monitor** 377

Adaptive Network Control 378
Enable Adaptive Network Control in Cisco ISE 379
Configure Network Access Settings 379
  Create Authorization Profiles for Network Access through ANC 380
ANC NAS Port Shutdown Flow 380
Endpoints Purge Settings 381
Quarantined Endpoints Do Not Renew Authentication Following Policy Change 382
ANC Operations Fail when IP Address or MAC Address is not Found 382
Externally Authenticated Administrators Cannot Perform ANC Operations 383
Backup Data Type 383
Backup and Restore Repositories 384
  Create Repositories 385
  Repository Settings 387
  Enable RSA Public Key Authentication in SFTP Repository 387
  Download Files from Local Disk 388
    Upload a File to Local Disk 388
On-Demand and Scheduled Backups 389
  Perform an On-Demand Backup 389

  - On-Demand Backup Settings **391**
  - Schedule a Backup **392**
  - Scheduled Backup Settings **393**
  - Backup Using the CLI **394**
  - Backup History **394**
  - Backup Failures **394**
- Cisco ISE Restore Operation **395**
  - Guidelines for Data Restoration **395**
  - Restoration of Configuration or Monitoring (Operational) Backup from the CLI **396**
  - Restore Configuration Backups from the GUI **398**
  - Restoration of Monitoring Database **398**
    - Restore a Monitoring (Operational) Backup in a Standalone Environment **399**
    - Restore a Monitoring Backup with Administration and Monitor Personas **399**
    - Restore a Monitoring Backup with a Monitoring Persona **400**
  - Restore History **400**
- Export Authentication and Authorization Policy Configuration **400**
- Schedule Policy Export Settings **401**
- Synchronize Primary and Secondary Nodes in a Distributed Environment **402**
- Recovery of Lost Nodes in Standalone and Distributed Deployments **402**
  - Recovery of Lost Nodes Using Existing IP Addresses and Hostnames in a Distributed Deployment **402**
  - Recovery of Lost Nodes Using New IP Addresses and Hostnames in a Distributed Deployment **403**
  - Recovery of a Node Using Existing IP Address and Hostname in a Standalone Deployment **404**
  - Recovery of a Node Using New IP Address and Hostname in a Standalone Deployment **404**
  - Configuration Rollback **404**
  - Recovery of Primary Node in Case of Failure in a Distributed Deployment **405**
  - Recovery of Secondary Node in Case of Failure in a Distributed Deployment **405**
- Cisco ISE Logging Mechanism **406**
  - Configure Syslog Purge Settings **406**
- Cisco ISE System Logs **407**
- Configure Remote Syslog Collection Locations **407**
- Cisco ISE Message Codes **409**
  - Set Severity Levels for Message Codes **409**
- Cisco ISE Message Catalogs **409**
- Endpoint Debug Log Collector **410**

    Download Debug Logs for a Specific Endpoint 410
Collection Filters 410
    Configure Collection Filters 411
    Event Suppression Bypass Filter 411
Cisco ISE Reports 412
Report Filters 412
Create the Quick Filter Criteria 413
Create the Advanced Filter Criteria 413
Run and View Reports 414
Reports Navigation 414
Export Reports 414
My Reports 415
Scheduling Cisco ISE Reports 415
    Use Case: Scheduled Reports 417
Cisco ISE Active RADIUS Sessions 418
    Change Authorization for RADIUS Sessions 418
Available Reports 419
RADIUS Live Logs 443
    Authentication Latency 445
RADIUS Live Sessions 446
TACACS Live Logs 449
Export Summary 450
RADIUS Live Logs 452
    Authentication Latency 454
RADIUS Live Sessions 454
TACACS Live Logs 458
Export Summary 459

CHAPTER 7 **Device Administration** 461

TACACS+ Device Administration 461
Device Administration Work Center 462
Device Administration Deployment Settings 463
Device Admin Policy Sets 463
Create Device Administration Policy Sets 464

TACACS+ Authentication Settings and Shared Secret 465
Device Administration - Authorization Policy Results 466
  Allowed Protocols in FIPS and Non-FIPS Modes for TACACS+ Device Administration 467
  TACACS+ Command Sets 467
    Wildcards and Regex in Command Sets 467
    Command Line and Command Set List Match 467
    Process Rules with Multiple Command Sets 468
  Create TACACS+ Command Sets 469
  TACACS+ Profile 469
    Create TACACS+ Profiles 470
    Common Tasks Settings 471
Change the Enable Password Through the CLI 473
Configure Global TACACS+ Settings 473
Data Migration from Cisco Secure ACS to Cisco ISE 474
Monitor Device Administration Activity 474
  TACACS Live Logs 475

CHAPTER 8 **Guest and Secure WiFi** 477
Cisco ISE Guest Services 477
  End-User Guest and Sponsor Portals in Distributed Environment 478
Guest and Sponsor Accounts 478
  Guest Types and User Identity Groups 479
  Create or Edit Guest Types 479
  Disable a Guest Type 483
  Configure Maximum Simultaneous Logins for Endpoint Users 484
  Schedule When to Purge Expired Guest Accounts 485
  Add Custom Fields for Guest Account Creation 485
  Specify Email Addresses and SMTP Servers for Email Notifications 486
  Assign Guest Locations and SSIDs 487
  Rules for Guest Password Policies 488
  Set the Guest Password Policy and Expiration 488
  Rules for Guest Username Policies 489
  Set the Guest Username Policy 490
  SMS Providers and Services 490

    - Configure SMS Gateways to Send SMS Notifications to Guests 491
  - Social Login for Self-Registered Guests 493
    - Configuring Social Login 496
- Guest Portals 497
  - Credentials for Guest Portals 498
  - Guest Access with Hotspot Guest Portals 499
  - Guest Access with Credentialed Guest Portals 499
  - Employee Access with Credentialed Guest Portals 500
  - Guest Device Compliance 500
  - Guest Portals Configuration Tasks 500
    - Enable Policy Services 501
    - Add Certificates for Guest Portals 501
    - Create External Identity Sources 502
    - Create Identity Source Sequences 503
    - Create Endpoint Identity Groups 504
    - Create a Hotspot Guest Portal 504
    - Create a Sponsored-Guest Portal 504
    - Create a Self-Registered Guest Portal 506
    - Authorize Portals 510
    - Customize Guest Portals 511
  - Configure Periodic AUP Acceptance 511
  - Forcing Periodic AUP 511
  - Guest Remember Me 512
- Sponsor Portals 512
  - Managing Guest Accounts on the Sponsor Portal 513
    - Managing Sponsor Accounts 514
    - Configure Account Content for Sponsor Account Creation 518
  - Configure a Sponsor Portal Flow 519
    - Enable Policy Services 520
    - Add Certificates for Guest Services 520
    - Create External Identity Sources 520
    - Create Identity Source Sequences 521
    - Create a Sponsor Portal 521
    - Customize Sponsor Portals 522

    - Configuring Account Content for Sponsor Account Creation **522**
    - Configuring the Time Settings Available to Sponsors **523**
    - Kerberos Authentication for the Sponsor Portal **523**
    - Sponsors Cannot Log In to the Sponsor Portal **525**
- Monitor Guest and Sponsor Activity **526**
  - Metrics Dashboard **526**
  - AUP Acceptance Status Report **526**
  - Guest Accounting Report **526**
  - Primary Guest Report **526**
  - Sponsor Login and Audit Report **527**
  - Audit Logging for Guest and Sponsor Portals **527**
- Guest Access Web Authentication Options **527**
  - NAD with Central WebAuth Process **528**
  - Wireless LAN Controller with Local WebAuth Process **530**
  - Wired NAD with Local WebAuth Process **530**
    - IP Address and Port Values Required for the Login.html Page **531**
    - HTTPS Server Enabled on the NAD **531**
    - Support for Customized Authentication Proxy Web Pages on the NAD **531**
    - Configure Web Authentication on the NAD **532**
  - Device Registration WebAuth Process **532**
- Guest Portal Settings **534**
  - Portal Identification Settings **534**
  - Portal Settings for Hotspot Guest Portals **535**
  - Acceptable Use Policy (AUP) Page Settings for Hotspot Guest Portals **537**
  - Post-Access Banner Page Settings for Hotspot Portals **538**
  - Portal Settings for Credentialed Guest Portals **538**
  - Login Page Settings for Credentialed Guest Portals **540**
  - Self-Registration Page Settings **541**
  - Self Registration Success Page Settings **544**
  - Acceptable Use Policy (AUP) Page Settings for Credentialed Guest Portals **545**
  - Guest Change Password Settings for Credentialed Guest Portals **545**
  - Guest Device Registration Settings for Credentialed Guest Portals **546**
  - BYOD Settings for Credentialed Guest Portals **546**
  - Post-Login Banner Page Settings for Credentialed Guest Portals **547**

  - Guest Device Compliance Settings for Credentialed Guest Portals **548**
  - VLAN DHCP Release Page Settings for Guest Portals **548**
  - Authentication Success Settings for Guest Portals **549**
  - Support Information Page Settings for Guest Portals **549**
- Sponsor Portal Application Settings **550**
  - Portal Identification Settings **550**
  - Portal Settings for Sponsor Portals **551**
  - Login Settings for Sponsor Portals **554**
  - Acceptable Use Policy (AUP) Settings for Sponsor Portals **554**
  - Sponsor Change Password Settings for Sponsor Portals **555**
  - Post-Login Banner Settings for Sponsor Portals **555**
  - Support Information Page Settings for Sponsor Portals **555**
  - Notify Guests Customization for Sponsor Portals **556**
  - Manage and Approve Customization for Sponsor Portals **557**
- Global Settings for Guest and Sponsor Portals **557**
- Guest Type Settings **558**
- Sponsor Group Settings **560**
- End-User Portals **563**
- Customization of End-User Web Portals **563**
- Portal Content Types **565**
- Basic Customization of Portals **565**
  - Modify the Portal Theme Colors **566**
  - Change the Portal Display Language **566**
  - Change the Portal Icons, Images, and Logos **567**
  - Update the Portal Banner and Footer Elements **567**
  - Change the Titles, Instructions, Buttons, and Label Text **568**
  - Format and Style Text Box Content **568**
  - Variables for Portal Pages Customization **569**
  - View Your Customization **572**
  - Custom Portal Files **573**
- Advanced Customization of Portals **573**
  - Portal Theme and Structure CSS Files **574**
  - Changing Theme Colors with jQuery Mobile **575**
    - Change Theme Colors with jQuery Mobile **576**

- Location Based Customization 577
- User Device Type Based Customization 578
- Export a Portal’s Default Theme CSS File 578
- Create a Custom Portal Theme CSS File 578
- Embed Links in Portal Content 579
- Insert Variables for Dynamic Text Updates 580
- Use Source Code to Format Text and Include Links 581
- Add an Image as an Advertisement 581
- Set Up Carousel Advertising 582
- Customize Greetings Based on Guest Location 584
- Customize Greetings Based on User Device Type 585
- Modify the Portal Page Layout 586
- Import the Custom Portal Theme CSS File 587
- Delete a Custom Portal Theme 588
- View Your Customization 588

Portal Language Customization 589
- Export the Language File 590
- Add or Delete Languages from the Language File 590
- Import the Updated Language File 591

Customization of Guest Notifications, Approvals, and Error Messages 592
- Customize Email Notifications 592
- Customize SMS Text Message Notifications 593
- Customize Print Notifications 594
- Customize Approval Request Email Notifications 594
- Edit Error Messages 595

Portal Pages Titles, Content and Labels Character Limits 595
- Character Limits for Portal Pages Titles, Content and Labels 596

Portal Customization 597
- CSS Classes and Descriptions for End-User Portals Page Layout 598

HTML Support for a Portal Language File 598
- HTML Support for the Blocked List Portal Language File 599
- HTML Support for Bring Your Own Device Portals Language Files 599
- HTML Support for Certificate Provisioning Portal Language Files 600
- HTML Support for Client Provisioning Portal Language Files 601

HTML Support for Credential Guest Portals Language Files 602

HTML Support for Hotspot Guest Portals Language Files 604

HTML Support for Mobile Device Management Portals Language Files 605

HTML Support for My Devices Portals Language Files 606

HTML Support for Sponsor Portals Language Files 607

CHAPTER 9 Asset Visibility 609

Administrative Access to Cisco ISE Using an External Identity Store 610

External Authentication and Authorization 611

Configure a Password-Based Authentication Using an External Identity Store 611

Create an External Administrator Group 612

Create an Internal Read-Only Admin 612

Map External Groups to the Read-Only Admin Group 613

Configure Menu Access and Data Access Permissions for External Administrator Group 613

Create an RBAC Policy for External Administrator Authentication 613

Configure Admin Access Using an External Identity Store for Authentication with Internal Authorization 614

External Authentication Process Flow 614

External Identity Sources 615

LDAP Identity Source Settings 615

RADIUS Token Identity Sources Settings 621

RSA SecurID Identity Source Settings 622

Cisco ISE Users 624

User Identity 624

User Groups 624

User Identity Groups 624

User Role 625

User Account Custom Attributes 625

User Authentication Settings 626

Generate Automatic Password for Users and Administrators 628

Internal User Operations 628

To Add Users 628

Export Cisco ISE User Data 628

Import Cisco ISE Internal Users 629

    - Endpoint Settings 629
    - Endpoint Import from LDAP Settings 631
  - Identity Group Operations 632
    - Create a User Identity Group 632
    - Export User Identity Groups 633
    - Import User Identity Groups 633
    - Endpoint Identity Group Settings 633
  - Configure Maximum Concurrent Sessions 634
    - Maximum Concurrent Sessions for a Group 634
    - Configure Counter Time Limit 635
  - Disable Account Policy 635
  - Disable Individual User Accounts 636
  - Disable User Accounts Globally 637
- Internal and External Identity Sources 637
  - Create an External Identity Source 639
  - Authenticate Internal Users Against External Identity Store Password 640
- Certificate Authentication Profiles 640
  - Add a Certificate Authentication Profile 640
- Active Directory as an External Identity Source 641
  - Active Directory-Supported Authentication Protocols and Features 642
  - Active Directory Attribute and Group Retrieval for Use in Authorization Policies 643
    - Support for Boolean Attributes 644
  - Active Directory Certificate Retrieval for Certificate-Based Authentication 645
  - Active Directory User Authentication Process Flow 645
  - Configure Resource Owner Password Credentials Flow to Authenticate Users with Microsoft Entra ID 645
    - Configure an Application for Resource Owner Password Credentials Flow in Microsoft Entra ID 646
    - Configure Resource Owner Password Credentials Flow in Cisco ISE 647
  - Support for Active Directory Multidomain Forests 647
  - Prerequisites for Integrating Active Directory and Cisco ISE 648
    - Active Directory Account Permissions Required to Perform Various Operations 649
    - Network Ports that Must Be Open for Communication 650
    - DNS Server 650

Configure Active Directory as an External Identity Source 651
  Add an Active Directory Join Point and Join Cisco ISE Node to the Join Point 651
  Add Domain Controllers 653
  MSRPC Protocol for Passive ID 653
  Leave the Active Directory Domain 656
  Configure Authentication Domains 656
  Configure Active Directory User Groups 657
  Configure Active Directory User and Machine Attributes 658
  Modify Password Changes, Machine Authentications, and Machine Access Restriction Settings 658
  Configure Maximum Password Attempts for Active Directory Account 659
  Machine Access Restriction Cache 661
  Configure Custom Schema 661
Support for Active Directory Multijoin Configuration 662
  Create a New Scope to Add Active Directory Join Points 662
Identity Rewrite 663
  Enable Identity Rewrite 664
Identity Resolution Settings 664
  Avoid Identity Resolution Issues 665
  Configure Identity Resolution Settings 665
Test Users for Active Directory Authentication 666
Delete Active Directory Configurations 666
View Active Directory Joins for a Node 667
Diagnose Active Directory Problems 667
Enable Active Directory Debug Logs 668
Obtain the Active Directory Log File for Troubleshooting 668
Active Directory Alarms and Reports 668
Active Directory Advanced Tuning 669
Configure Preferred Domain Controllers 669
Active Directory Identity Search Attributes 670
Supplemental Information for Setting Up Cisco ISE with Active Directory 671
  Configure Group Policies in Active Directory 671
  Configure Odyssey 5.X Supplicant for EAP-TLS Machine Authentications Against Active Directory 671
  Configure Agent for Machine Authentication 672

Active Directory Requirements to Support Easy Connect and Passive Identity services **672**
  Configure Active Directory for Passive Identity service **673**
  Set the Windows Audit Policy **675**
  Set Permissions when Microsoft Active Directory Users are in Domain Admin Group **676**
  Permissions for Microsoft Active Directory Users Not in Domain Admin Group **676**
  Permissions to Use DCOM on the Domain Controller **678**
Easy Connect **679**
  Configure Easy Connect Enforcement Mode **682**
  Configure Easy Connect Visibility Mode **683**
PassiveID Work Center **683**
  Initial Setup and Configuration **685**
  PassiveID Work Center Dashboard **685**
  Active Directory as a Probe and a Provider **686**
    Getting Started with the PassiveID Setup **686**
    Manage the Active Directory Provider **688**
    Active Directory Settings **688**
  Additional Passive Identity Service Providers **690**
  Active Directory Agents **693**
    Automatically Install and Deploy Active Directory Agents **693**
    Manually Install and Deploy Active Directory Agents **694**
    Uninstall the Agent **695**
    Active Directory Agent Settings **696**
  API Providers **697**
    Configure a Bridge to the ISE REST Service for Passive Identity Services **698**
    Send API Calls to the Passive ID REST Service **698**
    API Provider Settings **699**
    API Calls **699**
  SPAN **701**
    Working with SPAN **701**
    SPAN Settings **702**
  Syslog Providers **703**
    Configure Syslog Clients **703**
    Customize Syslog Message Structures (Templates) **707**
    Work with Syslog Predefined Message Templates **712**

- Filter Passive Identity Services 724
- Endpoint Probe 724
  - Work with the Endpoint Probe 726
  - Endpoint Probe Settings 726
- Subscribers 727
- Generate pxGrid Certificates for Subscribers 728
- Enable Subscribers 729
- View Subscriber Events from Live Logs 729
- Configure Subscriber Settings 729
- Monitoring and Troubleshooting Service in PassiveID Work Center 730

LDAP 730
- LDAP Directory Service 730
- Multiple LDAP Instances 731
- LDAP Failover 731
- LDAP Connection Management 731
- LDAP User Authentication 732
- LDAP Group and Attribute Retrieval for Use in Authorization Policies 732
- Errors Returned by the LDAP Server 734
- LDAP User Lookup 735
- LDAP MAC Address Lookup 735
- Add LDAP Identity Sources 735
  - LDAP Identity Source Settings 735
  - Configure LDAP Schema 741
  - Configure Primary and Secondary LDAP Servers 742
  - Enable Cisco ISE to Obtain Attributes from the LDAP Server 742
  - Retrieve Group Membership Details from the LDAP Server 742
  - Retrieve User Attributes from the LDAP Server 743
- Enable Secure Authentication with LDAP Identity Source 744

ODBC Identity Source 744
- Credential Check for ODBC Database 745
- Add ODBC Identity Source 749

RADIUS Token Identity Sources 752
- RADIUS Token Server-Supported Authentication Protocols 752
- Ports Used by the RADIUS Token Servers for Communication 752

  - RADIUS Shared Secret 752
  - Failover in RADIUS Token Servers 753
  - Configurable Password Prompt in RADIUS Token Servers 753
  - RADIUS Token Server User Authentication 753
  - User Attribute Cache in RADIUS Token Servers 753
  - RADIUS Identity Source in Identity Sequence 753
  - RADIUS Server Returns the Same Message for All Errors 754
  - Safeword Server Supports Special Username Format 754
  - Authentication Request and Response in RADIUS Token Servers 754
  - RADIUS Token Identity Sources Settings 755
  - Add a RADIUS Token Server 756
  - Delete a RADIUS Token Server 758
- RSA Identity Sources 758
  - Cisco ISE and RSA SecurID Server Integration 759
    - RSA Configuration in Cisco ISE 759
    - RSA Agent Authentication Against the RSA SecurID Server 759
    - RSA Identity Sources in a Distributed Cisco ISE Environment 759
    - RSA Server Updates in a Cisco ISE Deployment 759
    - Override Automatic RSA Routing 759
    - RSA Node Secret Reset 760
    - RSA Automatic Availability Reset 760
  - RSA SecurID Identity Source Settings 760
  - Add RSA Identity Sources 761
    - Import the RSA Configuration File 762
    - Configure the Options File for a Cisco ISE Server and Resetting SecurID and sdstatus.12 Files 762
    - Configure Authentication Control Options for RSA Identity Source 763
    - Configure RSA Prompts 764
    - Configure RSA Messages 764
- SAMLv2 Identity Provider as an External Identity Source 764
  - Enabling Session Services 766
  - Configure SAML Identity Providers in Cisco ISE 766
    - Add a SAML Identity Provider to Cisco ISE 766
    - Add an SAML Identity Provider as Authentication Method of a Portal 767
    - Configure SAML ID Provider 767

- Delete an Identity Provider **770**
- SAML-Based Admin Login **770**
- Authentication Failure Log **771**

Identity Source Sequences **772**

- Create Identity Source Sequences **772**
- Delete Identity Source Sequences **773**

Identity Source Details in Reports **773**

- Authentications Dashlet **773**
- Identity Source Reports **773**

Profiled Endpoints on the Network **773**

Profiler Condition Settings **774**

Profiled Endpoints on the Network **774**

Profiler Condition Settings **775**

Cisco ISE Profiling Service **775**

- Profiler Work Center **776**
- Profiler Dashboard **776**
- Endpoint Inventory Using Profiling Service **776**
- Cisco ISE Profiler Queue Limit Configuration **777**
- Martian IP Addresses **777**

Profiler Forwarder Persistence Queue **778**

Configure Profiling Service in Cisco ISE Nodes **778**

Network Probes Used by Profiling Service **778**

- IP Address and MAC Address Binding **779**
- NetFlow Probe **779**
- DHCP Probe **780**
  - Wireless LAN Controller Configuration in DHCP Bridging Mode **780**
- DHCP SPAN Probe **780**
- HTTP Probe **781**
- HTTP SPAN Probe **781**
  - Unable to Collect HTTP Attributes in Cisco ISE Running on VMware **781**
- pxGrid Probe **781**
- RADIUS Probe **782**
- Network Scan (NMAP) Probe **783**
  - SNMP Read Only Community Strings for NMAP Manual Subnet Scan **784**

        - Manual NMAP Scan Results **784**
    - DNS Probe **784**
        - DNS FQDN Lookup **785**
        - Configure Call Station ID Type in the WLC Web Interface **785**
    - SNMP Query Probe **786**
        - Cisco Discovery Protocol Support with SNMP Query **786**
        - Link Layer Discovery Protocol Support with SNMP Query **786**
    - SNMP Trap Probe **787**
    - Active Directory Probe **788**
- Configure Probes for Each Cisco ISE Node **788**
- Setup CoA, SNMP RO Community, and Endpoint Attribute Filter **789**
    - Global Configuration of Change of Authorization for Authenticated Endpoints **790**
    - Use Cases for Issuing Change of Authorization **791**
    - Exemptions for Issuing a Change of Authorization **791**
    - Change of Authorization Issued for Each Type of CoA Configuration **792**
- Attribute Filters for ISE Database Persistence and Performance **793**
    - Global Setting to Filter Endpoint Attributes **793**
- Attributes Collection from Cisco IOS Sensor-Embedded Switches **795**
    - Cisco IOS Sensor-Embedded Network Access Devices **795**
    - Configuration Checklist for Cisco IOS Sensor-Enabled Network Access Devices **796**
- Support for Cisco IND Controllers by ISE Profiler **797**
- Cisco ISE Support for MUD **799**
- Profiler Conditions **800**
- Profiling Network Scan Actions **801**
    - Create a New Network Scan Action **801**
        - NMAP Operating System Scan **802**
        - Operating System Ports **803**
        - NMAP SNMP Port Scan **806**
        - NMAP Common Ports Scan **807**
        - Common Ports **807**
        - NMAP Custom Ports Scan **808**
        - NMAP Include Service Version Information Scan **808**
        - NMAP SMB Discovery Scan **808**
        - Skip NMAP Host Discovery **809**

    - NMAP Scan Workflow 809
    - Exclude Subnets from NMAP Scan 811
    - Manual NMAP Scan Settings 811
    - Configure Profiler Policies Using the McAfee ePolicy Orchestrator 812
    - Profiler Endpoint Custom Attributes 814
- Create a Profiler Condition 815
- Endpoint Profiling Policy Rules 815
- Endpoint Profiling Policies Settings 816
- Create Endpoint Profiling Policies 819
  - Change of Authorization Configuration for Each Endpoint Profiling Policy 820
  - Import Endpoint Profiling Policies 821
  - Export Endpoint Profiling Policies 821
- Predefined Endpoint Profiling Policies 822
  - Predefined Endpoint Profiling Policies Overwritten During Upgrade 823
  - Unable to Delete Endpoint Profiling Policies 823
  - Predefined Profiling Policies for Draeger Medical Devices 823
  - Endpoint Profiling Policy for Unknown Endpoints 824
  - Endpoint Profiling Policy for Statically Added Endpoints 824
  - Endpoint Profiling Policy for Static IP Devices 824
  - Endpoint Profiling Policy Matching 824
  - Endpoint Profiling Policies Used for Authorization 825
- Wi-Fi Device Analytics Data from Cisco Catalyst 9800 Wireless LAN Controller 825
- Endpoint Profiling Policies Grouped into Logical Profiles 826
  - Create Logical Profiles 827
- Profiling Exception Actions 827
  - Create Exception Actions 828
- Create Endpoints with Static Assignments of Policies and Identity Groups 828
  - Import Endpoints Using a CSV File 829
    - Default Import Template Available for Endpoints 830
    - Unknown Endpoints Reprofiled During Import 830
    - Endpoints with Invalid Attributes Not Imported 831
  - Import Endpoints from LDAP Server 831
  - Export Endpoints Using CSV File 832
- Identified Endpoints 833

- Identified Endpoints Locally Stored in Policy Service Nodes Database **833**
- Policy Service Nodes in Cluster **834**

Create Endpoint Identity Groups **835**

- Identified Endpoints Grouped in Endpoint Identity Groups **835**
- Default Endpoint Identity Groups Created for Endpoints **835**
- Endpoint Identity Groups Created for Matched Endpoint Profiling Policies **836**
- Add Static Endpoints in Endpoint Identity Groups **836**
- Dynamic Endpoints Reprofiled After Adding or Removing in Identity Groups **837**
- Endpoint Identity Groups Used in Authorization Rules **837**

Anycast and Profiler Services **837**

Profiler Feed Service **838**

- Configure Profiler Feed Service **838**
- Configure Profiler Feed Services Offline **840**
  - Download Offline Update Package **840**
  - Apply Offline Feed Updates **841**
  - Configure Email Notifications for Profile and OUI Updates **841**
- Undo Feed Updates **841**

Profiler Reports **841**

Detect Anomalous Behavior of Endpoints **842**

- Set Authorization Policy Rules for Endpoints with Anomalous Behavior **843**
- View Endpoints with Anomalous Behavior **843**

Agent Download Issues on Client Machine **844**

Endpoints **844**

- Endpoint Settings **844**
- Endpoint Import from LDAP Settings **846**
- Endpoint Profiling Policies Settings **847**
- Endpoint Context Visibility Using UDID Attribute **851**
- Endpoint Scripts Wizard for Windows and MacOS Endpoints **851**
  - Endpoint Scripts Provisioning Summary Report **853**

Agent Download Issues on Client Machine **854**

Endpoints **854**

- Endpoint Settings **854**
- Endpoint Import from LDAP Settings **856**
- Endpoint Profiling Policies Settings **857**

  - Endpoint Context Visibility Using UDID Attribute 861
  - Endpoint Scripts Wizard for Windows and MacOS Endpoints 861
    - Endpoint Scripts Provisioning Summary Report 863
- IF-MIB 864
- SNMPv2-MIB 864
- IP-MIB 864
- CISCO-CDP-MIB 865
- CISCO-VTP-MIB 866
- CISCO-STACK-MIB 866
- BRIDGE-MIB 866
- OLD-CISCO-INTERFACE-MIB 866
- CISCO-LWAPP-AP-MIB 867
- CISCO-LWAPP-DOT11-CLIENT-MIB 868
- CISCO-AUTH-FRAMEWORK-MIB 869
- EEE8021-PAE-MIB: RFC IEEE 802.1X 869
- HOST-RESOURCES-MIB 869
- LLDP-MIB 870
- Session Trace for an Endpoint 870
  - Session Removal from the Directory 872
- Global Search for Endpoints 872
- Session Trace for an Endpoint 873
  - Session Removal from the Directory 875
- Global Search for Endpoints 875

CHAPTER 10 **Bring Your Own Device (BYOD)** 877

- Personal Devices on a Corporate Network (BYOD) 877
  - End-User Device Portals in a Distributed Environment 877
  - Global Settings for Device Portals 878
- Personal Device Portals 878
  - Access Device Portals 878
  - Blocked List Portal 879
  - Certificate Provisioning Portal 879
  - Bring Your Own Device Portal 879
  - Client Provisioning Portal 880

Mobile Device Management Portal 880
My Devices Portal 881
BYOD Deployment Options and Status Flow 881
Limit the Number of Personal Devices Registered by Employees 884
Support Device Registration Using Native Supplicants 884
Operating Systems Supported by Native Supplicants 884
Allow Employees to Register Personal Devices Using Credentialed Guest Portals 885
Provide a URL to Reconnect with BYOD Registration 885
Device Portals Configuration Tasks 886
Enable Policy Services 887
Add Certificates to the Device Portal 887
Create External Identity Sources 888
Create Identity Source Sequences 888
Create Endpoint Identity Groups 889
Edit the Blocked List Portal 889
Create a BYOD Portal 892
Create a Certificate Provisioning Portal 893
Create a Client Provisioning Portal 894
Create an MDM Portal 896
Create a My Devices Portal 897
Create Authorization Profiles 898
Create Authorization Profiles 898
Create Authorization Policy Rules 899
Customize Device Portals 899
Manage Personal Devices Added by Employees 900
Display Devices Added by an Employee 900
Errors When Adding Devices to My Devices Portal 900
Devices Deleted from My Devices Portal Remain in Endpoints Database 900
Limit the Number of Personal Devices Registered by Employees 901
Monitor My Devices Portals and Endpoints Activity 901
My Devices Login and Audit Report 901
Registered Endpoints Report 901

CHAPTER 11 Secure Access 903

Define Network Devices in Cisco ISE 903
  Define a Default Network Device in Cisco ISE 904
  Network Devices 905
    Network Device Definition Settings 905
    Default Network Device Definition Settings 914
    Network Device Import Settings 916
  Add a Network Device in Cisco ISE 917
  Import Network Devices into Cisco ISE 917
  Export Network Devices from Cisco ISE 918
  Troubleshoot Network Device Configuration Issues 919
  The Execute Network Device Command Diagnostic Tool 919
Third-Party Network Device Support in Cisco ISE 919
  Network Device Profiles 922
  Configure a Third-Party Network Device in Cisco ISE 923
  Create a Network Device Profile 924
  Export Network Device Profiles from Cisco ISE 925
  Import Network Device Profiles into Cisco ISE 926
Manage Network Device Groups 926
  Network Device Group Settings 926
  Network Device Group Import Settings 927
Network Device Groups 928
  Network Device Attributes Used by Cisco ISE in Policy Evaluation 929
  Import Network Device Groups into Cisco ISE 929
  Export Network Device Groups from Cisco ISE 930
  Manage Network Device Groups 930
    Network Device Group Settings 930
    Network Device Group Import Settings 930
Import Templates in Cisco ISE 931
  Network Devices Import Template Format 931
  Network Device Groups Import Template Format 934
IPsec Security to Secure Communication Between Cisco ISE and NAD 935
  Configure RADIUS IPSec on Cisco ISE 935
    Configure and Install X.509 Certificates on ESR-5921 939
    Example: Output of Pre-shared Key Configuration on Cisco Catalyst 3850 Series Switches 944

Mobile Device Manager Interoperability with Cisco ISE **945**
  - Supported Mobile Device Management Use Cases **946**
  - Supported Unified Endpoint Management and Mobile Device Management Servers **950**
  - Ports Used by the Mobile Device Management Server **951**
  - Mobile Device Management Integration Process Flow **951**
  - Handle Random and Changing MAC Addresses with Mobile Device Management Servers **952**

Set Up Mobile Device Management Servers with Cisco ISE **953**
  - Import Mobile Device Management Server Certificate into Cisco ISE **954**
  - Define Device Management Servers in Cisco ISE **954**
  - Configure Mobile Device Management Servers in Cisco ISE **955**
  - Cisco ISE MDM Support for Microsoft Intune and Microsoft SCCM **960**
  - Policy Set Example for Microsoft System Center Configuration Manager **961**
  - Configure the Microsoft System Center Configuration Manager Server for Cisco ISE **962**
    - Set Permissions when Microsoft Active Directory Users are in Domain Admin Group **963**
    - Permissions for Microsoft Active Directory Users Not in Domain Admin Group **963**
    - Permissions to Use DCOM on the Domain Controller **965**
    - Set Permissions for Access to WMI Root and CIMv2 Namespace **966**
  - Open Firewall Ports for WMI Access **967**
  - Select Configuration Baseline Policies for Endpoint Compliance from Desktop Device Manager Server **968**
  - Configure an Authorization Profile for Redirecting Nonregistered Devices **969**
  - Configure Authorization Policy Rules for the MDM Use Cases **970**
  - Configure ACLs on Wireless Controllers for MDM Interoperability **971**
  - Wipe or Lock a Device **972**
  - View Mobile Device Management Reports **973**
  - View Mobile Device Management Logs **973**

CHAPTER 12 **Segmentation** 975

Policy Sets **975**

Policy Set Configuration Settings **977**

Authentication Policies **978**
  - Authentication Failures—Policy Result Options **980**
    - Use Cases for Using Continue as the Course of Action for Authentication Failures **981**
  - Configure Authentication Policies **982**

- Authentication Policy Configuration Settings 983
- Password-Based Authentication 985
  - Secure Authentication Using Encrypted Passwords and Cryptographic Techniques 985
  - Authentication Methods and Authorization Privileges 986
- Authentication Dashlet 986
  - View Authentication Results 986
  - Authentication Reports and Troubleshooting Tools 987

Authorization Policies 987

- Cisco ISE Authorization Profiles 988
  - Permissions for Authorization Profiles 988
  - Location Based Authorization 989
  - Downloadable ACLs 990
  - Machine Access Restriction for Active Directory User Authorization 992
- Guidelines for Configuring Authorization Policies and Profiles 992
- Configure Authorization Policies 993
- Authorization Policy Settings 995
- Authorization Profile Settings 997
- Authorization Policy Exceptions 1001
  - Local and Global Exceptions Configuration Settings 1001

Policy Conditions 1001

- Dictionaries and Dictionary Attributes 1002
- System Defined Dictionaries and Dictionary Attributes 1007
- Display System Dictionaries and Dictionary Attributes 1007
- User-Defined Dictionaries and Dictionary Attributes 1007
- Create User-Defined Dictionaries 1008
- Create User-Defined Dictionary Attributes 1008
- RADIUS-Vendor Dictionaries 1008
  - Create RADIUS-Vendor Dictionaries 1009
  - Create RADIUS-Vendor Dictionary Attributes 1009
  - HP RADIUS IETF Service Type Attributes 1009
- RADIUS Vendor Dictionary Attribute Settings 1010
- Navigate the Conditions Studio 1011
- Configure, Edit and Manage Policy Conditions 1015

Special Network Access Conditions 1020

  - Configure Device Network Conditions 1020
  - Configure Device Port Network Condition 1021
  - Configure Endstation Network Conditions 1021
  - Create Time and Date Conditions 1022
  - Use IPv6 Condition Attributes in Authorization Policies 1022
- Policy Set Protocol Settings 1024
  - Supported Network Access Policy Set Protocols 1024
  - Guidelines for Using EAP-FAST as Protocol 1024
  - Configure EAP-FAST Settings 1025
  - Generate the PAC for EAP-FAST 1025
  - EAP-FAST Settings 1026
  - PAC Settings 1026
  - Using EAP-TTLS as Authentication Protocol 1028
  - Configure EAP-TTLS Settings 1028
  - EAP-TTLS Settings 1028
  - Configure EAP-TLS Settings 1029
  - EAP-TLS Settings 1029
  - Configure PEAP Settings 1030
  - PEAP Settings 1031
  - Configure RADIUS Settings 1031
  - RADIUS Settings 1032
  - Configure Security Settings 1036
  - Supported Cipher Suites 1040
  - RADIUS Protocol Support in Cisco ISE 1043
  - Allowed Protocols 1044
  - PAC Options 1054
  - Cisco ISE Acting as a RADIUS Proxy Server 1057
    - Configure External RADIUS Servers 1057
    - Define RADIUS Server Sequences 1058
  - Cisco ISE Acting as a TACACS+ Proxy Client 1058
    - Configure External TACACS+ Servers 1059
    - TACACS+ External Server Settings 1059
    - Define TACACS+ Server Sequences 1060
    - TACACS+ Server Sequence Settings 1061

    - Network Access Service 1061
        - Define Allowed Protocols for Network Access 1062
        - Network Access for Users 1063
- Enable MAB from Non-Cisco Devices 1068
- Enable MAB from Cisco Devices 1069
- TrustSec Architecture 1071
    - TrustSec Components 1071
    - TrustSec Terminology 1073
    - Supported Switches and Required Components for TrustSec 1073
- Integration with Cisco Catalyst Center 1074
- TrustSec Dashboard 1075
    - Metrics 1075
    - Current Network Status 1076
        - Active SGT Sessions 1076
        - Alarms 1076
        - Quick View 1077
    - Live Log 1078
- Configure TrustSec Global Settings 1078
    - General TrustSec Settings 1079
- Configure TrustSec Matrix Settings 1082
    - TrustSec Matrix Settings 1082
- Configure TrustSec Devices 1084
    - OOB TrustSec PAC 1084
        - Generate a TrustSec PAC from the Settings Screen 1084
        - Generate a TrustSec PAC from the Network Devices Screen 1085
        - Generate a TrustSec PAC from the Network Devices List Screen 1085
    - Push Button 1085
- Configure Cisco TrustSec AAA Servers 1086
- TrustSec HTTPS Servers 1087
    - Add an External Server to Cisco ISE TrustSec HTTPS Servers 1087
- Security Groups Configuration 1089
    - Managing Security Groups in Cisco ISE 1089
    - Import Security Groups into Cisco ISE 1090
    - Export Security Groups from Cisco ISE 1091

    - Add IP SGT Static Mapping 1091
    - Deploy IP SGT Static Mappings 1092
    - Import IP SGT Static Mappings into Cisco ISE 1093
    - Export IP SGT Static Mappings from Cisco ISE 1093
    - Add SGT Mapping Group 1093
    - Add Security Group Access Control Lists 1094
- Egress Policy 1096
    - Source Tree View 1096
    - Destination Tree View 1096
    - Matrix View 1097
        - Matrix Dimensions 1097
        - Create Custom View 1097
        - Matrix Operations 1098
    - Configure Work Process Settings 1099
    - Matrices Listing Page 1099
    - TrustSec Matrix Workflow Process 1100
    - Egress Policy Table Cells Configuration 1106
        - Add the Mapping of Egress Policy Cells 1106
        - Export Egress Policy 1107
        - Import Egress Policy 1108
    - Configure SGT from Egress Policy 1108
    - Monitor Mode 1109
        - Features of Monitor Mode 1109
        - The Unknown Security Group 1109
        - Default Policy 1109
- SGT Assignment 1110
    - NDAC Authorization 1111
        - Configure NDAC Authorization 1111
    - Configure End User Authorization 1111
- TrustSec Configuration and Policy Push 1112
    - CoA Supported Network Devices 1112
    - Push Configuration Changes to Non-CoA Supporting Devices 1112
        - SSH Key Validation 1113
    - Environment CoA Notification Flow 1114

    Environment CoA Triggers 1115
  Update SGACL Content Flow 1116
    Initiate an Update SGACL Named List CoA 1117
  Policies Update CoA Notification Flow 1118
  Update SGT Matrix CoA Flow 1118
    Initiate Update SGT Matrix CoA from Egress Policy 1119
  TrustSec CoA Summary 1119
Security Group Tag Exchange Protocol 1120
  Add an SXP Device 1122
Add an SXP Domain Filter 1122
Configure SXP Settings 1123
Connect Cisco Application Centric Infrastructure with Cisco ISE 1124
Configure ACI Settings 1125
Cisco ACI and Cisco SD-Access Integration with Virtual Network Awareness 1127
  Configure Cisco ISE for Cisco ACI and Cisco SD-Access Integration 1133
  Verify Cisco ACI and Cisco SD-Access Integration 1135
Run Top N RBACL Drops by User Report 1137

CHAPTER 13 Compliance 1139
Posture Types 1140
Agentless Posture 1142
Agentless Posture Troubleshooting 1145
Posture Administration Settings 1145
  Client Posture Requirements 1146
  Timer Settings for Clients 1147
    Set Remediation Timer for Clients to Remediate Within Specified Time 1147
    Set Network Transition Delay Timer for Clients to Transition 1148
    Set Login Success Window to Close Automatically 1148
  Set Posture Status for Nonagent Devices 1149
  Posture Lease 1149
  Periodic Reassessments 1150
    Configure Periodic Reassessments 1150
  Posture Troubleshooting Settings 1151
Posture General Settings 1152

Download Posture Updates to Cisco ISE 1153
  Cisco ISE Offline Updates 1154
    1154
  Download Posture Updates Automatically 1155
Posture Acceptable Use Policy Configuration Settings 1155
Configure Acceptable Use Policies for Posture Assessment 1156
Posture Conditions 1157
  Simple Posture Conditions 1157
  Create Simple Posture Conditions 1158
  Compound Posture Conditions 1158
    Create Compound Posture Conditions 1158
    Dictionary Compound Condition Settings 1159
  Predefined Condition for Enabling Automatic Updates in Windows Clients 1160
  Preconfigured Antivirus and Antispyware Conditions 1160
    Antivirus and Antispyware Support Chart 1160
Compliance Module 1161
Check Posture Compliance 1162
Create Patch Management Conditions 1162
Create Disk Encryption Conditions 1163
Posture Condition Settings 1164
  File Condition Settings 1164
  Firewall Condition Settings 1170
  Registry Condition Settings 1171
  Continuous Endpoint Attribute Monitoring 1172
  Application Condition Settings 1172
  Service Condition Settings 1173
  Posture Compound Condition Settings 1174
  AntiVirus Condition Settings 1175
  Antispyware Compound Condition Settings 1177
  Antimalware Condition Settings 1179
  Dictionary Simple Condition Settings 1180
  Dictionary Compound Condition Settings 1181
  Patch Management Condition Settings 1182
  Disk Encryption Condition Settings 1184

  - USB Condition Settings 1185
  - Hardware Attributes Condition Settings 1186
  - Posture External DataSource Condition 1186
- Configure Posture Policies 1186
- Configure AnyConnect Workflow 1188
- Prerequisite for Certificate-Based Conditions 1190
- Default Posture Policies 1192
- Client Posture Assessment 1193
- Posture Assessment Options 1193
- Posture Remediation Options 1195
- Custom Conditions for Posture 1195
- Posture Endpoint Custom Attributes 1196
- Create Posture Policy Using Endpoint Custom Attributes 1196
- Custom Posture Remediation Actions 1197
  - Add an Antispyware Remediation 1197
  - Add an Antivirus Remediation 1197
  - Add a File Remediation 1198
  - Add a Script Remediation 1198
    - Establish Trust to Execute Script Condition 1199
    - Script Download 1200
  - Add a Launch Program Remediation 1200
    - Troubleshoot Launch Program Remediation 1201
  - Add a Link Remediation 1201
  - Add a Patch Management Remediation 1202
  - Add a Windows Server Update Services Remediation 1202
  - Add a Windows Update Remediation 1202
- Posture Assessment Requirements 1203
  - Client System Stuck in Noncompliant State 1204
  - Create Client Posture Requirements 1204
- Posture Reassessment Configuration Settings 1205
- Custom Permissions for Posture 1207
- Configure Standard Authorization Policies 1208
- Best Practices for Network Drive Mapping with Posture 1208
- Configure AnyConnect Stealth Mode Workflow 1208

  Create an AnyConnect Agent Profile 1209
  Create an AnyConnect Configuration for AnyConnect Packages 1210
  Upload an Open DNS Profile in Cisco ISE 1210
  Create a Client Provisioning Policy 1210
  Create a Posture Condition 1211
  Create Posture Remediation 1211
  Create Posture Requirement in Stealth Mode 1211
  Create Posture Policy 1212
Enable AnyConnect Stealth Mode Notifications 1212
Configure Cisco Temporal Agent Workflow 1213
  Create Posture Condition 1213
  Create Posture Requirements 1214
  Create the Posture Policy 1214
  Configure the Client Provisioning Policy 1214
  Download and Launch Cisco Temporal Agent 1214
Posture Troubleshooting Tool 1215
Configure Endpoint Login Credentials 1215
Endpoint Scripts Settings 1215
Configure Client Provisioning in Cisco ISE 1216
Client Provisioning Resources 1217
  Add Client Provisioning Resources from Cisco 1218
  Add Cisco Provided Client Provisioning Resources from a Local Machine 1219
  Add Customer Created Resources for AnyConnect from a Local Machine 1220
Create Native Supplicant Profiles 1220
  Native Supplicant Profile Settings 1221
Client Provisioning Without URL Redirection for Different Networks 1223
AMP Enabler Profile Settings 1224
  Create an AMP Enabler Profile Using the Embedded Profile Editor 1225
  Create an AMP Enabler Profile Using the Standalone Editor 1225
  Troubleshoot Common AMP Enabler Installation Errors 1227
Cisco ISE Support for Onboarding Chromebook Devices 1227
  Best Practices for Using Chromebook Device in a Shared Environment 1229
  Chromebook Onboarding Process 1229
  Configure the Network and Force Extensions in the Google Admin Console 1229

Configure Cisco ISE for Chromebook Onboarding 1231
Wipe a Chromebook Device 1232
Enroll Chromebook to the Google Admin Console 1232
Connect Chromebook to the Cisco ISE Network for BYOD On Boarding 1233
Google Admin Console - Wi-Fi Network Settings 1233
Monitor Chromebook Device Activities in Cisco ISE 1237
Troubleshoot Chromebook Device Onboarding 1237
Cisco AnyConnect Secure Mobility 1238
Create AnyConnect Configuration 1238
Create a Posture Agent Profile 1240
Client IP Address Refresh Configuration 1240
Posture Protocol Settings 1242
Continuous Endpoint Attribute Monitoring 1242
Posture State Synchronization 1243
Configure Posture State Synchronization 1244
Cisco Web Agent 1245
Configure Client Provisioning Resource Policies 1245
Configure Cisco ISE Posture Agent in the Client Provisioning Policy 1246
Configure Native Supplicants for Personal Devices 1247
Client Provisioning Reports 1248
Client Provisioning Event Logs 1248
Portal Settings for Client Provisioning Portals 1248
HTML Support for Client Provisioning Portal Language Files 1251
Portal Settings for Client Provisioning Portals 1252
HTML Support for Client Provisioning Portal Language Files 1254

CHAPTER 14 **Threat Containment** 1257
Threat Centric NAC Service 1257
Enable Threat Centric NAC Service 1260
Add SourceFire FireAMP Adapter 1261
Configure Cognitive Threat Analytics Adapter 1262
Configure Authorization Profiles for CTA Adapter 1263
Configure Authorization Policy using the Course of Action Attribute 1264
Support for Vulnerability Assessment in Cisco ISE 1264

- Enable and Configure Vulnerability Assessment Service 1265
  - Enable Threat Centric NAC Service 1266
  - Configure Qualys Adapter 1266
  - Configure Nexpose Adapter 1269
  - Configure Tenable Adapter 1270
  - Configure Authorization Profile 1273
  - Configure Exception Rule to Quarantine a Vulnerable Endpoint 1273
  - Vulnerability Assessment Logs 1274

Trusted Certificate Settings 1274

Maintenance Settings 1276
- Repository Settings 1276
- On-Demand Backup Settings 1277
- Scheduled Backup Settings 1278
- Schedule Policy Export Settings 1279

General TrustSec Settings 1279

Network Resources 1282
- Support for Session Aware Networking (SAnet) 1282
- Network Devices 1282
  - Network Device Definition Settings 1283
  - Default Network Device Definition Settings 1292
  - Device Security Settings 1294
  - Network Device Import Settings 1294
- Manage Network Device Groups 1295
  - Network Device Group Settings 1295
  - Network Device Group Import Settings 1296
- Network Device Profiles Settings 1296
- External RADIUS Server Settings 1301
- RADIUS Server Sequences 1302
- NAC Manager Settings 1303

Device Portal Management 1304
- Configure Device Portal Settings 1304
  - Portal Identification Settings for Device Portals 1304
  - Portal Settings for BYOD and MDM Portals 1305
  - BYOD Settings for BYOD Portals 1307

Portal Settings for Certificate Provisioning Portal 1308
Portal Settings for Client Provisioning Portals 1311
Employee Mobile Device Management Settings for MDM Portals 1313
Portal Settings for My Devices Portals 1314
Login Page Settings for My Devices Portals 1316
Acceptable Use Policy Page Settings for My Devices Portals 1317
Post-Login Banner Page Settings for My Devices Portals 1317
Employee Change Password Settings for My Devices Portals 1317
Manage Device Settings for My Devices Portal 1318
Add, Edit, and Locate Device Customization for My Devices Portals 1319
Support Information Page Settings for Device Portals 1319

CHAPTER 15 **Cisco pxGrid** 1321
Cisco pxGrid and ISE 1321
pxGrid Summary Page 1324
pxGrid Client Management 1324
Control pxGrid Policies 1325
Enable pxGrid Service 1326
pxGrid Diagnostics 1326
pxGrid Settings 1327
Generate Cisco pxGrid Certificate 1327
Known Limitations in pxGrid Certificate Generation 1328

CHAPTER 16 **Integration** 1331
Enable Your Switch to Support Standard Web Authentication 1331
Define Local Username and Password for Synthetic RADIUS Transactions 1332
Configure NTP Server for Accurate Log and Accounting Timestamps 1332
Command to Enable AAA Functions 1332
RADIUS Server Configuration on the Switch 1333
Enable Switch to Handle RADIUS Change of Authorization (CoA) 1333
Enable Device Tracking and DHCP Snooping on Switch Ports 1334
Enable 802.1X Port-Based Authentication for Switch Ports 1334
Enable EAP for Critical Authentications 1334
Throttle AAA Requests Using Recovery Delay 1334

VLAN Definitions Based on Enforcement States 1335
Local (Default) Access List (ACL) Definitions on the Switch 1335
Enable Switch Ports for 802.1X and MAB 1336
Command to Enable 802.1X based on Identity-Based Networking Services 1338
Enable EPM Logging 1340
Enable Switch to Receive SNMP Traps 1340
Enable SNMP v3 Query for Profiling on Switch 1340
Enable MAC Notification Traps for Profiler to Collect 1340
Configure RADIUS Idle-Timeout on the Switch 1340
Wireless Controller Configuration for iOS Supplicant Provisioning 1341
Configure ACLs on Wireless Controllers for MDM Interoperability 1341

CHAPTER 17

Troubleshoot 1343

Monitoring and Troubleshooting Service in Cisco ISE 1343
  Open TAC Support Cases in Cisco ISE 1344
  Health Check 1346
    Run Health Check 1347
  Network Privilege Framework Event Flow Process 1348
  User Roles and Permissions for Monitoring and Troubleshooting Capabilities 1349
  Data Stored in the Monitoring Database 1349
Cisco ISE Telemetry 1349
Information that Telemetry Gathers 1350
SNMP Traps to Monitor Cisco ISE 1352
Cisco ISE Alarms 1355
  Alarm Settings 1370
  Configure Authorization Result Alarm 1371
  Add Custom Alarms 1372
  Cisco ISE Alarm Notifications and Thresholds 1373
  Enable and Configure Alarms 1373
  Cisco ISE Alarms for Monitoring 1373
  View Monitoring Alarms 1373
Log Collection 1374
  Alarm Syslog Collection Location 1374
RADIUS Live Logs 1375

TACACS Live Logs 1377

Live Authentications 1378

  Monitor Live Authentications 1379

    Filter Data in the Live Authentications Page 1379

RADIUS Live Sessions 1380

Export Summary 1384

Authentication Summary Report 1385

  Troubleshoot Network Access Issues 1385

Cisco Support Diagnostics for Deployment and Support Information 1386

Obtain Configuration Backup Using Cisco Support Diagnostics Connector 1387

Diagnostic Troubleshooting Tools 1388

  The RADIUS Authentication Troubleshooting Tool 1388

  Troubleshoot Unexpected RADIUS Authentication Results 1388

  The Execute Network Device Command Diagnostic Tool 1389

  Execute Cisco IOS show Commands to Check Configuration 1389

  The Evaluate Configuration Validator Tool 1389

  Agentless Posture Troubleshooting 1389

  Troubleshoot Network Device Configuration Issues 1390

  Troubleshoot Endpoint Posture Failure 1390

Session Trace Test Cases 1391

  Configure a Session Trace Test Case 1391

TCP Dump Utility to Validate Incoming Traffic 1392

  Use TCP Dump to Monitor Network Traffic 1392

  Save a TCP Dump File 1393

  Compare Unexpected SGACL for an Endpoint or User 1394

  Egress Policy Diagnostic Flow 1394

  Troubleshoot Connectivity Issues in a Trustsec-Enabled Network with SXP-IP Mappings 1394

  Troubleshoot Connectivity Issues in a TrustSec-Enabled Network with IP-SGT Mappings 1395

  Device SGT Tool 1395

  Troubleshoot Connectivity Issues in a TrustSec-Enabled Network by Comparing Device SGT Mappings 1395

Obtaining Additional Troubleshooting Information 1396

  Cisco ISE Support Bundle 1396

  Support Bundle 1397

Download Cisco ISE Log Files **1397**

Cisco ISE Debug Logs **1398**

  Obtain Debug Logs **1398**

  Cisco ISE Components and Corresponding Debug Logs **1398**

  Configure Debug Wizard by Function **1400**

Download Debug Logs **1401**

CHAPTER 1

New and Changed Information

- New and Changed Information, on page 1

New and Changed Information

The following table summarizes the new and changed features and tells you where they are documented.

Table 1: New and Changed Features in Cisco ISE Release 3.1

Feature	Description
Cisco ISE Release 3.1 Patch 8	
Wi-Fi Device Analytics Data from Cisco Catalyst 9800 Wireless LAN Controller	You can create profiling policies, authorization conditions, and authentication conditions and policies for Apple, Intel, and Samsung endpoints, using device analytics data from the Cisco Wireless LAN Controllers integrated with your Cisco ISE. For more information, see "Wi-Fi Device Analytics Data from Cisco Catalyst 9800 Wireless LAN Controller" in the Chapter "Asset Visibility" in the Cisco ISE Administration Guide, Release 3.1.
Cisco ISE Release 3.1 Patch 7	
Link External LDAP Users to Cisco ISE Endpoint Groups	From Cisco ISE Release 3.1 Patch 7, you can assign external LDAP user groups to Endpoint Identity Groups for guest devices using the **Dynamic** option. For more information, see "Create or Edit Guest Types" in the chapter "Guest and Secure WiFi" in the *Cisco Identity Services Engine Administrator Guide, Release 3.1*.
Cisco ISE Release 3.1 Patch 5	

Feature	Description
Automatically Assign Logical Profiles to Endpoints	When an endpoint goes through Cisco ISE profiling workflows, if the endpoint matches an endpoint profiling policy with an associated logical profile, the endpoint is automatically assigned the logical profile. For more information, see "Endpoint Profiling Policies Grouped into Logical Profiles" in the chapter "Asset Visibility" in the *Cisco Identity Services Engine Administrator Guide, Release 3.1*.
Support for Cisco Secure Client	Cisco ISE 3.1 Patch 5 supports both AnyConnect and Cisco Secure Client for Windows, macOS, and Linux operating systems. The following Cisco Secure Client versions are supported for these operating systems: • Windows: Cisco Secure Client version 5.00529 and later • macOS: Cisco Secure Client version 5.00556 and later • Linux: Cisco Secure Client version 5.00556 and later You can configure both AnyConnect and Cisco Secure Client for your endpoints on these operating systems but only one policy will be considered at run time for an endpoint. For more information, see the Chapter "Compliance" in *Cisco ISE Administrator Guide, Release 3.1*.
Cisco ISE Release 3.1 Patch 4	
Enhancement to the Groups tab in the REST Identity Store	You can now retrieve, filter, and delete REST identity store groups while configuring Resource Owner Password Credentials in Cisco ISE. While adding the groups, click Retrieve Groups to import the user groups from the connected identity source. Check the check boxes next to the groups that you want to select and click Save. You can also select all the groups, if needed. The selected groups are listed in the Groups tab. You can filter the results using the filter option. To delete a user group, check the check box next to the group that you want to delete and click Delete. For more information, see "Configure Resource Owner Password Credentials Flow" in the Chapter "Asset Visibility" in the *Cisco ISE Administrator Guide, Release 3.1*.

Feature	Description
Cisco ISE Release 3.1 Patch 3	
Upate of OCSP Responder Certificates	From Cisco ISE Release 3.1 Cumulative Patch 3 onwards, the following rules are applicable for the renewal of OCSP certificates: • For a multi-node Cisco ISE deployment, OCSP certificates are renewed automatically if you install the patch through the Cisco ISE GUI. If you install the patch through the Cisco ISE CLI, we recommend you to renew the OCSP certificate manually. • For a standalone Cisco ISE deployment, OCSP certificates are renewed automatically irrespective of whether you install the patch through the Cisco ISE GUI or the Cisco ISE CLI. • If you uninstall Patch 3, you have to renew the OCSP certificate manually. This one-time OCSP certificate renewal process is because of the change in certificate hierarchy. For more information, see Update of OCSP Responder Certificates in the "Basic Setup" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 3.1*.
Opening TAC Support Cases in Cisco ISE	You can now open TAC Support Cases for Cisco ISE and other Cisco products from the Cisco ISE GUI. For more information, see "Open TAC Support Cases in Cisco ISE" in the Chapter "Troubleshoot" in *Cisco ISE Administrator Guide, Release 3.1*.
SHA1 Ciphers Disabled by Default	From Cisco ISE Relase 3.1 Patch 2, SHA1 ciphers on port 443 are disabled by default. For more information, see "Configure Security Settings" in the Chapter "Segmentation" in *Cisco ISE Administrator Guide, Release 3.1*.
Cisco ISE Release 3.1 Patch 1	

Feature	Description
OpenAPI Service	The following OpenAPIs have been introduced in Cisco ISE Release 3.1 Cumulative Patch 1: • License • Generate Self-Signed Certificate • Patch and Hot Patch • Deployment For more information, see "Enable API Service" in the Chapter "Basic Setup" in *Cisco ISE Administrator Guide, Release 3.1*.
Signed SAML Authentication Request for Cisco ISE	Cisco ISE now only accepts signed SAML requests and assertions for authentication. For more information, see "Configure SAML ID Provider" in the Chapter "Asset Visibility" in *Cisco ISE Administrator Guide, Release 3.1*.
Cisco ISE Release 3.1	
MacOS Versions in Posture Policy Configurations	In Cisco ISE 3.0 and earlier, you could configure posture policies and requirements with minor MacOS versions such as MacOS 11.1, MacOS 11.2, and so on. In Cisco ISE 3.1, you can only choose major MacOS versions such as MacOS 11 (All) to configure posture policies and requirements. When you upgrade to Cisco ISE 3.1, any posture condition that includes a minor MacOS version is automatically updated to the corresponding major MacOS version. For example, a posture condition that was configured for MacOS 11.1 will be updated to MacOS 11 (All). For more information, see "Posture Types" in the Chapter "Compliance" in the *Cisco ISE Administrator Guide, Release 3.1*.

Feature	**Description**
Android Settings for Native Supplicant Profile	Android settings are added for native supplicant profile. You can select one of the following options for Certificate Enrollment Protocol: • Enrollment over Secure Transport (EST) • Simple Certificate Enrollment Protocol (SCEP) If you choose the EST protocol, Cisco ISE will ask for additional password inputs from Android users while issuing certificates. For more information, see "Native Supplicant Profile Settings" in the Chapter "Compliance" in the *Cisco ISE Administrator Guide, Release 3.1*.
Posture State Synchronization	You can configure AnyConnect to probe Cisco ISE at specified intervals when the posture status is not compliant. This helps prevent a client from being stuck in pending state. The posture state synchronization is supported for Windows, Linux, and MacOS clients. For more information, see "Posture State Synchronization" in the Chapter "Compliance" in the *Cisco ISE Administrator Guide, Release 3.1*.
Obtain Configuration Backup Using Cisco Support Diagnostics Connector	You can use Cisco Support Diagnostics Connector to trigger configuration backup and upload the backup files to the Cisco Support Diagnostics folder. After uploading the backup files to the Cisco Support Diagnostics folder, you can delete the backup files from the Cisco ISE local disk. To use this feature, you must enable smart licensing and Cisco Support Diagnostics in Cisco ISE. For more information, see "Obtain Configuration Backup Using Cisco Support Diagnostics Connector" in the Chapter "Troubleshoot" in the *Cisco ISE Administrator Guide, Release 3.1*.

Feature	Description
Configuration of Authorization Result Alarm	You can configure alarms based on the results of authorization policies. This allows you to monitor the impact of any networking, infrastructure, or application changes on endpoint authorizations. You can define the scope of your alarms by choosing specific Network Device Groups (NDGs). For each NDG you choose, a new Authorization Result alarm is created. You can filter the authorization logs to be monitored for an alarm by choosing specific authorization profiles and Security Group Tags (SGTs). Only endpoints that have met authorization policy sets with the specified authorization profiles and SGTs are monitored by the alarm. For more information, see "Configure Authorization Result Alarm" in the Chapter "Troubleshoot" in the *Cisco ISE Administrator Guide, Release 3.1*.
Configuration of Preferred Domain Controllers	You can specify the domain controllers that you want to use in case of domain failover. If a domain fails, Cisco ISE compares the priority scores of the domain controllers that are added to the preferred list and selects the one with the highest priority score. If that domain controller is offline or is not reachable because of an issue, the next one in the preferred list with the highest priority score is used. If all the domain controllers in the preferred list are down, a domain controller outside the list is selected based on the priority score. When the domain controller that was used before the failover is restored, Cisco ISE switches back to that domain controller. For more information, see "Configure Preferred Domain Controllers" in the Chapter "Asset Visibility" in the *Cisco ISE Administrator Guide, Release 3.1*.

Feature	Description
Context Visibility Enhancements	• In the **Export Endpoints** dialog box, you can now check the **Importable Only** check box if you want to export only the attributes that can be imported to Cisco ISE without any modification to the CSV file. Using this option prevents the need to modify the columns or metadata in the exported CSV file before importing it to Cisco ISE. • While using the **Quick Filter** or **Advanced Filter** option, you can use the **Export Filtered** option to export only the filtered endpoints. For more information, see "Export Endpoints Using CSV File" in the Chapter "Asset Visibility" in the *Cisco ISE Administrator Guide, Release 3.1*.
Virtual Appliance Licenses	Cisco ISE Release 3.1 and later supports the ISE VM license, which replaces the VM Small, VM Medium, and VM Large licenses that were supported in releases prior to Release 3.1. The new ISE VM license covers the Cisco ISE VM nodes in both on-premises and cloud deployments. For more information, see "Cisco ISE Licenses" in the Chapter "Licensing" in the *Cisco ISE Administrator Guide, Release 3.1*.
Download or Upload Files from Local Disk	You can easily add, download, or delete the files that are used for local disk management. For more information, see "Download and Upload Files from Local Disk" in the Chapter "Maintain and Monitor" in the *Cisco ISE Administrator Guide, Release 3.1*.

Feature	Description

OpenAPI Service	OpenAPIs are REST APIs based on HTTPS operating over port 443. From Cisco ISE 3.1 onwards, newer APIs are available in the OpenAPI format. For more information on Cisco ISE OpenAPIs, see https://<*ise-ip*>/api/swagger-ui/index.html.
	The following OpenAPIs have been introduced in Cisco ISE 3.1:
	• Repository Management
	• Configuration Data Backup and Restore
	• Certificate Management
	• Policy Management
	  • RADIUS Policy
	  • TACACS+ Policy
	For more information, see "Enable API Service" in the Chapter "Basic Setup" in *Cisco ISE Administrator Guide, Release 3.1*.

Feature	Description

Posture Support for Linux Operating System	Posture is a service in Cisco ISE that allows you to check the state of all the endpoints that are connecting to a network for compliance with corporate security policies. Cisco ISE 3.1 supports the following Linux operating system versions, in addition to Windows and Mac operating systems:
	• Ubuntu
	  • 18.04
	  • 20.04
	• Red Hat
	  • 7.5
	  • 7.9
	  • 8.1
	  • 8.2
	  • 8.3
	• SUSE
	  • 12.3
	  • 12.4
	  • 12.5
	  • 15.0
	  • 15.1
	  • 15.2
	The following posture conditions are supported for Linux operating system:
	• File Condition
	• Application Condition
	• Antimalware Condition
	• Patch Management Condition
	You can configure agent profiles for Linux clients. You can add client-provisioning resources for AnyConnect Linux clients.
	For more information, see the Chapter "Compliance" in *Cisco ISE Administrator Guide, Release 3.1*.

Feature	Description
ERS Service Auto Enabled on VMware Cloud Environment	The External RESTful Services (ERS) API service is enabled by default when the Amazon Machine Image (AMI) version of Cisco ISE is deployed on a VMware Cloud environment. This helps in easy integration of Cisco ISE with other Cisco products and third-party applications, without the need to enable the ERS service from the Cisco ISE GUI. For more information, see "Enable API Service" in the Chapter "Basic Setup" in the *Cisco ISE Administrator Guide, Release 3.1*.
Configuration of Maximum Password Attempts for Active Directory Account	You can configure the badPwdCount attribute to prevent Active Directory account lockout due to too many bad password attempts. Before authenticating the user, Cisco ISE compares the maximum bad password attempts configured in Cisco ISE with the current value of the badPwdCount attribute on Active Directory. When the maximum bad password attempts configured in Cisco ISE is equal to the value of the badPwdCount attribute, the authentication is dropped and not sent to Active Directory. For more information, see "Configure Maximum Password Attempts for AD Account" in the Chapter "Asset Visibility" in the *Cisco ISE Administrator Guide, Release 3.1*.
Handle Random and Changing MAC Addresses with Mobile Device Management Servers	As a privacy measure, mobile devices and some desktop operating systems increasingly use random and changing MAC addresses for each SSID that they connect to. In Cisco ISE, you can now work around this problem by configuring Cisco ISE to use a unique device identifier called GUID instead of MAC addresses. When an endpoint enrolls with a Mobile Device Management (MDM) server, the MDM server sends a certificate with a GUID value to the endpoint. The endpoint uses this certificate for authentication with Cisco ISE. Cisco ISE receives the GUID for the endpoint from the certificate. All communications between Cisco ISE and the MDM server now use the GUID to identify the endpoint, ensuring accuracy and consistency between the two systems. For more information, see "Handle Random and Changing MAC Addresses With Mobile Device Management Servers" in the Chapter "Secure Wired Access" in *Cisco ISE Administrator Guide, Release 3.1*

Feature	Description
MAC Randomization for BYOD	Android and iOS devices increasingly use random and changing MAC addresses for each SSID that they connect to. Cisco ISE and MDM systems see different MAC addresses for the same device depending on which SSID they use to connect to the service. Therefore, a unique identifier is generated by the Cisco ISE Provisioning service to identify these endpoints. For more information, see "MAC Randomization for BYOD" in the Chapter "Basic Setup" in *Cisco ISE Administrator Guide, Release 3.1*.
Posture Script Remediation	You can create and upload posture remediation scripts to Cisco ISE to resolve non-compliance issues in endpoints. For more information, see "Add a Script Remediation" in the Chapter "Compliance" in *Cisco ISE Administrator Guide, Release 3.1*.
SAML-Based Admin Login	SAML-based admin login adds a single sign on capability to Cisco ISE using the SAML 2.0 standard. You can use an external Identity Provider such as Okta or any Identity Provider that implements SAML 2.0. For more information, see "SAML-based Admin Login" in the Chapter "‘Asset Visibility" in *Cisco ISE Administrator Guide, Release 3.1*.
Specific License Reservation	Specific License Reservation is a smart licensing method that helps you manage your smart licensing when your organization's security requirements do not allow a persistent connection between Cisco ISE and the Cisco Smart Software Manager (CSSM). Specific License Reservation allows you to reserve specific license entitlements on a Cisco ISE node. You can create a Specific License Reservation by defining the type and number of licenses you need to reserve, and then activate the reservation on a Cisco ISE node. The Cisco ISE node on which you register and enable the reservation then tracks license usage and enforces license consumption compliance. For more information, see "Specific License Reservation" in the Chapter "Licensing" in *Cisco ISE Administrator Guide, Release 3.1*.

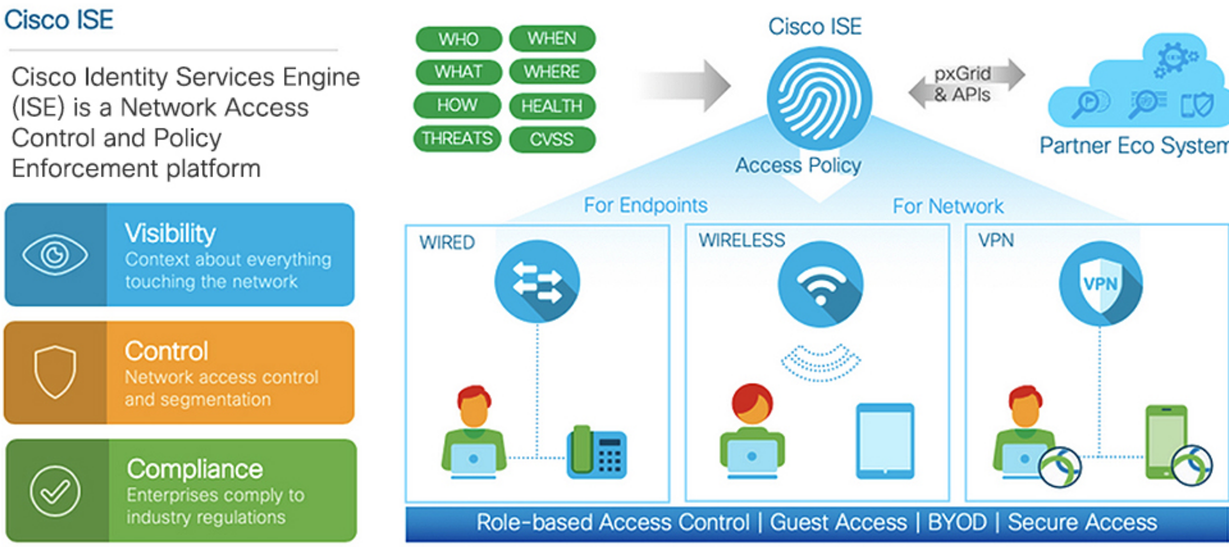
Feature	Description
Upgrade to pxGrid 2.0	From Cisco ISE Release 3.1, all pxGrid connections must be based on pxGrid 2.0. pxGrid 1.0-based (XMPP-based) integrations will cease to work on Cisco ISE from Release 3.1 onwards. pxGrid Version 2.0, which is based on WebSockets, was introduced in Cisco ISE Release 2.4. We recommend that you plan and upgrade your other systems to pxGrid 2.0-compliant versions in order to prevent potential disruptions, if any, to integrations. For more information, see the Chapter "pxGrid" in *Cisco ISE Administrator Guide, Release 3.1*.

CHAPTER 2

Overview of Cisco ISE

- Introduction to Cisco ISE, on page 13
- Cisco ISE Features, on page 14
- Cisco ISE Administrators, on page 15
- Cisco ISE Administrator Groups, on page 17
- Administrative Access to Cisco ISE, on page 25

Introduction to Cisco ISE



Cisco Identity Services Engine (ISE) is a Network Access Control and Policy Enforcement platform

Cisco ISE
Visibility
Context about everything touching the network
Control
Network access control and segmentation
Compliance
Enterprises comply to industry regulations
WHO
WHEN
WHAT
WHERE
HOW
HEALTH
THREATS
CVSS
Cisco ISE
pxGrid & APIs
Partner Eco System
Access Policy
For Endpoints
For Network
WIRED
WIRELESS
VPN
VPN
Role-based Access Control | Guest Access | BYOD | Secure Access

Cisco Identity Services Engine (ISE) is an identity-based network access control and policy enforcement system. It functions as a common policy engine that enables endpoint access control and network device administration for enterprises.

You can leverage Cisco ISE to ensure compliance, enhance infrastructure security, and streamline service operations.

A Cisco ISE administrator can gather real-time contextual data for a network, including users and user groups (who?), device type (what?), access time (when?), access location (where?), access type (wired, wireless, or VPN) (how?), and network threats and vulnerabilities.

As a Cisco ISE administrator, you can use this information to make network governance decisions. You can also tie identity data to various network elements to create policies that govern network access and usage.

Cisco ISE Features

Cisco ISE software must be installed as is. You cannot install any other third-party applications at the underlying operating system level.

Cisco ISE empowers you with the following capabilities:

- **Device Administration**: Cisco ISE uses the TACACS+ security protocol to control and audit the configuration of network devices. It facilitates granular control of who can access which network device and change the associated network settings. Network devices can be configured to query Cisco ISE for authentication and authorization of device administrator actions. These devices also send accounting messages to Cisco ISE to log such actions.
- **Guest and Secure Wireless**: Cisco ISE enables you to provide secure network access to visitors, contractors, consultants, and customers. You can use web-based and mobile portals to on-board guests to your company's network and internal resources. You can define access privileges for different types of guests, and assign sponsors to create and manage guest accounts.
- **Bring Your Own Device (BYOD)**: Cisco ISE allows your employees and guests to securely use their personal devices on your enterprise network. BYOD feature end users can use configured pathways to add their devices, and provision predefined authentications and levels of network access.
- **Asset Visibility**: Cisco ISE gives you visibility and control over who and what is on your network consistently, across wireless, wired, and VPN connections. Cisco ISE uses probes and device sensors to listen to the way devices connect to the network. The Cisco ISE profile database, which is extensive, then classifies the device. This gives the visibility and context you need to grant the right level of network access.
- **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods.
- **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation.
- **Posture or Compliance**: Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services.
- **Threat Containment**: If Cisco ISE detects threat or vulnerability attributes from an endpoint, adaptive network control policies are sent to dynamically change the access levels of the endpoint. After the threat or vulnerability is evaluated and addressed, the endpoint is given back its original access policy.
- **Security Ecosystem Integrations**: The pxGrid feature allows Cisco ISE to securely share context-sensitive information, policy and configuration data, and so on, with connected network devices, third-party vendors, or Cisco partner systems.

Cisco ISE Administrators

Administrators can use the admin portal to:

- Manage deployments, help desk operations, and network devices, and node monitoring and troubleshooting.
- Manage Cisco ISE services, policies, administrator accounts, and system configuration and operations.
- Change administrator and user passwords.

A CLI administrator can start and stop the Cisco ISE application, apply software patches and upgrades, reload or shut down the Cisco ISE appliance, and view all the system and application logs. Because of the special privileges that are granted to a CLI administrator, we recommend that you protect the CLI administrator credentials and create web-based administrators for configuring and managing Cisco ISE deployments.

The username and password that you configure during setup is intended only for administrative access to the CLI. This role is considered to be the CLI admin user, also known as CLI administrator. By default, the username for a CLI admin user is admin, and the password is defined during setup. There is no default password. This CLI admin user is the default admin user, and this user account cannot be deleted. However, other administrators can edit it, including options to enable, disable, or change password for the corresponding account.

You can either create an administrator, or promote an existing user to an administrator role. Administrators can also be demoted to simple network user status by disabling the corresponding administrative privileges.

Administrators are users who have local privileges to configure and operate the Cisco ISE system.

Administrators are assigned to one or more admin groups.

Note From Cisco ISE Release 2.7, use alphanumeric values while creating user accounts in Cisco ISE.

Related Topics

Cisco ISE Administrator Groups, on page 17

Force CLI Administrator to Use External Identity Store

Authentication with an external identity source is more secure than using the internal database.

Define a User's Attributes in the Active Directory User Directory

Using the Windows server running Active Directory, modify the attributes for each user that you plan to configure as a CLI Administrator.

1. From the **Server Manager** window, choose **Server Manager** > **Roles** > **Active Directory Domain Services** > **Active Directory Users and Computers > [ad.adserver] <*ad_server*>.local**.
2. Enable **Advanced Features** under the **View** menu so that you can edit a user's attributes.
3. Navigate to the Active Directory group that contains a list of all the admin users and select a user.
4. Double-click the corresponding user ID.

The **Properties** window is displayed.

5. Click the **Attribute Editor**.
6. Click any attribute and start entering **gid** to locate the *gidNumber*. If you don't find the gidNumber attribute, click the **Filter** button and uncheck the **Show only attributes that have values** check box.
7. Double-click an attribute name to edit each attribute. For each user:
    - Assign a *uidNumber* greater than 60000, and make sure that the number is unique. Do not change the uidNumber after assignment.
    - Assign *gidNumber* as 110 or 111. While 110 denotes an admin user, whereas 111 denotes a read-only user. If you modify the gidNumber, wait for at least five minutes before making an SSH connection.

Join the Admin CLI User to the Active Directory Domain

Connect to the Cisco ISE CLI, run the **identity-store** command, and assign the Admin user to the ID store. For example, to map the CLI admin user to the Active Directory defined in ISE as adpool1, run the **identity-store active-directory domain-name adpool1 user admincliuser** command.

After the join is complete, connect to the Cisco ISE CLI and log in as the Admin CLI user to verify your configuration.

If the domain you use in this command was previously joined to the ISE node, you must rejoin the domain in the Administrators console.

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources**.
2. In the left-hand pane, click **Active Directory** and select your Active Directory name.

Note If you test the connection, with the test user using either MS-RPC or Kerberos, the status for your Active Directory connection might show **Operational**, but error messages are displayed.

3. Verify that you can still log in to the Cisco ISE CLI as the Admin CLI user.

Create a New Administrator

Cisco ISE administrators need accounts with specific roles assigned to them in order to perform specific administrative tasks. You can create multiple administrator accounts and assign one or more roles to these admins based on the administrative tasks that these admins have to perform.

Use the **Admin Users** window to view, create, modify, delete, change the status, duplicate, or search for attributes of Cisco ISE administrators.

Note We recommend that you configure Active Directory access in the CLI before you join it in the GUI if the admin user's domain is the same in both the CLI and the GUI. Else, you must rejoin the domain from the GUI to avoid authentication failures to that domain.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Users** > **Add**.

Step 2 From the **Add** drop-down list, choose one of the following options:

- **Create an Admin User**

  If you choose **Create an Admin User**, a **New Administrator** window appears, from where you can configure account information for the new admin user.

- **Select from Network Access Users**

  If you choose **Select from Network Access Users**, a list of current users appears, from which you can choose a user. Subsequently, the **Admin User** window corresponding to this user appears.

Step 3 Enter values in the fields. The characters supported for the **Name** field are # $ ’ ( ) * + - . / @ _.

The admin user name must be unique. If you have entered an existing user name, an error pop-up window displays the following message:

```
User can't be created. A User with that name already exists.
```

Step 4 Click **Submit** to create a new administrator in the Cisco ISE internal database.

Related Topics

Read-Only Admin Policy, on page 155
Customize Menu Access for the Read-Only Administrator, on page 156

Cisco ISE Administrator Groups

Administrator groups are role-based access control (RBAC) groups in Cisco ISE. All the administrators who belong to the same group share a common identity and have the same privileges. An administrator’s identity as a member of a specific administrative group can be used as a condition in authorization policies. An administrator can belong to more than one administrator group.

Cisco ISE supports multiple external identity stores for enhanced user access management by admins.

An administrator account with any level of access can be used to modify or delete the objects for which it has permission, on any window it has access to.

The Cisco ISE security model limits administrators to create administrative groups that contain the same set of privileges that the administrator has. The privileges given are based on the administrative role of the user, as defined in the Cisco ISE database. Thus, administrative groups form the basis for defining privileges to access the Cisco ISE systems.

The following table lists the admin groups that are predefined in Cisco ISE, and the tasks that members from these groups can perform.

Table 2: Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions

Admin Group Role	Access Level	Permissions	Restrictions
Customization Admin	Manage sponsor, guest, and personal device portals.	• Configure guest and sponsor access. • Manage guest access settings. • Customize end-user web portals.	• Cannot perform any policy management, identity management, or system-level configuration tasks in Cisco ISE. • Cannot view any reports.
Helpdesk Admin	Query monitoring and troubleshooting operations	• Run all reports. • Run all troubleshooting flows. • View the Cisco ISE dashboard and live logs. • View alarms.	Cannot create, update, or delete reports, troubleshooting flows, live authentications, or alarms.
Identity Admin	• Manage user accounts and endpoints. • Manage identity sources.	• Add, edit, and delete user accounts and endpoints. • Add, edit, and delete identity sources. • Add, edit, and delete identity source sequences. • Configure general settings for user accounts (attributes and password policy). • View the Cisco ISE dashboard, live logs, alarms, and reports. • Run all troubleshooting flows.	Cannot perform any policy management or system-level configuration tasks in Cisco ISE.
MnT Admin	Perform all the monitoring and troubleshooting operations.	• Manage all the reports (run, create, and delete). • Run all the troubleshooting flows. • View the Cisco ISE dashboard and live logs. • Manage alarms (create, update, view, and delete).	Cannot perform any policy management, identity management, or system-level configuration tasks in Cisco ISE.

Admin Group Role	Access Level	Permissions	Restrictions
Network Device Admin	Manage Cisco ISE network devices and network device repository.	• Read and write permissions on network devices • Read and write permissions on Network Device Groups and all network resource object types. • View the Cisco ISE dashboard, live logs, alarms, and reports. • Run all the troubleshooting flows.	Cannot perform any policy management, identity management, or system-level configuration tasks in Cisco ISE.
Policy Admin	Create and manage policies for all the Cisco ISE services across the network, which are related to authentication, authorization, posture, profiler, client provisioning, and work centers.	• Read and write permissions on all the elements that are used in policies, such as authorization profiles, Network Device Groups (NDGs), and conditions. • Read and write permissions on identities, endpoints, and identity groups (user identity groups and endpoint identity groups). • Read and write permissions on services policies and settings. • View the Cisco ISE dashboard, live logs, alarms, and reports. • Run all the troubleshooting flows. • Device Administration: Access to device administration work centers. Permission for TACACS policy conditions and results. Network device permissions for TACACS proxy and proxy sequences.	Cannot perform any identity management or system-level configuration tasks in Cisco ISE. Device Administration: Access to the work center does not guarantee access to the subordinate links.

Admin Group Role	Access Level	Permissions	Restrictions
RBAC Admin	All the tasks under the **Operations** menu, except for Adaptive Network Control, and partial access to some menu items under **Administration**.	• View the authentication details. • Enable or disable Adaptive Network Control • Create, edit, and delete alarms; generate and view reports; and use Cisco ISE to troubleshoot problems in your network. • Read permissions on administrator account settings and admin group settings • View permissions on admin access and data access permissions in the **RBAC Policy** window. • View the Cisco ISE dashboard, live logs, alarms, and reports. • Run all the troubleshooting flows.	Cannot perform any identity management or system-level configuration tasks in Cisco ISE.

Admin Group Role	Access Level	Permissions	Restrictions
Read-Only Admin	Read-only access to the ISE GUI.	• View and use the functions of the dashboard, reports, and live logs or sessions, such as filtering data, querying, saving options, printing, and exporting data. • Change passwords of their own accounts. • Query ISE using global search, reports, and live logs or sessions. • Filter and save data based on the attributes. • Export data pertaining to authentication policies, profile policies, users, endpoints, network devices, network device groups, identities (including groups), and other configurations. • Customize report queries, save, print, and export them. • Generate custom report queries, save, print, or export the results. • Save GUI settings for future reference. • Download logs, such as ise-psc-log from the **Operations** > **Troubleshoot** > **Download Logs** window.	• Perform any configuration changes such as create, update, delete, import, quarantine, and Mobile Device Management (MDM) actions of objects, such as authorization policies, authentication policies, posture policies, profiler policies, endpoints, and users. • Perform system operations, such as backup and restore, registration or deregistration of nodes, synchronization of nodes, creating, editing, and deleting node groups, or upgrade and installation of patches. • Import data pertaining to policies, network devices, network device groups, identities (including groups), and other configurations. • Perform operations, such as CoA, endpoint debugging, modifying collection filters, bypassing suppression on live sessions data, modifying the PAN-HA failover settings, and editing the personas or services of Cisco ISE nodes. • Run commands that might have a heavy impact on performance. For example, access to the **TCP Dump** in the **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** window is restricted. • Generate support bundles.

Admin Group Role	Access Level	Permissions	Restrictions
Super Admin	All Cisco ISE administrative functions. The default administrator account belongs to this group.	Create, read, update, delete, and eXecute (CRUDX) permissions on all Cisco ISE resources. A super admin can modify the credentials of any Cisco ISE local user at any time. **Note** The super admin user cannot modify the default system-generated RBAC policies and permissions. To do this, you must create new RBAC policies with the necessary permissions based on your needs, and map these policies to an admin group. Device Administration: Access to device administration work centers. Permission for TACACS policy conditions and results. Network device permissions for TACACS proxy and proxy sequences. In addition, permission to enable TACACS global protocol settings.	• Device Administration: Access to the work center does not guarantee access to the subordinate links. • Only an admin user from the default Super Admin Group can modify or delete other admin users. Even an externally mapped user who is part of an Admin Group cloned with the Menu and Data Access privileges of the Super Admin Group cannot modify or delete an admin user.

Admin Group Role	Access Level	Permissions	Restrictions
System Admin	All Cisco ISE configuration and maintenance tasks.	Full access (read and write permissions) to perform all the activities under the **Operations** tab and partial access to some menu items under the **Administration** tab: • Read permissions on administrator account settings and administrator group settings. • Read permissions on admin access and data access permissions along with the **RBAC policy** window. • Read and write permissions for all options under **Administration** > **System**. • View authentication details. • Enable or disable Adaptive Network Control • Create, edit, and delete alarms; generate and view reports; and use Cisco ISE to troubleshoot problems in your network. • Device Administration: Permission to enable TACACS global protocol settings.	Cannot perform any policy management or system-level configuration tasks in Cisco ISE.
Elevated System Admin (available in Cisco ISE, Release 2.6, Patch 2 and above)	All Cisco ISE configuration and maintenance tasks.	In addition to all the privileges of the System Admin, an Elevated System Admin can create Admin users.	• Cannot create or delete Super Admin users. • Cannot manage the Super Admin groups.
External RESTful Services (ERS) Admin	Full access to all the ERS API requests such as GET, POST, DELETE, PUT	• Create, read, update, and delete ERS API requests.	The role is meant only for ERS authorization supporting internal users, identity groups, endpoints, endpoint groups, and SGT .
External RESTful Services (ERS) Operator	Read-only access to ERS API, only GET	• Can only read ERS API requests	The role is meant only for ERS authorization supporting internal users, identity groups, endpoints, endpoint groups, and SGT.

Admin Group Role	Access Level	Permissions	Restrictions
TACACS+ Admin	Full access	Access to: • Device Administration Work Center. • Deployment: To enable TACACS+ services. • External ID stores. • **Operations** > **TACACS Live Logs** window.	—

Related Topics

Cisco ISE Administrators, on page 15

Create an Admin Group

The **Admin Groups** window allows you to view, create, modify, delete, duplicate, or filter Cisco ISE network admin groups.

Before you begin

To configure an external administrator group type, you must have already specified one or more external identity stores.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Groups**

Step 2 Click **Add**, and enter a name and description.

The supported special characters for the **Name** field are: space, # $ & ‘ ( ) * + - . / @ _ .

Step 3 Check the corresponding check box to specify the **Type** of administrator group you are configuring:

- **Internal**: Administrators assigned to this group type authenticate against the credentials that are stored in the Cisco ISE internal database.
- **External**: Administrators assigned to this group authenticate against the credentials stored in the external identity store that you select in the **Administration > System > Admin Access > Authentication > Authentication Method** window. You can specify the external groups, if required.

Note If an internal user is configured with an external identity store for authentication, while logging in to the ISE Admin portal, the internal user must select the external identity store as the **Identity Source**. Authentication will fail if **Internal Identity Source** is selected.

Step 4 Click **Add** in the **Member Users** area to add users to this admin group. To delete users from the admin group, check the check box corresponding to the user that you want to delete, and click **Remove**.

Step 5 Click **Submit**.

Administrative Access to Cisco ISE

Cisco ISE administrators can perform various administrative tasks based on the administrative group to which they belong. These administrative tasks are critical. Grant administrative access only to users who are authorized to administer Cisco ISE in your network.

Note When a Cisco ISE server is added to a network, it is marked to be in Running state after its web interface comes up. However, it might take some more time for all the services to be fully operational because some advanced services, such as posture services, might take longer to be available.

Administrative Access Methods

You can connect to the Cisco ISE servers in several ways. The policy administration node (PAN) runs the Administrators portal. An admin password is required to log in. Other ISE persona servers are accessible through SSH or the console, from where you run the CLI. This section describes the process and password options available for each connection type:

- **Admin password**: The Cisco ISE Admin user that you created during installation, times out in 45 days by default. You can prevent that by turning off **Password Lifetime** from **Administration** > **System** > **Admin Settings**. Click the **Password Policy** tab, and uncheck the**Administrative passwords expire** check box under **Password Lifetime**.

  If you do not do this, and the password expires, you can reset the admin password in the CLI by running the **application reset-passwd** command. You can reset the admin password by connecting to the console to access the CLI, or by rebooting the ISE image file to access the boot options menu.

- **CLI password**: You must enter a CLI password during installation. If you have a problem logging in to the CLI because of an invalid password, you can reset the CLI password. Connect to the console and run the **password** CLI command to rest the password. See the Cisco Identity Services Engine CLI Reference Guide for more information.

- **SSH access to the CLI**: You can enable SSH access either during installation or after, using the **service sshd** command. You can also force SSH connections to use a key. Note that when you do this, SSH connections to all the network devices also use that key. For more information, see SSH Key Validation, on page 1113. You can force the SSH key to use the Diffie-Hellman algorithm. Note that ECDSA keys are not supported for SSH keys.

Role-Based Admin Access Control in Cisco ISE

Cisco ISE provides role-based access control (RBAC) policies that ensure security by restricting administrative privileges. RBAC policies are associated with default admin groups to define roles and permissions. A standard set of permissions (for menu as well as data access) is paired with each of the predefined admin groups, and is thereby aligned with the associated role and job function.

Some features in the user interface require certain permissions for their use. If a feature is unavailable, or you are not allowed to perform a specific task, your admin group may not have the necessary permissions to perform the task that utilizes the feature.

Regardless of the level of access, any administrator account can modify or delete objects for which it has permission, on any window that it can access.

Note Only system-defined admin users with Super Admin or Read Only Admin permissions can see the identity-based users who are not a part of a user group. Admins you create without these permissions cannot see these users.

Role-Based Permissions

Cisco ISE allows you to configure permissions at the menu and data levels. These are called menu access and data access permissions.

The menu access permissions allow you to show or hide the menu and submenu items of the Cisco ISE administrative interface. This feature lets you create permissions so that you can restrict or enable access at the menu level.

The data access permissions allow you to grant read and write, read only, or no access to the Admin Groups, User Identity Groups, Endpoint Identity Groups, Locations, and Device Types data in the Cisco ISE interface.

RBAC Policies

RBAC policies determine if an administrator can be granted a specific type of access to a menu item or other identity group data elements. You can grant or deny access to a menu item or identity group data element to an administrator based on the admin group, by using RBAC policies. When administrators log in to the Admin portal, they can access menus and data that are based on the policies and permissions defined for the admin groups with which they are associated.

RBAC policies map admin groups to menu access and data access permissions. For example, you can prevent a network administrator from viewing the Admin Access operations menu and the policy data elements. This can be achieved by creating a custom RBAC policy for the admin group with which that network administrator is associated.

Note If you are using customized RBAC policies for admin access, ensure that you provide all the relevant menu access for a given data access. For example, to add or delete endpoints with data access of Identity or Policy Admin, you must provide menu access to **Work Center > Network Access** and **Administration > Identity Management**.

Default Menu Access Permissions

Cisco ISE provides an out-of-the-box set of permissions that are associated with a set of predefined admin groups. Having predefined admin group permissions allow you to set permissions so that a member of any admin group can have full or limited access to the menu items within the administrative interface (known as menu access) and to delegate an admin group to use the data access elements of other admin groups (known as data access). These permissions are reusable entities that can be further used to formulate RBAC policies for various admin groups. Cisco ISE provides a set of system-defined menu access permissions that are already used in the default RBAC policies. Apart from the predefined menu access permissions, Cisco ISE also allows you to create custom menu access permissions that you can use in RBAC policies. The key icon represents menu access privileges for the menus and submenus, and the key with a close icon represents no access for different RBAC groups.

Note For a Super Admin user, all the menu items are available. For other admin users, all the menu items in the **Menu Access Privileges** column are available for standalone deployment, and primary node in a distributed deployment. For secondary nodes in a distributed deployment, the menu items under the **Administration** tab are not available.

Table 3: Default Menu Access Permissions for Different Admin Groups

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Home	√	√	√	√	√	√	√	√	x	x
Home > Introduction	√	√	√	√	√	√	√	√	x	x
Home > Dashboard	√	√	√	√	√	√	√	√	x	x
Context Visibility	√	√	√	√	√	√	√	√	x	x
Context Visibility > Endpoints	√	√	√	√	√	√	√	√	x	x
Context Visibility > Users	√	√	√	√	√	√	√	√	x	x
Context Visibility > Network Devices	√	√	√	√	√	√	√	√	x	x
Context Visibility > Application	√	√	√	√	√	√	√	√	x	x
Operations	√	√	√	√	√	√	√	√	x	√
Operations > Adaptive Network Control	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Operations > Adaptive Network Control > Policy List	√	√	x	x	x	x	x	x	x	x
Operations > Adaptive Network Control > Endpoint Assignment	√	√	x	x	x	x	x	x	x	x
Operations > Reports	√	√	√	√	√	√	√	√	x	x
Operations > RADIUS	√	√	√	√	√	√	√	√	x	x
Operations > RADIUS > Live Logs	√	√	√	√	√	√	√	√	x	x
Operations > RADIUS > Live Sessions	√	√	√	√	√	√	√	√	x	x
Operations > Threat-Centric NAC Live Logs	√	√	√	√	√	√	√	√	x	x
Operations > TACACS	√	√	√	√	√	√	√	√	x	√

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Operations > TACACS > Live Logs	√	√	√	√	√	√	√	√	x	√
Operations > Troubleshoot	√	√	√	√	√	√	√	√	x	x
Operations > Troubleshoot > Download Logs	√	x	x	x	x	x	x	x	x	x
Operations > Troubleshoot > Diagnostic Tools	√	√	√	√	√	√	√	√	x	x
Operations > Troubleshoot > Diagnostic Tools > General Tools	√	√	√	√	√	√	√	√	x	x
Operations > Troubleshoot > Diagnostic Tools > General Tools > RADIUS Authentication Troubleshooting	√	√	√	√	√	√	√	√	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Operations > Troubleshoot > Diagnostic Tools > General Tools > Execute Network Device Command	√	√	√	√	√	√	√	√	x	x
Operations > Troubleshoot > Diagnostic Tools > General Tools > Evaluate Configuration Validator	√	√	√	√	√	√	√	√	x	x
Operations > Troubleshoot > Diagnostic Tools > General Tools > Posture Troubleshooting	√	√	√	√	√	√	√	√	x	x
Operations > Troubleshoot > Diagnostic Tools > General Tools > Agentless Posture Troubleshooting	√	√	√	√	√	√	√	√	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Operations > Troubleshoot > Diagnostic Tools > General Tools > EndPoint Debug	√	x	x	x	x	x	x	x	x	x
Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump	√	x	x	x	x	x	x	x	x	x
Operations > Troubleshoot > Diagnostic Tools > General Tools > Session Trace Tests	√	√	√	√	√	√	√	√	x	x
Operations > Troubleshoot > Diagnostic Tools > Security Group Access Tools	√	√	√	√	√	√	√	√	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Operations > Troubleshoot > Diagnostic Tools > Security Group Access Tools > SXP-IP Mappings	√	√	√	√	√	√	√	√	x	x
Operations > Troubleshoot > Diagnostic Tools > Security Group Access Tools > IP User SGT	√	√	√	√	√	√	√	√	x	x
Operations > Troubleshoot > Diagnostic Tools > Security Group Access Tools > Egress (SGACL) Policy	√	√	√	√	√	√	√	√	x	x

Menus and Submenus	**Super Admin Menu Access**	**Policy Admin Menu Access**	**Helpdesk Admin Menu Access**	**Identity Admin Menu Access**	**Network Admin Menu Access**	**System Admin Menu Access**	**RBAC Admin Menu Access**	**MnT Admin Menu Access**	**Customization Admin Menu Access**	**TACACS+ Admin Menu Access**
Operations > Troubleshoot > Diagnostic Tools > Security Group Access Tools > Device SGT	√	√	√	√	√	√	√	√	x	x
Operations > Troubleshoot > Debug Wizard	√	√	√	√	√	√	√	√	x	x
Operations > Troubleshoot > Debug Wizard > Debug Log Configuration	√	√	√	√	√	√	√	√	x	x
Operations > Troubleshoot > Debug Wizard > Debug Profile Configuration	√	√	√	√	√	√	√	√	x	x
Policy	√	√	x	x	x	x	x	x	x	x
Policy > Policy Sets	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Policy > Policy Elements > Dictionaries	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Library Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Library Conditions > Simple Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Smart Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Authorization	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Policy > Policy Elements > Conditions > Authorization > Simple Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Authorization > Compound Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Time and Date	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Posture	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Posture > AntiSpyware Conditions	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Policy > Policy Elements > Conditions > Posture > Application Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Posture > Dictionary Compound Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Posture > Dictionary Simple Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Posture > Disk Encryption Conditions	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Policy > Policy Elements > Conditions > Posture > External DataSource Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Posture > File Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Posture > Firewall Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Posture > Hardware Attributes Conditions	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Policy > Policy Elements > Conditions > Posture > Patch Management Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Posture > Registry Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Posture > Service Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Posture > USB Conditions	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Policy > Policy Elements > Conditions > Posture > Anti-Malware Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Posture > Anti-Virus Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Posture > Compound Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Network Conditions	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Policy > Policy Elements > Conditions > Network Conditions > Endstation Network Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Network Conditions > Device Port Network Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Network Conditions > Device Network Conditions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Conditions > Profiling	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Policy > Policy Elements > Results	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Results > Authentication	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Results > Authentication > Allowed Protocols	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Results > Authorization	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Results > Authorization > Authorization Profiles	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Policy > Policy Elements > Results > Authorization > Downloadable ACLs	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Results > Profiling	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Results > Profiling > Exception Actions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Results > Profiling > Network Scan (NMAP) Actions	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Policy > Policy Elements > Results > Posture	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Results > Posture > Requirements	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Results > Posture > Remediation Actions	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Results > Posture > Remediation Actions > AntiMalware Remediation	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Policy > Policy Elements > Results > Posture > Remediation Actions > Anti-Virus Remediation	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Results > Posture > Remediation Actions > Firewall Remediation	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Results > Posture > Remediation Actions > Link Remediation	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Policy > Policy Elements > Results > Posture > Remediation Actions > Script Remediation	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Results > Posture > Remediation Actions > USB Remediation	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Results > Posture > Remediation Actions > Windows Update Remediation	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Policy > Policy Elements > Results > Posture > Remediation Actions > Application Remediation	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Results > Posture > Remediation Actions > AntiSpyware Remediation	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Results > Posture > Remediation Actions > File Remediation	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Policy > Policy Elements > Results > Posture > Remediation Actions > Launch Program Remediation	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Results > Posture > Remediation Actions > Patch Management Remediation	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Results > Posture > Remediation Actions > Windows Server Update Services Remediation	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Policy > Policy Elements > Results > Client Provisioning	√	√	x	x	x	x	x	x	x	x
Policy > Policy Elements > Results > Client Provisioning > Resources	√	√	x	x	x	x	x	x	x	x
Policy > Policy Sets	√	√	x	x	x	x	x	x	x	x
Policy > Authentication	√	√	x	x	x	x	x	x	x	x
Policy > Authorization	√	√	x	x	x	x	x	x	x	x
Policy > Profiling	√	√	x	x	x	x	x	x	x	x
Policy > Posture	√	√	x	x	x	x	x	x	x	x
Policy > Client Provisioning	√	√	x	x	x	x	x	x	x	x
Administration	√	√	x	√	√	√	√	x	√	√
Administration > Identity Management	√	√	x	√	x	x	x	x	x	√

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > Identity Management > Identities	√	√	x	√	x	x	x	x	x	x
Administration > Identity Management > Identities > Users	√	√	x	√	x	x	x	x	x	x
Administration > Identity Management > Identities > Latest Manual Network Scan Results	√	√	x	√	x	x	x	x	x	x
Administration > Identity Management > Groups	√	√	x	√	x	x	x	x	x	x
Administration > Identity Management > External Identity Sources	√	√	x	√	x	x	x	x	x	√

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > Identity Management > Identity Source Sequences	√	√	x	√	x	x	x	x	x	x
Administration > Identity Management > Settings	√	√	x	√	x	x	x	x	x	x
Administration > Identity Management > Settings > User Custom Attributes	√	√	x	√	x	x	x	x	x	x
Administration > Identity Management > Settings > Endpoint Purge	√	√	x	√	x	x	x	x	x	x
Administration > Identity Management > Settings > User Authentication Settings	√	√	x	√	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > Identity Management > Settings > Endpoint Custom Attributes	√	√	x	√	x	x	x	x	x	x
Administration > Identity Management > Settings > REST ID Store Settings	√	√	x	√	x	x	x	x	x	x
Administration > Device Portal Management	√	√	x	x	x	x	x	x	√	x
Administration > Device Portal Management > BYOD	√	√	x	x	x	x	x	x	√	x
Administration > Device Portal Management > Client Provisioning	√	√	x	x	x	x	x	x	√	x
Administration > Device Portal Management > My Devices	√	√	x	x	x	x	x	x	√	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > Device Portal Management > Blocked List	√	√	x	x	x	x	x	x	√	x
Administration > Device Portal Management > Certificate Provisioning	√	x	x	x	x	x	x	x	x	x
Administration > Device Portal Management > Mobile Device Management	√	√	x	x	x	x	x	x	√	x
Administration > Device Portal Management > Custom Portal Files	√	x	x	x	x	x	x	x	x	x
Administration > Device Portal Management > Settings	√	√	x	x	x	x	x	x	√	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > Device Portal Management > Settings > Retry URL	√	√	x	x	x	x	x	x	√	x
Administration > Device Portal Management > Settings > Employee Registered Devices	√	√	x	x	x	x	x	x	√	x
Administration > Network Resources	√	x	x	x	√	x	x	x	x	x
Administration > Network Resources > Network Devices	√	x	x	x	√	x	x	x	x	x
Administration > Network Resources > Network Devices > Default Device	√	x	x	x	√	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > Network Resources > Network Devices > Network Devices	√	x	x	x	√	x	x	x	x	x
Administration > Network Resources > Network Devices > Device Security Settings	√	x	x	x	√	x	x	x	x	x
Administration > Network Resources > Network Device Groups	√	x	x	x	√	x	x	x	x	x
Administration > Network Resources > External RADIUS Servers	√	x	x	x	√	x	x	x	x	x
Administration > Network Resources > NAC Managers	√	x	x	x	√	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > Network Resources > Location Services	√	x	x	x	√	x	x	x	x	x
Administration > Network Resources > Location Services > Location Servers	√	x	x	x	√	x	x	x	x	x
Administration > Network Resources > Location Services > Location Tree	√	x	x	x	√	x	x	x	x	x
Administration > Network Resources > Network Device Profiles	√	x	x	x	√	x	x	x	x	x
Administration > Network Resources > RADIUS Server Sequences	√	x	x	x	√	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > Network Resources > External MDM	√	x	x	x	x	x	x	x	x	x
Administration > pxGrid Services	√	x	x	x	x	√	x	x	x	x
Administration > pxGrid Services > Summary	√	x	x	x	x	√	x	x	x	x
Administration > pxGrid Services > Client Management	√	x	x	x	x	√	x	x	x	x
Administration > pxGrid Services > Client Management > Clients	√	x	x	x	x	√	x	x	x	x
Administration > pxGrid Services > Client Management > Policy	√	x	x	x	x	√	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > pxGrid Services > Client Management > Groups	√	x	x	x	x	√	x	x	x	x
Administration > pxGrid Services > Client Management > Certificates	√	x	x	x	x	√	x	x	x	x
Administration > pxGrid Services > Client Management > pxCloud Connection	√	x	x	x	x	√	x	x	x	x
Administration > pxGrid Services > Client Management > pxCloud Policy	√	x	x	x	x	√	x	x	x	x
Administration > pxGrid Services > Diagnostics	√	x	x	x	x	√	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > pxGrid Services > Diagnostics > WebSocket	√	x	x	x	x	√	x	x	x	x
Administration > pxGrid Services > Diagnostics > Log	√	x	x	x	x	√	x	x	x	x
Administration > pxGrid Services > Diagnostics > Tests	√	x	x	x	x	√	x	x	x	x
Administration > pxGrid Services > Settings	√	x	x	x	x	√	x	x	x	x
Administration > System	√	√	x	x	x	√	√	x	x	√
Administration > System > Backup & Restore	√	x	x	x	x	√	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > System > Backup & Restore > Policy Export	√	x	x	x	x	√	x	x	x	x
Administration > System > Backup & Restore > Backup & Restore	√	x	x	x	x	√	x	x	x	x
Administration > System > Admin Access	√	x	x	x	x	√	√	x	x	x
Administration > System > Admin Access > Administrators	√	x	x	x	x	√	√	x	x	x
Administration > System > Admin Access > Administrators > Admin Users	√	x	x	x	x	√	√	x	x	x
Administration > System > Admin Access > Administrators > Admin Groups	√	x	x	x	x	√	√	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > System > Admin Access > Authentication	√	x	x	x	x	√	√	x	x	x
Administration > System > Admin Access > Authorization	√	x	x	x	x	√	√	x	x	x
Administration > System > Admin Access > Authorization > Permissions	√	x	x	x	x	√	√	x	x	x
Administration > System > Admin Access > Authorization > Permissions > Menu Access	√	x	x	x	x	√	√	x	x	x
Administration > System > Admin Access > Authorization > Permissions > Data Access	√	x	x	x	x	√	√	x	x	x
Administration > System > Admin Access > Authorization > Policy	√	x	x	x	x	√	√	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > System > Admin Access > Settings	√	x	x	x	x	√	x	x	x	x
Administration > System > Admin Access > Settings > Access	√	x	x	x	x	√	x	x	x	x
Administration > System > Admin Access > Settings > Session	√	x	x	x	x	√	x	x	x	x
Administration > System > Admin Access > Settings > Portal Customization	√	x	x	x	x	x	x	x	x	x
Administration > System > Settings	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Max Sessions	√	√	x	x	x	√	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > System > Settings > Interactive User Guide	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > DHCP & DNS Services	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Light Session Directory	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Protocols	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Protocols > EAP-FAST	√	√	x	x	x	√	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > System > Settings > Protocols > EAP-FAST > EAP FAST Settings	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Protocols > EAP-FAST > Generate PAC	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Protocols > EAP-TTLS	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Protocols > EAP-TLS	√	√	x	x	x	√	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > System > Settings > Protocols > PEAP	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Protocols > IPSec	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Protocols > RADIUS	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Network Success Diagnostics	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Network Success Diagnostics > Telemetry	√	√	x	x	x	√	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > System > Settings > Network Success Diagnostics > Cisco Support Diagnostics	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Client Provisioning	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > FIPS Mode	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Security Settings	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Proxy	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > SMTP Server	√	√	x	x	x	√	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > System > Settings > SMS Gateway	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > System Time(Primary Node)	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Alarm Settings	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Posture	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Posture > Updates	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Posture > General Settings	√	√	x	x	x	√	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > System > Settings > Posture > Reassessments	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Posture > Acceptable Use Policy	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Profiling	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Endpoint Scripts	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > Endpoint Scripts > Login Configuration	√	√	x	x	x	√	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > System > Settings > Endpoint Scripts > Settings	√	√	x	x	x	√	x	x	x	x
Administration > System > Settings > API Gateway Settings	√	√	x	x	x	√	x	x	x	x
Administration > System > Deployment	√	x	x	x	x	√	x	x	x	√
Administration > System > Licensing	√	x	x	x	x	√	x	x	x	x
Administration > System > Upgrade	√	x	x	x	x	x	x	x	x	x
Administration > System > Health Checks	√	x	x	x	x	x	x	x	x	x
Administration > System > Certificates	√	x	x	x	x	√	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > System > Certificates > Certificate Management	√	x	x	x	x	√	x	x	x	x
Administration > System > Certificates > Certificate Management > Trusted Certificates	√	x	x	x	x	√	x	x	x	x
Administration > System > Certificates > Certificate Management > Certificate Signing Requests	√	x	x	x	x	√	x	x	x	x
Administration > System > Certificates > Certificate Management > System Certificates	√	x	x	x	x	√	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > System > Certificates > Certificate Management > OCSP Client Profile	√	x	x	x	x	√	x	x	x	x
Administration > System > Certificates > Certificate Management > Certificate Periodic Check Settings	√	x	x	x	x	√	x	x	x	x
Administration > System > Certificates > Certificate Authority	√	x	x	x	x	√	x	x	x	x
Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates	√	x	x	x	x	√	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > System > Certificates > Certificate Authority > Overview	√	x	x	x	x	√	x	x	x	x
Administration > System > Certificates > Certificate Authority > Issued Certificates	√	x	x	x	x	√	x	x	x	x
Administration > System > Certificates > Certificate Authority > Internal CA Settings	√	x	x	x	x	√	x	x	x	x
Administration > System > Certificates > Certificate Authority > Certificate Templates	√	x	x	x	x	√	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > System > Certificates > Certificate Authority > External CA Settings	√	x	x	x	x	√	x	x	x	x
Administration > System > Logging	√	x	x	x	x	√	x	x	x	x
Administration > System > Logging > Logging Categories	√	x	x	x	x	√	x	x	x	x
Administration > System > Logging > Collection Filters	√	x	x	x	x	√	x	x	x	x
Administration > System > Logging > Log Settings	√	x	x	x	x	√	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > System > Logging > Remote Logging Targets	√	x	x	x	x	√	x	x	x	x
Administration > System > Logging > Message Catalog	√	x	x	x	x	√	x	x	x	x
Administration > System > Maintenance	√	x	x	x	x	√	x	x	x	x
Administration > System > Maintenance > Repository	√	x	x	x	x	√	x	x	x	x
Administration > System > Maintenance > Localdisk Management	√	x	x	x	x	√	x	x	x	x
Administration > System > Maintenance > Patch Management	√	x	x	x	x	√	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > System > Maintenance > Operational Data Purging	√	x	x	x	x	√	x	x	x	x
Administration > System > Session Info	√	x	x	x	x	x	x	x	x	x
Administration > System > System Time(Secondary Node)	√	√	x	x	x	√	x	x	x	x
Administration > System > Server Certificate	√	x	x	x	x	√	x	x	x	x
Administration > System > Certificate Signing Requests	√	x	x	x	x	√	x	x	x	x
Administration > Feed Service	√	√	x	x	x	√	x	x	x	x
Administration > Feed Service > Profiler	√	√	x	x	x	√	x	x	x	x
Administration > Threat Centric NAC	√	x	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Administration > Threat Centric NAC > Third Party Vendors	√	x	x	x	x	x	x	x	x	x
Work Centers	√	√	√	√	√	√	√	√	√	√
Work Centers > TrustSec	√	√	√	√	√	√	√	√	x	x
Work Centers > TrustSec > Components	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > Components > IP SGT Static Mapping	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > Components > Network Devices	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > TrustSec > Components > Security Groups	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > Components > Security Group ACLs	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > Components > Trustsec Servers	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > Components > Trustsec Servers > AAA Servers	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > TrustSec > Components > Trustsec Servers > HTTPS Servers	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > TrustSec Policy	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > TrustSec Policy > Egress Policy	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > TrustSec Policy > Egress Policy > Matrix	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > TrustSec > TrustSec Policy > Egress Policy > Destination Tree	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > TrustSec Policy > Egress Policy > Matrices List	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > TrustSec Policy > Egress Policy > Source Tree	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > TrustSec Policy > Network Device Authorization	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > TrustSec > Policy Sets	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > Authorization Policy	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > SXP	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > SXP > SXP Devices	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > SXP > All SXP Mappings	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > ACI	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > TrustSec > Reports	√	√	√	√	√	√	√	√	x	x
Work Centers > TrustSec > Overview	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > Overview > Introduction	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > Overview > Dashboard	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > Policy Sets	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > Policy Sets	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > TrustSec > Authentication Policy	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > Troubleshoot	√	√	√	√	√	√	√	√	x	x
Work Centers > TrustSec > Troubleshoot > Egress (SGACL) Policy	√	√	√	√	√	√	√	√	x	x
Work Centers > TrustSec > Troubleshoot > IP User SGT	√	√	√	√	√	√	√	√	x	x
Work Centers > TrustSec > Troubleshoot > SXP-IP Mappings	√	√	√	√	√	√	√	√	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > TrustSec > Troubleshoot > Device SGT	√	√	√	√	√	√	√	√	x	x
Work Centers > TrustSec > Settings	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > Settings > General TrustSec Settings	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > Settings > Work Process Settings	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > Settings > ACI Settings	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > TrustSec > Settings > TrustSec Matrix Settings	√	√	x	x	x	x	x	x	x	x
Work Centers > TrustSec > Settings > SXP Settings	√	√	x	x	x	x	x	x	x	x
Work Centers > Profiler	√	√	√	√	√	√	√	√	x	x
Work Centers > Profiler > Ext Id Sources	√	√	x	√	x	x	x	x	x	x
Work Centers > Profiler > Endpoint Classification	√	√	x	x	x	x	x	x	x	x
Work Centers > Profiler > Node Config	√	√	x	x	x	√	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Profiler > Manual Scans	√	√	x	x	x	x	x	x	x	x
Work Centers > Profiler > Manual Scans > Manual NMAP Scan Results	√	√	x	x	x	x	x	x	x	x
Work Centers > Profiler > Manual Scans > Manual NMAP Scan	√	√	x	x	x	x	x	x	x	x
Work Centers > Profiler > Policy Sets	√	√	x	x	x	x	x	x	x	x
Work Centers > Profiler > Authorization Policy	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Profiler > Reports	√	√	√	√	√	√	√	√	x	x
Work Centers > Profiler > Feeds	√	√	x	x	x	x	x	x	x	x
Work Centers > Profiler > Policy Elements	√	√	x	x	x	x	x	x	x	x
Work Centers > Profiler > Policy Elements > Profiler Conditions	√	√	x	x	x	x	x	x	x	x
Work Centers > Profiler > Policy Elements > NMAP Scan Actions	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Profiler > Policy Elements > Exception Actions	√	√	x	x	x	x	x	x	x	x
Work Centers > Profiler > Profiling Policies	√	√	x	x	x	x	x	x	x	x
Work Centers > Profiler > Policy Sets	√	√	x	x	x	x	x	x	x	x
Work Centers > Profiler > Troubleshoot	√	√	√	√	√	√	√	√	x	x
Work Centers > Profiler > Troubleshoot > Execute Network Device Command	√	√	√	√	√	√	√	√	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Profiler > Troubleshoot > EndPoint Debug	√	x	x	x	x	x	x	x	x	x
Work Centers > Profiler > Troubleshoot > Evaluate Configuration Validator	√	√	√	√	√	√	√	√	x	x
Work Centers > Profiler > Troubleshoot > TCP Dump	√	x	x	x	x	x	x	x	x	x
Work Centers > Profiler > Settings	√	√	x	x	x	x	x	x	x	x
Work Centers > Profiler > Settings > Profiler Settings	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Profiler > Settings > NMAP Scan Subnet Exclusions	√	√	x	x	x	x	x	x	x	x
Work Centers > Profiler > Dictionaries	√	√	x	x	x	x	x	x	x	x
Work Centers > Profiler > Overview	√	√	x	x	x	x	x	x	x	x
Work Centers > Profiler > Network Devices	√	√	x	x	√	x	x	x	x	x
Work Centers > Posture	√	√	√	√	√	√	√	√	√	x
Work Centers > Posture > Network Devices	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Posture > Posture Policy	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Sets	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Authorization Policy	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Reports	√	√	√	√	√	√	√	√	x	x
Work Centers > Posture > Settings	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Settings > Posture General Settings	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Posture > Settings > Acceptable Use Policy	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Settings > Software Updates	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Settings > Software Updates > Client Provisioning	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Settings > Software Updates > Posture Updates	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Posture > Settings > Software Updates > Proxy Settings	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Settings > Reassessment configurations	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Overview	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Client Provisioning	√	√	x	x	x	x	x	x	√	x
Work Centers > Posture > Client Provisioning > Client Provisioning Policy	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Posture > Client Provisioning > Client Provisioning Portal	√	√	x	x	x	x	x	x	√	x
Work Centers > Posture > Client Provisioning > Resources	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Conditions	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Conditions > Anti-Spyware	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Posture > Policy Elements > Conditions > Application	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Conditions > Compound	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Conditions > Dictionary Compound	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Conditions > File	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Posture > Policy Elements > Conditions > Registry	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Conditions > AntiMalware	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Conditions > Anti-Virus	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Conditions > Dictionary Simple	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Posture > Policy Elements > Conditions > Disk Encryption	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Conditions > External DataSource	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Conditions > Firewall Condition	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Conditions > Hardware Attributes Condition	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Posture > Policy Elements > Conditions > Patch Management	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Conditions > Service	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Conditions > USB	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Requirements	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Posture > Policy Elements > Remediations	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Remediations > Anti-Virus	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Remediations > Firewall	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Remediations > Link	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Posture > Policy Elements > Remediations > Script	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Remediations > Windows Server Update Services	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Remediations > AntiMalware	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Remediations > AntiSpyware	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Posture > Policy Elements > Remediations > File	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Remediations > Launch Program	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Remediations > Patch Management	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Remediations > USB	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Posture > Policy Elements > Remediations > Windows Update	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Elements > Authorization Profiles	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Policy Sets	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Authentication Policy	√	√	x	x	x	x	x	x	x	x
Work Centers > Posture > Troubleshoot	√	√	√	√	√	√	√	√	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Posture > Troubleshoot > Agentless Posture Troubleshooting	√	√	√	√	√	√	√	√	x	x
Work Centers > Device Administration	√	√	√	√	√	√	√	√	x	√
Work Centers > Device Administration > Overview	√	√	x	x	x	x	x	x	x	√
Work Centers > Device Administration > Overview > Introduction	√	√	x	x	x	x	x	x	x	√
Work Centers > Device Administration > Overview > TACACS Livelog	√	√	x	x	x	x	x	x	x	√

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Device Administration > Overview > Deployment	√	√	x	x	x	x	x	x	x	√
Work Centers > Device Administration > Identities	√	√	x	√	x	x	x	x	x	√
Work Centers > Device Administration > Identities > Users	√	√	x	√	x	x	x	x	x	√
Work Centers > Device Administration > User Identity Groups	√	√	x	√	x	x	x	x	x	√
Work Centers > Device Administration > Ext Id Sources	√	√	x	√	x	x	x	x	x	√
Work Centers > Device Administration > Network Resources	√	√	x	x	√	x	x	x	x	√

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Device Administration > Network Resources > Network Devices	√	√	x	x	x	x	x	x	x	√
Work Centers > Device Administration > Network Resources > Network Device Groups	√	√	x	x	√	x	x	x	x	√
Work Centers > Device Administration > Network Resources > Default Devices	√	√	x	x	x	x	x	x	x	√
Work Centers > Device Administration > Network Resources > TACACS External Servers	√	√	x	x	x	x	x	x	x	√

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Device Administration > Network Resources > TACACS Server Sequence	√	√	x	x	x	x	x	x	x	√
Work Centers > Device Administration > Policy Elements	√	√	x	x	x	x	x	x	x	√
Work Centers > Device Administration > Policy Elements > Conditions	√	√	x	x	x	x	x	x	x	√
Work Centers > Device Administration > Policy Elements > Conditions > Authentication Simple Conditions	√	√	x	x	x	x	x	x	x	√

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Device Administration > Policy Elements > Conditions > Library Conditions	√	√	x	x	x	x	x	x	x	√
Work Centers > Device Administration > Policy Elements > Conditions > Smart Conditions	√	√	x	x	x	x	x	x	x	√
Work Centers > Device Administration > Policy Elements > Conditions > Authorization Simple Conditions	√	√	x	x	x	x	x	x	x	√

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Device Administration > Policy Elements > Conditions > Authorization Compound Conditions	√	√	x	x	x	x	x	x	x	√
Work Centers > Device Administration > Policy Elements > Network Conditions	√	√	x	x	x	x	x	x	x	√
Work Centers > Device Administration > Policy Elements > Network Conditions > Endstation Network Conditions	√	√	x	x	x	x	x	x	x	√

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Device Administration > Policy Elements > Network Conditions > Device Network Conditions	√	√	x	x	x	x	x	x	x	√
Work Centers > Device Administration > Policy Elements > Network Conditions > Device Port Network Conditions	√	√	x	x	x	x	x	x	x	√
Work Centers > Device Administration > Policy Elements > Results	√	√	x	x	x	x	x	x	x	√
Work Centers > Device Administration > Policy Elements > Results > Allowed Protocols	√	√	x	x	x	x	x	x	x	√

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets	√	√	x	x	x	x	x	x	x	√
Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles	√	√	x	x	x	x	x	x	x	√
Work Centers > Device Administration > Device Admin Policy Sets	√	√	x	x	x	x	x	x	x	√
Work Centers > Device Administration > Reports	√	√	√	√	√	√	√	√	x	√
Work Centers > Device Administration > Settings	√	√	x	x	x	x	x	x	x	√

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > PassiveID	√	√	√	x	x	x	x	x	x	x
Work Centers > PassiveID > Overview	√	√	x	x	x	x	x	x	x	x
Work Centers > PassiveID > Overview > Introduction	√	√	x	x	x	x	x	x	x	x
Work Centers > PassiveID > Overview > Dashboard	√	√	x	x	x	x	x	x	x	x
Work Centers > PassiveID > Overview > Live Sessions	√	√	x	x	x	x	x	x	x	x
Work Centers > PassiveID > Troubleshoot	√	√	√	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > PassiveID > Certificates	√	√	x	x	x	x	x	x	x	x
Work Centers > PassiveID > Certificates > System Certificates	√	√	x	x	x	x	x	x	x	x
Work Centers > PassiveID > Certificates > OCSP Client Profile	√	√	x	x	x	x	x	x	x	x
Work Centers > PassiveID > Certificates > Certificate Periodic Check Settings	√	√	x	x	x	x	x	x	x	x
Work Centers > PassiveID > Certificates > Issued Certificates	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > PassiveID > Certificates > Internal CA Settings	√	√	x	x	x	x	x	x	x	x
Work Centers > PassiveID > Certificates > Certificate Templates	√	√	x	x	x	x	x	x	x	x
Work Centers > PassiveID > Certificates > Trusted Certificates	√	√	x	x	x	x	x	x	x	x
Work Centers > PassiveID > Certificates > Certificate Signing Requests	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > PassiveID > Certificates > Overview	√	√	x	x	x	x	x	x	x	x
Work Centers > PassiveID > Certificates > Certificate Authority Certificates	√	√	x	x	x	x	x	x	x	x
Work Centers > PassiveID > Reports	√	√	√	x	x	x	x	x	x	x
Work Centers > PassiveID > Providers	√	√	x	x	x	x	x	x	x	x
Work Centers > PassiveID > Providers > Agents	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > PassiveID > Providers > SPAN	√	√	x	x	x	x	x	x	x	x
Work Centers > PassiveID > Providers > Mapping Filters	√	√	x	x	x	x	x	x	x	x
Work Centers > PassiveID > Providers > Active Directory	√	√	x	x	x	x	x	x	x	x
Work Centers > PassiveID > Providers > API Providers	√	√	x	x	x	x	x	x	x	x
Work Centers > PassiveID > Providers > Syslog Providers	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > PassiveID > Providers > Endpoint Probes	√	√	x	x	x	x	x	x	x	x
Work Centers > PassiveID > Subscribers	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD	√	√	√	√	√	√	√	√	√	x
Work Centers > BYOD > Overview	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Network Devices	√	√	x	x	√	x	x	x	x	x
Work Centers > BYOD > Client Provisioning	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Client Provisioning > Resources	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > BYOD > Client Provisioning > Client Provisioning Policy	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Policy Elements	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Policy Elements > Results	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Policy Elements > Results > Authorization Profiles	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Policy Elements > Results > Allowed Protocols	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > BYOD > Policy Elements > Results > Downloadable ACLs	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Policy Elements > Conditions	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Policy Elements > Conditions > Authentication Simple Conditions	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Policy Elements > Conditions > Authorization Simple Conditions	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > BYOD > Policy Elements > Conditions > Library Conditions	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Policy Elements > Conditions > Smart Conditions	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Policy Elements > Conditions > Authorization Compound Conditions	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Policy Sets	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Authentication Policy	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > BYOD > Reports	√	√	√	√	√	√	√	√	x	x
Work Centers > BYOD > Settings	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Settings > Employee Registered Devices	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Settings > Client Provisioning	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Settings > Retry URL	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Identities	√	√	x	√	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > BYOD > Identities > Endpoints	√	√	x	√	x	x	x	x	x	x
Work Centers > BYOD > Identities > Identity Source Sequences	√	√	x	√	x	x	x	x	x	x
Work Centers > BYOD > Identities > Network Access Users	√	√	x	√	x	x	x	x	x	x
Work Centers > BYOD > Identity Groups	√	√	x	√	x	x	x	x	x	x
Work Centers > BYOD > Ext Id Sources	√	√	x	√	x	x	x	x	x	x
Work Centers > BYOD > Portals & Components	√	√	x	x	x	x	x	x	√	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > BYOD > Portals & Components > BYOD Portals	√	√	x	x	x	x	x	x	√	x
Work Centers > BYOD > Portals & Components > Blocked List Portal	√	√	x	x	x	x	x	x	√	x
Work Centers > BYOD > Portals & Components > My Devices Portals	√	√	x	x	x	x	x	x	√	x
Work Centers > BYOD > Portals & Components > Certificates	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > BYOD > Portals & Components > Certificates > Certificate Templates	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Portals & Components > Certificates > Internal CA Settings	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Portals & Components > Certificates > External CA Templates	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Policy Sets	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > BYOD > Authorization Policy	√	√	x	x	x	x	x	x	x	x
Work Centers > BYOD > Custom Portal Files	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access	√	√	√	√	√	√	√	√	x	x
Work Centers > Network Access > Policy Sets	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Policy Sets	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Authentication Policy	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Network Access > Reports	√	√	√	√	√	√	√	√	x	x
Work Centers > Network Access > Settings	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Settings > Client Provisioning	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Settings > Collection Filters	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Settings > Protocols	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Network Access > Settings > Protocols > EAP TLS	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Settings > Protocols > EAP-FAST	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Settings > Protocols > EAP-FAST > EAP FAST	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Network Access > Settings > Protocols > EAP-FAST > Generate PAC	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Settings > Protocols > PEAP	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Settings > Protocols > RADIUS	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Settings > Proxy Settings	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Network Access > Dictionaries	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Overview	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Overview > Introduction	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Overview > RADIUS Livelog	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Identities	√	√	x	√	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Network Access > Identities > Endpoints	√	√	x	√	x	x	x	x	x	x
Work Centers > Network Access > Identities > Network Access Users	√	√	x	√	x	x	x	x	x	x
Work Centers > Network Access > Identities > Identity Source Sequences	√	√	x	√	x	x	x	x	x	x
Work Centers > Network Access > Id Groups	√	√	x	√	x	x	x	x	x	x
Work Centers > Network Access > Ext Id Sources	√	√	x	√	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Network Access > Network Resources	√	√	x	x	√	x	x	x	x	x
Work Centers > Network Access > Network Resources > Network Devices	√	√	x	x	√	x	x	x	x	x
Work Centers > Network Access > Network Resources > Device Groups	√	√	x	x	√	x	x	x	x	x
Work Centers > Network Access > Network Resources > Default Device	√	√	x	x	√	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Network Access > Network Resources > External RADIUS Servers	√	√	x	x	√	x	x	x	x	x
Work Centers > Network Access > Network Resources > RADIUS Server Sequences	√	√	x	x	√	x	x	x	x	x
Work Centers > Network Access > Network Resources > External MDM Servers	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Policy Elements	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Network Access > Policy Elements > Conditions	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Policy Elements > Conditions > Authentication Simple Conditions	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Policy Elements > Conditions > Library Conditions	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Network Access > Policy Elements > Conditions > Smart Conditions	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Policy Elements > Conditions > Authorization Simple Conditions	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Policy Elements > Conditions > Authorization Compound Conditions	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Network Access > Policy Elements > Conditions > Time and Date Conditions	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Policy Elements > Results	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Policy Elements > Results > Allowed Protocols	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Network Access > Policy Elements > Results > Authorization Profiles	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Policy Elements > Results > Downloadable ACLs	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Authorization Policy	√	√	x	x	x	x	x	x	x	x
Work Centers > Network Access > Troubleshoot	√	√	√	√	√	√	√	√	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Network Access > Troubleshoot > EndPoint Debug	√	x	x	x	x	x	x	x	x	x
Work Centers > Network Access > Troubleshoot > TCP Dump	√	x	x	x	x	x	x	x	x	x
Work Centers > Network Access > Troubleshoot > Collection Filters	√	√	√	√	√	√	√	√	x	x
Work Centers > Network Access > Troubleshoot > RADIUS Authentication Troubleshooting	√	√	√	√	√	√	√	√	x	x
Work Centers > Guest Access	√	√	√	√	√	√	√	√	√	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Guest Access > Overview	√	√	x	x	x	x	x	x	x	x
Work Centers > Guest Access > Administration	√	√	x	x	x	√	x	x	x	x
Work Centers > Guest Access > Administration > SMS Gateway Providers	√	√	x	x	x	√	x	x	x	x
Work Centers > Guest Access > Administration > Certificates	√	√	x	x	x	√	x	x	x	x
Work Centers > Guest Access > Administration > Certificates > System Certificates	√	√	x	x	x	√	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Guest Access > Administration > Certificates > Certificate Periodic Check Settings	√	√	x	x	x	√	x	x	x	x
Work Centers > Guest Access > Administration > Certificates > Certificate Signing Requests	√	√	x	x	x	√	x	x	x	x
Work Centers > Guest Access > Administration > SMTP Server	√	√	x	x	x	√	x	x	x	x
Work Centers > Guest Access > Portals & Components	√	√	x	x	x	x	x	x	√	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Guest Access > Portals & Components > Guest Types	√	√	x	x	x	x	x	x	√	x
Work Centers > Guest Access > Portals & Components > Sponsor Portals	√	√	x	x	x	x	x	x	√	x
Work Centers > Guest Access > Portals & Components > Guest Portals	√	√	x	x	x	x	x	x	√	x
Work Centers > Guest Access > Portals & Components > Sponsor Groups	√	√	x	x	x	x	x	x	√	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Guest Access > Policy Sets	√	√	x	x	x	x	x	x	x	x
Work Centers > Guest Access > Authorization Policy	√	√	x	x	x	x	x	x	x	x
Work Centers > Guest Access > Custom Portal Files	√	√	x	x	x	x	x	x	x	x
Work Centers > Guest Access > Identities	√	√	x	x	x	x	x	x	x	x
Work Centers > Guest Access > Identities > Endpoints	√	√	x	x	x	x	x	x	x	x
Work Centers > Guest Access > Identities > Network Access Users	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Guest Access > Identities > Identity Source Sequences	√	√	x	x	x	x	x	x	x	x
Work Centers > Guest Access > Identity Groups	√	√	x	√	x	x	x	x	x	x
Work Centers > Guest Access > Ext Id Sources	√	√	x	√	x	x	x	x	x	x
Work Centers > Guest Access > Network Devices	√	√	x	x	x	x	x	x	x	x
Work Centers > Guest Access > Manage Accounts	√	√	x	x	x	x	x	x	√	x
Work Centers > Guest Access > Policy Elements	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Guest Access > Policy Elements > Conditions	√	√	x	x	x	x	x	x	x	x
Work Centers > Guest Access > Policy Elements > Conditions > Authorization Simple Conditions	√	√	x	x	x	x	x	x	x	x
Work Centers > Guest Access > Policy Elements > Conditions > Common Time and Date Conditions	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Guest Access > Policy Elements > Conditions > Authorization Compound Conditions	√	√	x	x	x	x	x	x	x	x
Work Centers > Guest Access > Policy Elements > Results	√	√	x	x	x	x	x	x	x	x
Work Centers > Guest Access > Policy Elements > Results > Allowed Protocols	√	√	x	x	x	x	x	x	x	x
Work Centers > Guest Access > Policy Elements > Results > Downloadable ACLs	√	√	x	x	x	x	x	x	x	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Guest Access > Policy Elements > Results > Authorization Profiles	√	√	x	x	x	x	x	x	x	x
Work Centers > Guest Access > Policy Sets	√	√	x	x	x	x	x	x	x	x
Work Centers > Guest Access > Authentication Policy	√	√	x	x	x	x	x	x	x	x
Work Centers > Guest Access > Reports	√	√	√	√	√	√	√	√	x	x
Work Centers > Guest Access > Settings	√	√	x	x	x	x	x	x	√	x
Work Centers > Guest Access > Settings > Guest Password Policy	√	√	x	x	x	x	x	x	√	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Guest Access > Settings > Guest Account Purge Policy	√	√	x	x	x	x	x	x	√	x
Work Centers > Guest Access > Settings > Guest Email Settings	√	√	x	x	x	x	x	x	√	x
Work Centers > Guest Access > Settings > Guest Username Policy	√	√	x	x	x	x	x	x	√	x
Work Centers > Guest Access > Settings > Logging	√	√	x	x	x	x	x	x	√	x
Work Centers > Guest Access > Settings > Custom Fields	√	√	x	x	x	x	x	x	√	x

Menus and Submenus	Super Admin Menu Access	Policy Admin Menu Access	Helpdesk Admin Menu Access	Identity Admin Menu Access	Network Admin Menu Access	System Admin Menu Access	RBAC Admin Menu Access	MnT Admin Menu Access	Customization Admin Menu Access	TACACS+ Admin Menu Access
Work Centers > Guest Access > Settings > Guest Locations and SSIDs	√	√	x	x	x	x	x	x	√	x
Work Centers > GPC	√	√	√	x	x	x	x	x	x	x
Wizard	√	x	x	x	x	x	x	x	x	x
Settings	√	x	x	x	x	x	x	x	x	x

Configure Menu Access Permissions

Cisco ISE allows you to create custom menu access permissions that you can map to an RBAC policy. Depending on the role of the administrators, you can allow them to access only specific menu options.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Authorization** > **Permissions** > **Menu Access**

Step 2 Click **Add**, and enter values for the **Name** and **Description** fields.

a) Expand the **ISE Navigation Structure** menu to the required level, and click the options for which you want to create permissions.

b) In the **Permissions for Menu Access** pane, click **Show**.

Step 3 Click **Submit**.

Prerequisites for Granting Data Access Permissions

When an RBAC admin has Full Access permission to an object (for example, **Employee** in the **User Identity Groups** data type), the admin can view, add, update, and delete users who belong to that group. Ensure that the admin has menu access permission granted for the **Users** window (**Administration > Identity Management > Identities > Users**). This is applicable for network devices and endpoint objects (based on the permissions granted to the **Network Device Groups** and **Endpoint Identity Groups** data types).

You cannot enable or restrict data access for network devices that belong to the default network device group objects—**All Device Types** and **All Locations.** All the network devices are displayed if Full Access data permission is granted to an object created under these default network device group objects. Therefore, we recommend that you create a separate hierarchy for the **Network Device Groups** data type, which is independent of the default network device group objects. You should assign the network device objects to the newly created network devices groups to create restricted access.

Note You can enable or restrict data access permissions only for the User Identity Groups, Network Device Groups, and Endpoint Identity Groups, but not to Admin Groups.

Default Data Access Permissions

Cisco ISE comes with a set of predefined data access permissions. These permissions enable multiple administrators to have the data access permissions within the same user population. You can enable or restrict the use of data access permissions to one or more admin groups. This process allows autonomous delegated control to administrators of one admin group to reuse data access permissions of the chosen admin groups through selective association. Data access permissions range from full access to no access for viewing selected admin groups or network device groups. RBAC policies are defined based on the administrator (RBAC) group, menu access, and data access permissions. You should first create menu access and data access permissions and then create an RBAC policy that associates an admin group with the corresponding menu access and data access permissions. The RBAC policy takes the form: If admin_group=Super Admin then assign SuperAdmin Menu Access permission + SuperAdmin Data Access permission. Apart from the predefined data access permissions, Cisco ISE also allows you to create custom data access permissions that you can associate with an RBAC policy.

There are three data access permissions, namely, Full Access, No Access, and Read Only access that can be granted to admin groups.

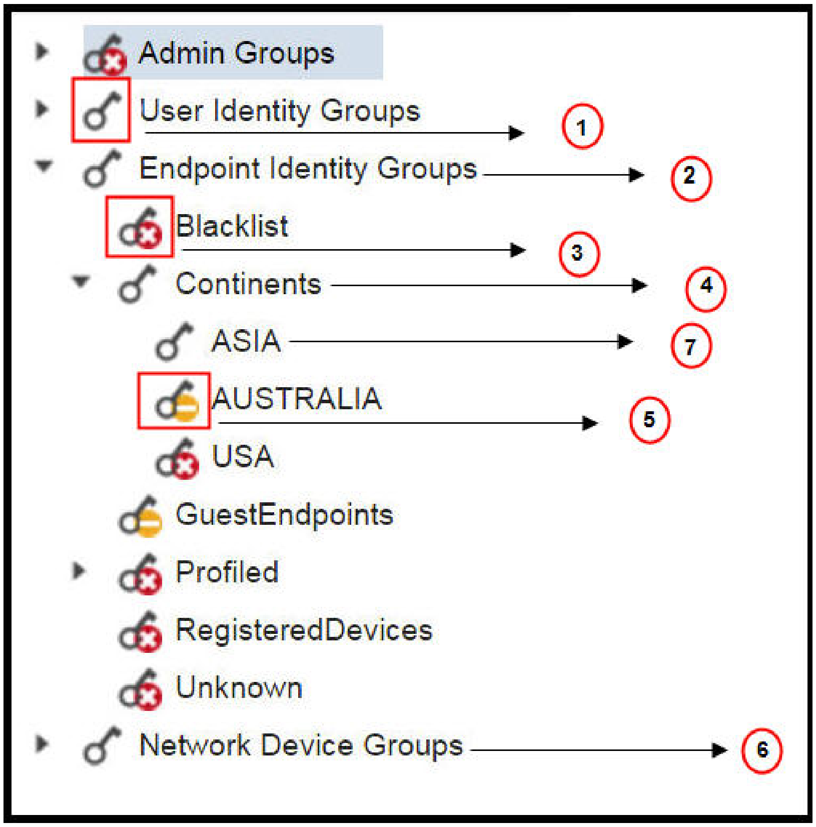
The Read Only permission can be granted to the following admin groups:

- **Administration** > **Admin Access** > **Administrators** > **Admin Groups**
- **Administration** > **Groups** > **User Identity Group**
- **Administration** > **Groups** > **Endpoint Identity Groups**
- **Network Visibility** > **Endpoints**
- **Administration** > **Network Resources** > **Network Device Groups**
- **Administration** > **Network Resources** > **Network Devices**
- **Administration** > **Identity Management** > **Identities**
- **Administration** > **Identity Management** > **Groups** > **User Identity Groups**
- **Administration** > **Identity Management** > **Groups** > **Endpoint Identity Groups**

If you have read-only permission for a data type (for example, Endpoint Identity Groups), you will not be able to perform CRUD operations on that data type. If you have read-only permission for an object (for example, GuestEndpoints), you cannot perform edit or delete operations on that object.

The following image shows how data access privileges are applied at the second-level or third-level menu that contains additional submenus or options for different RBAC groups.

Figure 1: Data Access Privileges


Admin Groups
User Identity Groups
Endpoint Identity Groups
Blacklist
Continents
ASIA
AUSTRALIA
USA
GuestEndpoints
Profiled
RegisteredDevices
Unknown
Network Device Groups
1
2
3
4
7
5
6

Label	Description
1	Denotes full access for the **User Identity Groups** data type.
2	Denotes that **Endpoint Identity Groups** derive the maximum permission (full access) that is granted to its child (Asia, in the example shown in the figure).
3	Denotes that there is no access for the object (blocked list).
4	Denotes that the parent (Continents) derives the maximum access permission granted to its child (Asia).
5	Denotes read-only access for the object (Australia).
6	Denotes that when full access is granted to the parent (**Network Device Groups**), it results in the children automatically inheriting permissions.
7	Denotes that when full access is granted to the parent (Asia), it results in the objects inheriting the Full Access permission, unless permissions are explicitly granted to the objects.

The following table shows the default data access permissions for different admin groups.

√: Denotes that a user has full access

x: Denotes that a user has no access

!: Denotes that a user has read-only access

Table 4: Data Access Permissions

Menus and Submenus	Super Admin Data Access	Policy Admin Data Access	Identity Admin Data Access	Network Admin Data Access	System Admin Data Access	RBAC Admin Data Access	Customization Admin Data Access	TACACS+ Admin Data Access	Read Only Admin Data Access
Admin Groups	√	x	x	x	√	√	x	x	!
Admin Groups > Super Admin	√	x	x	x	√	√	x	x	!
Admin Groups > Policy Admin	√	x	x	x	√	√	x	x	!
Admin Groups > Helpdesk Admin	√	x	x	x	√	√	x	x	!
Admin Groups > Identity Admin	√	x	x	x	√	√	x	x	!
Admin Groups > Network Device Admin	√	x	x	x	√	√	x	x	!
Admin Groups > System Admin	√	x	x	x	√	√	x	x	!
Admin Groups > RBAC Admin	√	x	x	x	√	√	x	x	!

Menus and Submenus	Super Admin Data Access	Policy Admin Data Access	Identity Admin Data Access	Network Admin Data Access	System Admin Data Access	RBAC Admin Data Access	Customization Admin Data Access	TACACS+ Admin Data Access	Read Only Admin Data Access
Admin Groups > MnT Admin	√	x	x	x	√	√	x	x	!
Admin Groups > ERS Admin	√	x	x	x	√	√	x	x	!
Admin Groups > ERS Operator	√	x	x	x	√	√	x	x	!
Admin Groups > Customization Admin	√	x	x	x	√	√	x	x	!
Admin Groups > TACACS+ Admin	√	x	x	x	√	√	x	x	!
Admin Groups > Read Only Admin	√	x	x	x	√	√	x	x	!
Admin Groups > Elevated System Admin	√	x	x	x	√	√	x	x	!
Admin Groups > SPOG Admin	√	x	x	x	√	√	x	x	!

Menus and Submenus	Super Admin Data Access	Policy Admin Data Access	Identity Admin Data Access	Network Admin Data Access	System Admin Data Access	RBAC Admin Data Access	Customization Admin Data Access	TACACS+ Admin Data Access	Read Only Admin Data Access
Admin Groups > ERS Trustsec	√	x	x	x	√	√	x	x	!
User Identity Groups	√	√	√	x	x	x	√	√	!
User Identity Groups > Guest_Type_Weekly (default)	√	√	√	x	x	x	√	√	!
User Identity Groups > OWN_ACCOUNTS (default)	√	√	√	x	x	x	√	√	!
User Identity Groups > GROUP_ACCOUNTS (default)	√	√	√	x	x	x	√	√	!
User Identity Groups > Guest_Type_SocialLogin (default)	√	√	√	x	x	x	√	√	!
User Identity Groups > Employee	√	√	√	x	x	x	√	√	!

Menus and Submenus	Super Admin Data Access	Policy Admin Data Access	Identity Admin Data Access	Network Admin Data Access	System Admin Data Access	RBAC Admin Data Access	Customization Admin Data Access	TACACS+ Admin Data Access	Read Only Admin Data Access
User Identity Groups > GuestType_Daily (default)	√	√	√	x	x	x	√	√	!
User Identity Groups > GuestType_Contractor (default)	√	√	√	x	x	x	√	√	!
User Identity Groups > ALL_ACCOUNTS (default)	√	√	√	x	x	x	√	√	!
Endpoint Identity Groups	√	√	√	x	x	x	√	x	!
Endpoint Identity Groups > Blocked List	√	√	√	x	x	x	√	x	!
Endpoint Identity Groups > GuestEndpoints	√	√	√	x	x	x	√	x	!
Endpoint Identity Groups > RegisteredDevices	√	√	√	x	x	x	√	x	!

Menus and Submenus	Super Admin Data Access	Policy Admin Data Access	Identity Admin Data Access	Network Admin Data Access	System Admin Data Access	RBAC Admin Data Access	Customization Admin Data Access	TACACS+ Admin Data Access	Read Only Admin Data Access
Endpoint Identity Groups > Unknown	√	√	√	x	x	x	√	x	!
Endpoint Identity Groups > Profiled	√	√	√	x	x	x	√	x	!
Endpoint Identity Groups > Profiled > Sony-Device	√	√	√	x	x	x	√	x	!
Endpoint Identity Groups > Profiled > Cisco-Meraki-Device	√	√	√	x	x	x	√	x	!
Endpoint Identity Groups > Profiled > Windows11-Workstation	√	√	√	x	x	x	√	x	!
Endpoint Identity Groups > Profiled > Apple-iDevice	√	√	√	x	x	x	√	x	!

Menus and Submenus	Super Admin Data Access	Policy Admin Data Access	Identity Admin Data Access	Network Admin Data Access	System Admin Data Access	RBAC Admin Data Access	Customization Admin Data Access	TACACS+ Admin Data Access	Read Only Admin Data Access
Endpoint Identity Groups > Profiled > BlackBerry	√	√	√	x	x	x	√	x	!
Endpoint Identity Groups > Profiled > Android	√	√	√	x	x	x	√	x	!
Endpoint Identity Groups > Profiled > Axis-Device	√	√	√	x	x	x	√	x	!
Endpoint Identity Groups > Profiled > Juniper-Device	√	√	√	x	x	x	√	x	!
Endpoint Identity Groups > Profiled > Epson-Device	√	√	√	x	x	x	√	x	!

Menus and Submenus	Super Admin Data Access	Policy Admin Data Access	Identity Admin Data Access	Network Admin Data Access	System Admin Data Access	RBAC Admin Data Access	Customization Admin Data Access	TACACS+ Admin Data Access	Read Only Admin Data Access
Endpoint Identity Groups > Profiled > Synology-Device	√	√	√	x	x	x	√	x	!
Endpoint Identity Groups > Profiled > Vizio-Device	√	√	√	x	x	x	√	x	!
Endpoint Identity Groups > Profiled > Trendnet-Device	√	√	√	x	x	x	√	x	!
Endpoint Identity Groups > Profiled > Cisco-IP-Phone	√	√	√	x	x	x	√	x	!
Endpoint Identity Groups > Profiled > OS_X_HighSierra-Workstation	√	√	√	x	x	x	√	x	!

Menus and Submenus	Super Admin Data Access	Policy Admin Data Access	Identity Admin Data Access	Network Admin Data Access	System Admin Data Access	RBAC Admin Data Access	Customization Admin Data Access	TACACS+ Admin Data Access	Read Only Admin Data Access
Endpoint Identity Groups > Profiled > Workstation	√	√	√	x	x	x	√	x	!
Network Device Groups	√	x	x	√	x	x	x	√	!
Network Device Groups > All Locations	√	x	x	√	x	x	x	√	!
Network Device Groups > All Locations > Asia	√	x	x	√	x	x	x	√	!
Network Device Groups > All Locations > Asia > India	√	x	x	√	x	x	x	√	!
Network Device Groups > Is IPSEC Device	√	x	x	√	x	x	x	√	!

Menus and Submenus	Super Admin Data Access	Policy Admin Data Access	Identity Admin Data Access	Network Admin Data Access	System Admin Data Access	RBAC Admin Data Access	Customization Admin Data Access	TACACS+ Admin Data Access	Read Only Admin Data Access
Network Device Groups > Is IPSEC Device > Yes	√	x	x	√	x	x	x	√	!
Network Device Groups > Is IPSEC Device > No	√	x	x	√	x	x	x	√	!
Network Device Groups > All Device Types	√	x	x	√	x	x	x	√	!
Customization	NA	NA	NA	NA	NA	NA	√	NA	NA

Configure Data Access Permissions

Cisco ISE allows you to create custom data access permissions that you can map to an RBAC policy. Based on the role of the administrator, you can choose to provide access to only select data.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Authorization** > **Permissions**

Step 2 Choose **Permissions** > **Data Access**.

Step 3 Click **Add**, and enter values for the **Name** and **Description** fields.

a) Click to expand the admin group and select the corresponding admin group.

b) Click **Full Access**, **Read Only Access,** or **No Access**.

Step 4 Click **Save**.

Read-Only Admin Policy

The default Read-Only Admin policy is available in the **Administration > System > Admin Access > Authorization > RBAC Policy** window. This policy is available for both new installations and upgraded deployments. The Read-Only Admin policy is applicable to the Read-Only Admin group. By default, Super Admin Menu Access and Read-Only Data Access permissions are granted to Read-Only administrators. This policy cannot be duplicated and the associated **Data Access** permission cannot be edited.

Note

- The default read-only policy is mapped to the Read Only Admin group. You cannot create custom RBAC policy using the Read Only Admin group.
- Cisco ISE supports the read-only functionality based on the static check of Read-Only Admin Group only.

Customize Menu Access for the Read-Only Administrator

By default, Read-Only Administrators are given Super Admin Menu Access and Read Only Admin Data Access. However, if the Super Admin requires that the Read-Only Administrator view only the **Home** and **Administration** tabs, the Super Admin can create a custom menu access or customize the default Permissions to, for example, MnT Admin Menu Access or Policy Admin Menu Access. The Super Admin cannot modify the Read Only Data Access mapped to the Read Only Admin Policy.

Step 1 Log in to the Admin portal as a Super Admin.

Step 2 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Authorization** > **Permissions** > **Menu Access**

Step 3 Click **Add** and enter a **Name** (for example, MyMenu) and **Description**.

Step 4 In the **Menu Access Privileges** section, you can enable the **Show** or **Hide** option to choose the required options (for example, **Home** and **Administration** tabs) that should be displayed for the Read-Only Administrator.

Step 5 Click **Submit**.
The custom menu access permission is displayed in the **Permissions** drop-down list corresponding to the Read-Only Admin Policy displayed in the **Administration > System > Admin Access > Authorization > Policy** window.

Step 6 Choose **Administration > System > Admin Access > Authorization > RBAC Policy** window.

Step 7 Click the **Permissions** drop-down list corresponding to the **Read-Only Admin Policy** and choose a default (MnT Admin Menu Access) or custom menu access permission (MyMenu) that you have created in the **Administration > System > Admin Access > Authorization > Permissions > Menu Access** window.

Step 8 Click **Save**.

Note

- You will encounter an error if you choose **Data Access** permissions for the Read-Only Admin policy.
- When you log in to the Read-Only Admin portal, a Read-Only icon appears at the top of the window, and you can view only the specified menu options without data access.

CHAPTER 3

Licensing

- Cisco ISE Licenses, on page 157
- Cisco ISE Smart Licensing, on page 160
- Smart Licensing for Air-Gapped Networks, on page 164

Cisco ISE Licenses

Cisco ISE services provide visibility and control over the increasing number of endpoints in your network. Cisco ISE features are mapped to specific licenses and you can enable the licenses that provide the Cisco ISE capabilities you need to meet your organizational needs.

Cisco ISE is bundled with a licensing mechanism with the following salient features:

- Built-in License: Cisco ISE comes with a built-in evaluation license that is valid for 90 days. You do not have to install a Cisco ISE license immediately after you install Cisco ISE. You can use the Evaluation license that provides all the Cisco ISE functionalities.
- Central Management of Licenses: The Cisco ISE Primary Administration node (PAN) centrally manages Cisco ISE licenses. In a distributed deployment that has primary and secondary PANs, the primary PAN automatically shares the licensing information with the secondary PAN.
- Concurrent Active Endpoint Count: Cisco ISE licenses include a count value for each tier license. Each tier license supports a specific number of active endpoints at any time. The count value refers to the number of active endpoints across the entire deployment that are using specific Cisco ISE services at any time. Because Cisco ISE licensing relies on RADIUS accounting, you must have RADIUS services enabled on the network devices.

  Concurrent active endpoints refer to the total number of supported users and devices. Here, an endpoint could mean users, PCs, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, or other types of network devices.

Cisco ISE Release 3.0 and later releases do not support legacy licenses, such as Base, Plus, and Apex licenses, that were used in Cisco ISE Release 2.x. Cisco ISE Release 3.x licenses are managed entirely through a centralized database that is called the Cisco Smart Software Manager (CSSM). You can register, activate, and manage all your licenses easily and efficiently with single-token registration.

To maximize economy for customers, licensing in Cisco ISE is supplied in the following packages:

- **Tier Licenses**

From Cisco ISE Release 3.0, a new set of licenses that are called Tier Licenses replace the Base, Apex, and Plus licenses used in releases earlier than Release 3.0. Tier Licenses include three licenses—Essentials, Advantage, and Premier.

If you currently have Base, Apex, or Plus licenses, use the CSSM to convert them into the new license types.

- **Device Administration Licenses**

  Policy Service nodes (PSN) that have the TACACS+ persona enabled on them use Device Administration licenses.

- **Virtual Appliance Licenses**

  Cisco ISE Release 3.1 supports the ISE VM License. This license replaces the VM Small, VM Medium, and VM Large licenses that were supported in releases earlier than 3.1. The ISE VM License covers the Cisco ISE VM nodes in both on-prem and cloud deployments.

  If a virtual appliance is used, but your Cisco ISE does not have an active VM license, you receive warnings and notifications of noncompliant license consumption until you procure and install a VM license. However, Cisco ISE services are not interrupted.

- **Evaluation Licenses**

  The Evaluation license is enabled by default when you first install Cisco ISE Release 3.0 and later releases and support up to 100 endpoints. Evaluation licenses are 90-day licenses that give you access to all the Cisco ISE features. During the evaluation period, license consumption is not reported to the CSSM.

If you are upgrading to Cisco ISE Release 3.0 and later releases with Base, Apex, and Plus licenses smart licenses, your smart licenses are upgraded to the new license types in Cisco ISE. However, you must register the new license types in CSSM to activate the licenses in the Cisco ISE release that you upgrade to.

If you own traditional Cisco ISE licenses, you must convert them to smart licenses to enable license consumption in Cisco ISE Release 3.0 and later releases. To convert Cisco ISE 2.x licenses to the new license types, open a case online through the Support Case Manager at http://cs.co/scmswl, or use the contact information that is provided at http://cs.co/TAC-worldwide.

Notifications about noncompliant license consumption are also displayed in Cisco ISE. If your license consumption is out of compliance for 45 days in a 60-day period, you will lose all administrative control of Cisco ISE until you purchase and activate the required licenses.

When upgrading from one licensing package to another, Cisco ISE continues to offer all the features that were available in the earlier package before the upgrade. However, you do have to reconfigure any settings that you had already configured. For example, if you currently use an Essentials license and later add an Advantage license, the features that are already configured using the Essentials license will not change.

You should update your license agreements if:

- The evaluation period has ended, and you have not yet registered your license.
- Your license has expired.
- The endpoint consumption exceeds your licensing agreement.

Cisco ISE Community Resource

Cisco Identity Services Engine Ordering Guide

For information on how to obtain evaluation licenses, see How to Get ISE Evaluation Licenses.

Tier Licenses

The following table specifies what the new Tier Licenses enable.

Table 5: Cisco ISE Tier Licenses

License Name	What Does this License Enable?
Essentials	• RADIUS authentication, authorization, and accounting, including 802.1X, MAC authentication bypass and easy connect, and web authentication. • MACsec. • Authentications that are based on Single Sign-On (SSO), Security Assertion Markup Language (SAML), and Open DataBase Connectivity (ODBC) standards. • Guest access and sponsor services. • Representational State Transfer (REST) APIs for monitoring purposes, and External RESTful Services APIs for CRUD operations. • Passive ID services. • Secure wired and wireless access.
Advantage	• All the features that are enabled by the Cisco ISE Essentials license. • Bring Your Own Device (BYOD) device registration and provisioning, with a built-in certification authority. Device registration occurs through the configured My Devices portals. • Security Group Tagging, TrustSec, and Cisco Application-Centric Infrastructure (ACI) integration. • Profiling services, including basic asset visibility and enforcement features. • Feed services. • Context sharing (such as pxGrid), and security ecosystem integrations. • Rapid Threat Containment, using Adaptive Network Control and context-sharing services. • Cisco AI Endpoint Analytics visibility and enforcement.
Premier	• All the features that are enabled by the Cisco ISE Essentials and Advantage licenses. • Posture visibility and enforcement. • Compliance visibility and enforcement through Enterprise Mobility Management and Mobile Device Management. • Threat-Centric Network Access Control visibility and enforcement.

Note You may witness higher Cisco ISE license consumption count if the privacy settings in endpoints permit MAC randomization or rotating and changing MAC. When an endpoint authenticates with a new random MAC address, a new Cisco ISE session is created.

Device Administration Licenses

A Device Administration license allows you to use TACACS services on a Policy Service node. In a high availability (HA) standalone deployment, a Device Administration license permits you to use TACACS services on a single Policy Service node in the HA pair.

Evaluation Licenses

Evaluation licenses are activated by default when you install or upgrade to Cisco ISE Release 3.0 and later releases and support up to 100 endpoints. The Evaluation license is active for 90 days, and you have access to all the Cisco ISE features during this time. Cisco ISE is considered to be in Evaluation mode when the Evaluation license is in use.

The Cisco ISE GUI displays messages with the number of days that are left in the Evaluation mode.

Note You must purchase and register Cisco ISE licenses by the end of the Evaluation mode to continue using the Cisco ISE features that you need.

Cisco ISE Smart Licensing

When a smart license token is active and registered in the Cisco ISE administration portal, the CSSM monitors the consumption of licenses by each endpoint session per product license. Smart Licensing notifies the administrator about license consumption by endpoint sessions with a simple table layout in Cisco ISE. Smart Licensing reports the peak usage of each enabled license to the centralized database daily. When licenses are available and not consumed, the administrator is notified of available licenses and can continue to monitor usage. When consumption exceeds the number of licenses available, an alarm is activated and the administrator is notified through alarms and notifications.

With Smart Licensing, you can also manage the different license entitlements included through your Cisco Smart Account, such as Essentials, Advantage, Premier, or Device Admin. From Cisco ISE, you can monitor basic consumption statistics per license entitlement. From your CSSM account, you can view additional information, statistics, and notifications, as well as make changes to your account and entitlements.

Cisco ISE takes internal samples of license consumption every 30 minutes. License compliancy and consumption is updated accordingly. To view this information in the **Licenses** table in Cisco ISE, from the main menu, choose **Administration** > **System** > **Licensing**, and click **Refresh**.

From the time you register your Cisco ISE Primary Administration node (PAN) with the CSSM, Cisco ISE reports peak counts of license consumption to the CSSM server every six hours. The peak count reports help ensure that license consumption in Cisco ISE is in compliance with the licenses purchased and registered. Cisco ISE communicates with the CSSM server by storing a local copy of the CSSM certificate. The CSSM certificate is automatically reauthorized during the daily synchronization, and when you refresh the **Licenses** table. Typically, CSSM certificates are valid for six months.

If there is a change in the compliance status when Cisco ISE synchronizes with the CSSM server, the **Last Authorization** column of the **Licenses** table is updated accordingly. In addition, when entitlements are no longer compliant, the number of days for which they are out of compliancy appears in the **Days Out of Compliancy** column. Noncompliancy is also indicated in the notifications displayed at the top of the **Licensing** area, and on the Cisco ISE toolbar next to the **License Warning** link. In addition to notifications, you can view alarms.

Note Device Admin licenses are authorized when Cisco ISE communicates with the CSSM server, but they are not session-based, and therefore, no consumption count is associated with them in the **Licenses** table.

The compliance column of the **Licenses** table displays one of the following values:

- **In Compliance**: The use of this license is in compliance.
- **Released Entitlement**: The licenses have been purchased and released for use, but none have been consumed so far in this Cisco ISE deployment. In such a scenario, the **Consumption Count** for the license is 0.
- **Evaluation**: Evaluation licenses are available for use.

Register and Activate Smart Licenses

Before you begin

- If you have traditional Cisco ISE licenses, you must convert them to smart licenses.
- If you are upgrading to Cisco ISE Release 3.0 and later releases with existing smart licenses, convert the licenses to the new smart license types in CSSM.
- Register your new smart license types in CSSM to receive a registration token.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Licensing**.

Step 2 In the **Licensing** window that is displayed, click **Registration Details**.

Step 3 In the **Registration Details** area that is displayed, enter the registration token that you received from CSSM, in the **Registration Token** field.

Step 4 Choose a connection method from the **Connection Method** drop-down list:

- **Direct HTTPS** if you have configured a direct connection to the internet.
- **HTTPS Proxy** if you do not have a direct connection to the internet and need to use a proxy server. (If you change your proxy server configuration after you register Cisco ISE Smart Licenses, you must update your Smart Licenses configuration in the **Licensing** window. Cisco ISE establishes a connection with the CSSM using the updated proxy server, avoiding disruption of Cisco ISE services.)
- **Transport Gateway** is the recommended option. If you have configured a Transport Gateway, this connection is chosen by default. To choose another connection method, you must remove the Transport Gateway configuration.

- **SSM On-Prem Server** to connect to the configured SSM on-prem server. This option is available in Cisco ISE Release 3.0 Patch 2 and later. See Smart Licensing for Air-Gapped Networks, on page 164.

Step 5 In the **Tier** and **Virtual Appliance** areas, check the check boxes for all the licenses you need to enable. The chosen licenses are activated and their consumption is tracked by CSSM.

Step 6 Click **Register**.

Manage Smart Licensing in Cisco ISE

After you activate and register your Smart Licensing token, you can manage license entitlements from Cisco ISE by:

- Enabling, disabling, and refreshing license entitlement certificates.
- Updating Smart Licensing registration.
- Identifying compliant and noncompliant licensing issues.

If you have carried out the legacy or new Cisco ISE split upgrade process, the secondary PAN is promoted to the primary PAN in the process. In the Cisco ISE administration portal, choose **Administration** > **Licensing**. In the **Cisco Smart Licensing** area, click **Update**.

A licensing alarm is displayed in your Cisco ISE until you update your licenses.

Before you begin

Ensure that you have activated and registered your Smart Licensing token.

Step 1 (Optional) When you first install Cisco ISE Release 3.0 and later releases, all the license entitlements are enabled automatically as part of the Evaluation mode. After you register your license token, if your CSSM account does not include certain entitlements and you did not disable them during registration, noncompliant notifications are displayed in Cisco ISE. Add those entitlements to your CSSM account (contact your CSSM account representative for assistance), and then, in the **Licenses** table, click **Refresh** to remove noncompliant notifications and continue to use the related features. After you refresh the authorization, log out and then log back in to Cisco ISE for the relevant noncompliancy messages to be removed.

Step 2 (Optional) If the daily automatic authorization does not succeed for any reason, noncompliancy messages may appear. Click **Refresh** to reauthorize your entitlements. After you refresh the authorization, log out and then log back in to Cisco ISE for the relevant noncompliancy messages to be removed.

Step 3 (Optional) When you first install Cisco ISE Release 3.0 and later releases, all license entitlements are enabled automatically as part of the evaluation period. After you register your token, if your CSSM account does not include certain entitlements and you did not disable them during registration, you can still disable those entitlements from Smart Licensing in ISE in order to avoid unnecessary noncompliant notifications. From the **Licenses** table, check the check boxes for the license entitlements that are not included in your token, and click **Disable** from the toolbar. After you have disabled license entitlements, log out and then log back in to Cisco ISE for the relevant features to be removed from the menus and for the noncompliancy messages to be removed.

Step 4 (Optional) After you add entitlements to your account, enable those entitlements. From the **Licenses** table, check the check boxes for the required disabled licenses, and click **Enable** from the toolbar.

Step 5 (Optional) The registration certificate is automatically refreshed every six months. To manually refresh your Smart Licensing certificate registration, click **Renew Registration** at the top of the **Licensing** window.

Step 6 (Optional) To remove your Cisco ISE registration (indicated by UDIs) from your Smart Account, but continue to use Smart Licensing till the end of the evaluation period, click **Deregister** at the top of the **Cisco Smart Licensing** area. You can do this, for example, if you need to change the UDIs you have indicated as part of the registration process. If you still have time remaining in your evaluation period, Cisco ISE remains in Smart Licensing. If your evaluation period is at an end, a notification appears when the browser is refreshed. After you deregister your smart license, you can follow the registration process again in order to register with the same or different UDIs.

Step 7 (Optional) To remove your Cisco ISE registration (indicated by UDIs) from your Smart Account entirely, and to revert to traditional licensing, click **Disable** at the top of the **Cisco Smart Licensing** area. You can do this, for example, if you need to change the UDIs you have indicated as part of the registration process. After you disable the smart license, follow the registration process again in order to activate and register with the same or different UDIs.

Troubleshooting: Unregistered License Usage

Issue

Endpoint license consumption relies on the attributes that are used in the authorization policy with which an endpoint is matched.

Consider a scenario where you only have a Cisco ISE Essentials license registered in your system, because you deleted the 90-day Evaluation license. You will be able to see and configure the corresponding Cisco ISE Essentials menu items and features.

If you configure an authorization policy to use a feature, for example, if you use the Session:PostureStatus attribute that requires an Premier license, and an endpoint matches this authorization policy, then:

- The endpoint consumes a Cisco ISE Premier license despite the fact that a Cisco Premier license has not been registered in the system.
- You see notifications of noncompliant license consumption whenever you log in.
- Cisco ISE displays notifications and alarms with the message `Exceeded license usage than allowed`. This is because there are no Cisco ISE Premier licenses that are registered in CSSM for your Cisco ISE, but an endpoint is consuming one.

Note The licensing alarm is displayed for about 60 days from the first occurrence of noncompliant license use even if you fix the licensing issue by registering the necessary licenses.

If the use of all three Tier licenses is out of compliance for 45 days in a 60-day period, administrative control of Cisco ISE is lost until you register the correct licenses. You will be able to access only the **Licensing** window in the Cisco ISE administration portal until the correct licenses are registered. However, Cisco ISE continues to handle authentications.

Possible Causes

Because of the configuration of an authorization policy, the **Licensing** table reports that Cisco ISE has used a license that you have not purchased and registered. Before you purchase an Advantage or Premier license, the Cisco ISE administration portal does not display the features covered by these licenses. However, after you purchase these licenses, the GUI continues to display the features that the licenses enable even after the license has expired or endpoint consumption of the license has exceeded a set limit. Thus, you can configure the features even if you do not currently have a valid license for them.

Solution

In the Cisco ISE administration portal, click the **Menu** icon (≡) and choose **Policy** > **Policy Sets**, identify the authorization rule that is using the feature for which you do not have a registered license, and reconfigure that rule.

Smart Licensing for Air-Gapped Networks

An air-gapped network does not allow any communication between a secured network and an external network. Cisco ISE Smart Licensing requires Cisco ISE to communicate with the CSSM. If your network is air-gapped, Cisco ISE is unable to report license usage to CSSM, and this lack of reporting results in the loss of administrative access to Cisco ISE and restrictions in Cisco ISE features.

To avoid licensing issues in air-gapped networks and enable full Cisco ISE functionality, you can:

- Configure a Smart Software Manager (SSM) On-Premises server.

  You must configure an SSM On-Prem and ensure that Cisco ISE can reach this server. This server takes over the role of CSSM in your air-gapped network, releasing license entitlements, as needed, and tracking usage metrics. The SSM On-Prem server also sends notifications, alarms, and warning messages that are related to licensing consumption and validity.

  For more information on how to configure the SSM On-Prem server connection, see Configure Smart Software Manager On-Prem for Smart Licensing, on page 164.
- Enable Specific License Reservation, which is a smart licensing method that helps you manage Smart Licensing when your organization's security requirements do not allow a persistent connection between Cisco ISE and the SSM. Specific License Reservation allows you to reserve specific license entitlements on a Cisco ISE PAN.

  For more information, see Specific License Reservation, on page 165.

Configure Smart Software Manager On-Prem for Smart Licensing

Before you begin

Configure an SSM On-Prem server and ensure that Cisco ISE can reach this server. For more information, see Smart Software Manager On-Prem Resources.

You must update to SSM On-Prem Release 8-202108 or later to register your license successfully for Cisco ISE 3.0 and later.

If you buy more licenses or modify your license purchases, you must connect the SSM On-Prem server to CSSM for the changes to be available in your local server.

Note ISE-PIC 2.7 and earlier do not support Smart Licensing.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Licensing**.

Step 2 Click **Registration Details**.

Step 3 In the **Registration Details** area that is displayed, in the **Registration Token** field, enter the registration token that you received from CSSM.

Step 4 From the **Connection Method** drop-down list, choose **SSM On-Prem server** .

The **Certificate** window in the SSM On-Prem portal displays either the IP address or the hostname (or FQDN) of the connected SSM On-Prem server.

Step 5 In the **SSM On-Prem server Host** field, enter the configured IP address or the hostname (or FQDN).

Step 6 In the **Tier** and **Virtual Appliance** areas, check the check boxes for all the licenses you want to enable. The chosen licenses are activated and their consumption is tracked by CSSM.

Step 7 Click **Register**.

Note Ensure that port 443 and the port used for ICMP communication are open while registering Cisco ISE with the SSM On-Prem server.

Specific License Reservation

Specific license reservation is a smart licensing method that helps you manage Smart Licensing when your organization's security requirements do not allow a persistent connection between Cisco ISE and the Cisco Smart Software Manager (CSSM). Specific license reservation allows you to reserve specific license entitlements on a Cisco ISE PAN.

While Cisco ISE smart licensing works as a nested-doll model where a higher tier license includes all the lower tier features, specific license reservation does not support such a model. In specific license reservation, you must reserve and activate the required license count for each Cisco ISE license type. For example, if you want to use Cisco ISE features enabled by Advantage and Premier licenses, you must reserve both Advantage and Premier licenses. You receive error or nonauthorized behavior notifications if your Cisco ISE contains only Premier licenses.

You can create a Specific License Reservation by defining the type and number of licenses you must reserve, and then activate the reservation on a Cisco ISE node. The Cisco ISE node on which you register and enable the reservation then tracks license use and enforces license consumption compliance.

A Specific License Reservation can be enabled only on the Cisco ISE node for which it is generated. Icen a distributed deployment, we recommend that you enable Specific License Reservations on your primary and secondary PANs.

If there are no Cisco ISE licenses registered on your secondary PAN, in the case of primary PAN failure, Cisco ISE access and services are impacted. You will not be able to view or modify any Cisco ISE policies or elements. We strongly recommend registering Cisco ISE licenses on both primary and secondary PANs for uninterrupted Cisco ISE access.

If Cisco ISE licenses are registered on the secondary PAN as well, in the event of a primary PAN failover, Cisco ISE will continue to be accessible through the newly promoted secondary PAN. You can then work on rejoining the primary PAN to its original state.

For tier licenses (Essentials, Advantage, Premier), we recommend that you register 100% of the required licenses on the primary PAN and an additional license count on the secondary PAN. The following table explains two approaches to ensuring uninterrupted access to Cisco ISE if you require 100 tier licenses:

Table 6: Recommended License Distribution for Tier Licenses

Minimum required license distribution that ensures Cisco ISE runs uninterrupted.		What to expect in the event of a primary PAN failover	Maximum license distribution that ensures Cisco ISE runs uninterrupted, without noncompliance alarms.		What to expect in the event of a primary PAN failover
Primary PAN	Secondary PAN		Primary PAN	Secondary PAN	
100	1	Since the newly promoted primary PAN doesn’t have sufficient licenses, your Cisco ISE goes out of compliance. Cisco ISE enters a 30-day grace period. Before the grace period expires, rejoin the original primary PAN with the higher license count. Alternatively, to continue working with the newly promoted primary PAN, release the licenses reserved on original PAN and reserve the required licenses on the newly promoted PAN.	100	100	No impact on Cisco ISE services or operations. No remediation actions are required. You must only rejoin the original PAN to Cisco ISE.

In the case of Device Admin and Virtual Appliance licenses, if you require 10 licenses of either type in your Cisco ISE, register ten on the primary PAN and at least one on the secondary PAN. The following table explains two approaches to ensuring uninterrupted access to Cisco ISE, if you need 10 virtual licenses or 10 device admin licenses:

Table 7: Recommended License Distribution for Virtual Licenses and Device Admin Licenses

Minimum required license distribution that ensures Cisco ISE runs uninterrupted.		What to expect in the event of a primary PAN failover	Maximum license distribution that ensures Cisco ISE runs uninterrupted, without noncompliance alarms.		What to expect in the event of a primary PAN failover
Primary PAN	Secondary PAN		Primary PAN	Secondary PAN	
10	1	Since the newly promoted primary PAN doesn't have sufficient licenses, your Cisco ISE goes out of compliance. Cisco ISE enters a 30-day grace period. Before the grace period expires, rejoin the original primary PAN with the higher license count. Alternatively, to continue working with the newly promoted primary PAN, release the licenses reserved on original PAN and reserve the required licenses on the newly promoted PAN.	10	10	No impact on Cisco ISE services or operations. No remediation actions are required. You must only rejoin the original PAN to Cisco ISE.

You will not be able to use any license entitlements that are not part of your Specific License Reservation. Out-of-compliance alerts are displayed in the Cisco ISE administration portal if license usage is not in compliance with the license reservation.

Enable Specific License Reservation

Step 1 In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration** > **System** > **Licensing**.

Step 2 In the **License Type** area, click the **Specific License Reservation** radio button.

Step 3 In the **SLR Configuration** area, click **Generate Code** in the **Standalone/Primary PAN** area.

A code is displayed in the **Reservation Code** field next to it.

Note After you generate the reservation code, click **Cancel Request** to return the reservation code to the CSSM server. This code is then rendered invalid. You must generate a new reservation code the next time you want to install and enable Specific License Reservation on your primary PAN.

Step 4 Copy the reservation code to submit it in the CSSM portal (Step 8).

Step 5 Log in to the software.cisco.com portal, and from the main menu, choose **License** > **Smart Software Licensing**.

Step 6 Choose **Inventory** > **Licenses** to view your purchased smart licenses, license entitlements in use, and available entitlements.

Step 7 Click **License Reservation**.

A **Smart License Reservation** workflow dialog box is displayed.

Step 8 In the **Step 1: Enter Request Code** tab, in the field that is displayed, enter the reservation code you received from Cisco ISE (Step 3).

Step 9 Click **Next**.

Step 10 In the **Step 2: Select Licenses** tab, click the **Reserve a specific license** radio button. Then, in the **Reserve** column of the table displayed, for each license type, enter the number of license entitlements you want to reserve on the primary PAN.

Step 11 Click **Next**.

Step 12 In the **Step 3: Review and Confirm** tab, review the details of your specific license reservation, and click **Generate Authorization Code**.

Step 13 The **Step 4: Authorization Code** tab contains a field that displays the authorization code in XML format. This XML content includes information on the license reservation and the Cisco ISE node for which the SLR is generated. Do not make any modifications to this content because tampered code is rejected by Cisco ISE. Click **Download As File** to download the .txt file with the XML content to your local system.

Step 14 In the **Licensing** window of the Cisco ISE administration portal, in the **Primary PAN** area, click **Upload SLR License Key** and choose the XML file that you downloaded from the CSSM portal.

It takes a few minutes for the key to upload to your node and for the activation of the Specific License Reservation.

Step 15 To configure Specific License Reservation on your secondary PAN, carry out the following steps in the **Secondary PAN (optional)** area:

a. Click **Generate Code**.

A code is displayed in the **Reservation Code** field next to it.

Note After you generate a reservation code, click **Cancel Request** to return the reservation code to the CSSM server. This code is then rendered invalid. You must generate a new reservation code the next time you want to install and enable Specific License Reservation on your secondary PAN.

b. Repeat Step 5 to Step 13 to configure the Specific License Reservation for your secondary PAN.

c. In the **Secondary PAN** area, click **Upload SLR License Key** and choose the XML file that you downloaded from the CSSM portal.

It takes a few minutes for the key to get uploaded to your node and for the activation of the Specific License Reservation.

Update Specific License Reservation

You can modify the Specific License Reservation for a node, as required. You might have to update your Specific License Reservation in the following scenarios:

- Evolving business needs that require you to modify your license reservation.
- A primary PAN failover after which the primary PAN cannot be recovered. When the primary PAN fails, the license entitlements reserved on it are no longer available in Cisco ISE. To avoid losing administrative access to Cisco ISE because of noncompliant license usage, you must return the Specific License Reservation that was enabled on the node, and update the Specific License Reservation on your new primary PAN (the promoted secondary PAN) accordingly.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Licensing**.

Step 2 From the **UDI Details** area, copy the serial number of the node for which you want to update the Specific License Reservation.

Step 3 Log in to the software.cisco.com portal, and from the main menu, choose **License** > **Smart Software Licensing**.

Step 4 Choose **Product Inventory**.

Step 5 Enter the serial number that you copied from Cisco ISE in the search bar displayed above the inventory list, to view the corresponding entry.

Step 6 From the **Actions** drop-down list, choose **Update Reserved Licenses**.

Step 7 Click the **Reserve a Specific License** radio button to view the list of licenses. Edit the number of license reservations in the corresponding field in the **Reserve** column.

Step 8 Click **Next**.

Step 9 In the **Step 3: Review and Confirm** tab, review the details of your specific license reservation and click **Generate Authorization Code**.

Step 10 The **Step 4: Authorization Code** tab contains a field that displays the authorization code in XML format. Do not make any modifications to this content because Cisco ISE rejects tampered code.

Step 11 Click **Download As File**. A .txt file with the XML content downloads gets downloaded to your local system.

Step 12 In the **Licensing** window of the Cisco ISE administration portal, in the required PAN area, click **Update SLR Code** and choose the XML file that you downloaded from the CSSM portal.

It takes a few minutes for the key to get uploaded to your node and for the Specific License Reservation to be activated.

Step 13 After you submit the updated Specific License Reservation code, a confirmation code is displayed in the **Update Reservation** dialog box. Copy this confirmation code to submit it in the CSSM portal.

Step 14 Repeat Step 3 and Step 4, and in the dialog box that is displayed, click **Enter Confirmation Code** and enter the confirmation code generated by Cisco ISE.

Return Specific License Reservation

If Specific License Reservation is enabled on multiple nodes, you must carry out the return reservation process for each node to completely remove Specific License Reservation.

If Specific License Reservation is active on your secondary PAN, and you return the Specific License Reservation that is active on your primary PAN, the reservation on your secondary PAN is also automatically returned.

In a high-availability PAN configuration, when you return the Specific License Reservation on the primary PAN, the secondary PAN's Specific License Reservation is also returned.

Each node has a unique return code generated, and you must submit each of the return codes in the CSSM to remove Specific License Reservations from the nodes.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Licensing**.

Step 2 Click **Return Reservation** for the node whose Specific License Reservation you want to return.

A return code is displayed in the **Return Reservation** dialog box.

Step 3 Copy this code and submit it in your CSSM to complete the reservation return process.

Step 4 Log in to the software.cisco.com portal, and from the main menu, choose **License** > **Smart Software Licensing**.

Step 5 In the **Smart Software Licensing** window, click **Product Inventory**.

Step 6 Enter the serial number that you copied from Cisco ISE in the search bar displayed above the inventory list to view the corresponding entry.

Step 7 From the **Actions** drop-down list, choose **Remove**.

Step 8 In the **Remove Product Instance** dialog box that is displayed, enter the Return Reservation code that you received from Cisco ISE.

Step 9 Click **Remove Product Instance**.

The license entitlements in the license reservation are now released and available in the CSSM.

CHAPTER 4

Deployment of Cisco ISE

- Cisco ISE Deployment Terminology, on page 171
- Personas in Distributed Cisco ISE Deployments, on page 172
- Configure a Cisco ISE Node, on page 172
- Support for Multiple Deployment Scenarios, on page 175
- Cisco ISE Distributed Deployment, on page 175
- Deployment and Node Settings, on page 179
- Logging Settings, on page 187
- Admin Access Settings, on page 189
- Administration Node, on page 192
- Support for Automatic Failover for the Administration Node, on page 200
- Policy Service Node, on page 200
- Monitoring Node, on page 203
- Monitoring Database, on page 207
- Configure MnT Nodes for Automatic Failover, on page 209
- Cisco pxGrid Node, on page 210
- Cisco pxGrid Cloud Overview, on page 216
- View Nodes in a Deployment, on page 223
- Download Endpoint Statistical Data from MnT Nodes, on page 223
- Database Crash or File Corruption Issues, on page 223
- Device Configuration for Monitoring, on page 224
- Synchronize Primary and Secondary Cisco ISE Nodes, on page 224
- Change Node Personas and Services, on page 224
- Effects of Modifying Nodes in Cisco ISE , on page 225
- Create a Policy Service Node Group, on page 225
- Remove a Node from Deployment, on page 226
- Shut Down a Cisco ISE Node, on page 227
- Scenarios In Which Need to Reregister a Node, on page 227
- Change the Hostname or IP Address of a Standalone Cisco ISE Node, on page 228

Cisco ISE Deployment Terminology

The following terms are commonly used when discussing Cisco ISE deployment scenarios:

- Service: A service is a specific feature that a persona provides, such as network access, profiler, posture, security group access, monitoring and troubleshooting, and so on.
- Node: A node is an individual instance that runs the Cisco ISE software. Cisco ISE is available as an appliance and also as a software that can be run on VMware. Each instance (appliance or VMware) that runs the Cisco ISE software is called a node.
- Persona: The persona of a node determines the services provided by the node. A Cisco ISE node can assume any of the following personas: Administration, Policy Service, Monitoring, and pxGrid. The menu options that are available through the Admin portal are dependent on the role and personas that a Cisco ISE node assumes.
- Deployment Model: Determines if your deployment is distributed, standalone, or high availability in standalone, which is a basic two-node deployment.

Personas in Distributed Cisco ISE Deployments

A Cisco ISE node can assume the Administration, Policy Service, or Monitoring personas.

A Cisco ISE node can provide various services based on the persona that it assumes. Each node in a deployment can assume the Administration, Policy Service, and Monitoring personas. In a distributed deployment, you can have the following combination of nodes in your network:

- Primary Policy Administration Node (primary PAN) and secondary Policy Administration Node (secondary PAN) for high availability
- Primary Monitoring Node (primary MnT node) and Secondary Monitoring Node (secondary MnT node) for high availability
- A pair of health check nodes or a single health check node for the primary PAN automatic failover
- One or more Policy Service Nodes (PSNs) for the session failover

Configure a Cisco ISE Node

After you install a Cisco ISE node, all the default services provided by the Administration, Policy Service, and Monitoring personas run on it. This node is in a standalone state. You must log in to the Admin portal of the Cisco ISE node to configure it. You cannot edit the personas or services of a standalone Cisco ISE node. You can, however, edit the personas and services of the primary and secondary Cisco ISE nodes. You must first configure a primary ISE node and then register secondary ISE nodes to the primary ISE node.

If you are logging in to the node for the first time, you must change the default administrator password and install a valid license.

We recommend that you do not change the host name and the domain name configured on Cisco ISE in production. If required, reimage the appliance, make changes, and configure the details during the initial deployment.

Before you begin

You should have a basic understanding of how distributed deployments are set up in Cisco ISE. See Guidelines for Setting Up a Distributed Deployment.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 2 Check the check box next to the Cisco ISE node that you want to configure, and click **Edit**.

Step 3 Enter the values, as required, and click **Save**.

Configure a Primary Policy Administration Node

To set up a distributed deployment, you must first configure a Cisco ISE node as your primary PAN.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

The **Register** button is disabled initially. To enable this button, configure a Primary PAN.

Step 2 Check the check box next to the current node, and click **Edit**.

Step 3 Click **Make Primary** to configure your primary PAN.

Step 4 Click **Save** to save the node configuration.

What to do next

1. Add secondary nodes to your deployment.
2. Enable the profiler service and configure the probes, if required.

Register a Secondary Cisco ISE Node

You can register Cisco ISE nodes to the primary PAN to form a multinode deployment. Nodes in a deployment other than the primary PAN are referred to as secondary nodes. While registering a node, you can select the personas and services that must be enabled on the node. Registered nodes can be managed from the primary PAN (for example, managing the node personas, services, certificates, licenses, applying patches, and so on).

When a node is registered, the primary PAN pushes the configuration data to the secondary node, and the application server on the secondary node restarts. After the complete data replication, further configuration changes done on the primary PAN are replicated to the secondary node. The time taken for the changes to be replicated on the secondary node depends on various factors, such as network latency, load on the system, and so on.

Before you begin

Ensure that the primary PAN and the node being registered are DNS resolvable to each other. If the node that is being registered uses an untrusted self-signed certificate, you are prompted with a certificate warning along with details of the certificate. If you accept the certificate, it is added to the trusted certificate store of the primary PAN to enable TLS communication with the node.

If the node uses a certificate that is not self-signed (for example, signed by an external CA), you must manually import the relevant certificate chain of that node to the trusted certificate store of the primary PAN. When you import the secondary node's certificate to the trusted certificate store, check the **Trust for Authentication**

within ISE check box in the **Trusted Certificates** window for the PAN to validate the secondary node's certificate.

While registering a node with session services enabled (such as Network Access, Guest, Posture, and so on), you can add it to a node group. See Create a Policy Service Node Group, on page 225 for more details.

Step 1 Log in to the primary PAN.

Step 2 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 3 Click **Register** to initiate registration of a secondary node.

Step 4 Enter the DNS-resolvable fully qualified domain name (FQDN) of the standalone node that you are going to register (in the format hostname.domain-name, for example, abc.xyz.com). The FQDN of the primary PAN and the node being registered must be resolvable from each other.

Step 5 Enter the GUI-based administrator credentials for the secondary node in the **Username** and **Password** fields.

Step 6 Click **Next**.

The primary PAN tries to establish TLS communication (for the first time) after the node is registered.

- If the node uses a certificate that is trusted, you can proceed to Step 7.
- If the node uses a self-signed certificate that is not trusted, a certificate warning message is displayed with details about the certificate (such as, Issued-to, Issued-by, Serial number, and so on), which can be verified against the actual certificate on the node. Click the **Import Certificate and Proceed** option to trust this certificate and proceed with registration. Cisco ISE imports the default self-signed certificate of that node to the trusted certificate store of the primary PAN. If you do not want to use the default self-signed certificate, click **Cancel Registration** and manually import the relevant certificate chain of that node to the trusted certificate store of the primary PAN. When you import the secondary node's certificate to the trusted certificate store, check the **Trust for Authentication within ISE** check box adjacent to the corresponding PAN to validate the secondary node's certificate.
- If the node uses a CA-signed certificate, an error message is displayed, stating that the registration cannot proceed until certificate trust is set up.

Step 7 Check the check boxes to select the personas and services to be enabled on the node, and then click **Save**.

When a node is registered, an alarm (which confirms that a node has been added to the deployment) is generated on the primary PAN. You can view this alarm in the **Alarms** dashlet in the Cisco ISE GUI **Dashboard**. After the registered node is synchronized and restarted, you can log in to the secondary node GUI using the same credentials used on the primary PAN.

What to do next

- For time-sensitive tasks such as guest user access and authorization, logging, and so on, ensure that the system time on your nodes is synchronized.
- If you registered a secondary PAN, and are using the internal Cisco ISE CA service, you must back up the Cisco ISE CA certificates and keys from the primary PAN and restore them on the secondary PAN.

Support for Multiple Deployment Scenarios

Cisco ISE can be deployed across an enterprise infrastructure, supporting 802.1X wired, wireless, and Virtual Private Networks (VPNs).

The Cisco ISE architecture supports both standalone and distributed (also known as *high availability* or *redundancy*) deployments, where one machine assumes the primary role, and another *backup* machine assumes the secondary role. Cisco ISE features distinct configurable personas, services, and roles, which allow you to create and apply Cisco ISE services where needed in the network. The result is a comprehensive Cisco ISE deployment that operates as a fully functional and integrated system.

Cisco ISE nodes can be deployed with one or more of the Administration, Monitoring, and Policy Service personas. Each persona performs a different, but vital, part in your overall network policy management topology. Installing Cisco ISE with an administration persona allows you to configure and manage your network from a centralized portal to promote efficiency and ease of use.

Cisco ISE Distributed Deployment

A deployment that has more than one Cisco ISE node is called a distributed deployment. To support failover and to improve performance, you can set up your deployment with multiple Cisco ISE nodes in a distributed fashion. In a Cisco ISE distributed deployment, the administration and monitoring activities are centralized, and processing is distributed across the PSNs. Depending on your performance needs, you can scale your deployment. Each Cisco ISE node in a deployment can assume any of these personas-Administration, Policy Service, and Monitoring.

Cisco ISE Deployment Setup

After you install Cisco ISE on all your nodes, as described in the *Cisco Identity Services Engine Hardware Installation Guide*, the nodes come up in a standalone state. You must then define one node as your primary PAN. While defining your primary PAN, you must enable the administration and monitoring personas on that node. You can optionally enable the policy service persona on the primary PAN. After you complete the task of defining personas on the primary PAN, you can register other secondary nodes to the primary PAN and define personas for the secondary nodes.

All Cisco ISE system and functionality-related configurations should be done only on the primary PAN. The configuration changes that you perform on the primary PAN are replicated to all the secondary nodes in your deployment.

There must be at least one MnT in a distributed deployment. At the time of configuring your primary PAN, you must enable the Monitoring persona. After you register an MnT node in your deployment, you can edit the primary PAN and disable the Monitoring persona, if required.

Data Replication from Primary to Secondary Cisco ISE Nodes

When you register a Cisco ISE node as a secondary node, Cisco ISE immediately creates a data replication channel from the primary to the secondary node and begins the process of replication. Replication is the process of sharing Cisco ISE configuration data from the primary to the secondary nodes. Replication ensures consistency among the configuration data available in all the Cisco ISE nodes that are part of your deployment.

, click the corresponding radio button to enable or disable the replication of the dynamically discovered endpoints across all the nodes in your Cisco ISE deployment:

To enable or disable endpoint replication using OpenAPI, see the Cisco ISE API Reference Guide.

A full replication typically occurs when you first register a Cisco ISE node as a secondary node. Incremental replication occurs after a full replication and ensures that any new changes, such as additions, modifications, or deletions to the configuration data in the PAN are reflected in the secondary nodes. The process of replication ensures that all the Cisco ISE nodes in a deployment are in sync. You can view the status of replication in the **Node Status** column in the **Deployment** window of the Cisco ISE Admin portal. When you register a Cisco ISE node as a secondary node or perform a manual synchronization with the PAN, the node status shows an orange icon, indicating that the requested action is in progress. After the synchronization is complete, the node status turns green, indicating that the secondary node is synchronized with the PAN.

Cisco ISE Node Deregistration

To remove a node from a deployment, you must deregister it. When you deregister a secondary node from the primary PAN, the status of the deregistered node changes to standalone, and the connection between the primary and the secondary node is lost. Replication updates are no longer sent to the deregistered standalone node.

When a PSN is deregistered, the endpoint data is lost. If you want the PSN to retain the endpoint data after it becomes a standalone node, you can do one of the following:

- Obtain a backup from the primary PAN, and when the PSN becomes a standalone node, restore this data backup on it.
- Change the persona of the PSN to administration (secondary PAN), synchronize the data from the **Deployment** window of the Admin portal, and then deregister the node. This node will now have all the data. You can then add a secondary PAN to the existing deployment.

Note You cannot deregister a primary PAN.

Node Status in a Cisco ISE Deployment

Table 8: Cisco ISE Node Status

Node Status	Description	Guidelines
Connected	Node is connected and replication works fine.	-
Replication Stopped	Node is connected but replication has stopped. The node is reachable on ports 443 and 12001. This is a temporary status that will change when the underlying replication issue is resolved.	The underlying issue may resolve by itself. If not, log in to the Cisco ISE GUI and perform a manual synchronization from the **Deployment** window.

Node Status	Description	Guidelines
Node Not Reachable	Node is not reachable on port 443 but replication works fine.	The node may come back up by itself when the underlying issue resolves. If not, log in to the Cisco ISE GUI and perform a manual synchronization from the **Deployment** window.
Disconnected	Node is not reachable and replication has stopped.	This status is set if the node is down for more than five minutes. The node may come back up by itself when the underlying issue resolves. If not, log in to the Cisco ISE GUI and perform a manual synchronization from the **Deployment** window.
Registration failed	Node registration has failed.	Perform a manual synchronization. Deregister and register the affected Cisco ISE node again.
In Progress	Node registration or manual sync is in progress. Currently, the In Progress status has a timeout value of 300 minutes, after which the status changes to: • Connected if registration or manual sync is successful. • Registration Failed if node registration fails. • Not in Sync if manual sync fails.	No action is required if the status changes to Connected. If it changes to Registration Failed or Not in Sync, check the respective rows and perfom the necessary actions.
Not in Sync	Node is not in sync.	Perform a manual synchronization. Deregister and register the affected Cisco ISE node again.
Upgrading	Node upgrade is in progress.	-

Guidelines for Setting Up a Distributed Deployment

Read the following statements carefully before you set up Cisco ISE in a distributed environment:

- Choose a node type for the Cisco ISE server. You must choose a Cisco ISE node for administration, policy service, and monitoring capabilities.
- Choose the same Network Time Protocol (NTP) server for all the nodes. To avoid timezone issues among the nodes, you must provide the same NTP server name when setting up each node. This setting ensures

that the reports and logs from the various nodes in your deployment are always synchronized with timestamps.

- Configure the Cisco ISE administrator password when you install Cisco ISE. The previous Cisco ISE administrator default login credentials (admin/cisco) are no longer valid. Use the username and password that was created during the initial setup, or the current password if it was changed later.
- Configure the DNS server. Enter the IP addresses and fully qualified domain names (FQDNs) of all the Cisco ISE nodes that are part of your distributed deployment in the DNS server. Otherwise, node registration fails.
- Configure the forward and the reverse DNS lookup for all the Cisco ISE nodes in your distributed deployment in the DNS server. Otherwise, you may run into deployment-related issues when registering and restarting Cisco ISE nodes. Performance might be degraded if reverse DNS lookup is not configured for all the nodes.
- (Optional) Deregister a secondary Cisco ISE node from the primary PAN to uninstall Cisco ISE from it.
- Back up the primary MnT, and restore the data to the new secondary MnT. This ensures that the history of the primary MnT is in sync with the new MnT because the new changes are replicated.
- Ensure that the primary PAN and the standalone node that you are about to register as a secondary node are running the same version of Cisco ISE.
- Enable **Internal CA Settings** on your Cisco ISE primary PAN before you add another node to your deployment to ensure that the Cisco ISE certificate services function as expected. To enable Internal CA Settings, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Certificate Authority** > **Internal CA Settings**.
- While adding a new node to the deployment, make sure that the issuer certificate chain of wildcard certificates is part of the trusted certificates of the new node. When the new node is added to the deployment, the wildcard certificates are replicated to the new node.
- When configuring your Cisco ISE deployment to support Cisco TrustSec, or when Cisco ISE is integrated with Cisco Catalyst Center, do not configure a PSN as SXP-only. SXP is an interface between Cisco TrustSec and non-Cisco TrustSec devices. SXP does not communicate with the Cisco TrustSec-enabled network devices.

Menu Options Available on Primary and Secondary Nodes

The menu options that are available in Cisco ISE nodes that are a part of a distributed deployment depend on the personas that are enabled on them. You must perform all administration and monitoring activities through the primary PAN. For other tasks, you must use the secondary nodes. Therefore, the user interface of the secondary nodes provides limited menu options based on the persona that is enabled on them.

If a node assumes more than one persona, for example, the Policy Service persona, and a Monitoring persona with a primary role, the menu options listed for the PSNs and the primary MnT are available on that node.

The following table lists the menu options that are available on the Cisco ISE nodes that assume different personas.

Table 9: Cisco ISE Nodes and Available Menu Options

Cisco ISE Node	Available Menu Options
All Nodes	• View and configure the system time and the NTP server settings. • Install the server certificate and manage certificate signing request. You can perform server certificate operations for all the nodes in the deployment through the primary PAN that centrally manages all the server certificates. **Note** The private keys are not stored in the local database and are not copied from the relevant node. The private keys are stored in the local file system.
Primary Policy Administration node (primary PAN)	All menus and submenus.
Primary Monitoring node (primary MnT node)	• Provides access to monitoring data. **Note** The **Operations** menu can be viewed only from the primary PAN. The **Operations** menu does not appear in the monitoring nodes.
PSNs (Policy Service nodes)	Options to join, leave, and test the Active Directory connection are available. Each PSN must be separately joined to the Active Directory domain. You must first define the domain information and join the PAN to the Active Directory domain. Then, join the other PSNs to the Active Directory domain individually.
Secondary Policy Administration node (secondary PAN)	Option to promote the secondary PAN to primary PAN. **Note** After you have registered the secondary nodes to the primary PAN, while logging in to the Admin portal of any of the secondary nodes, you must use the login credentials of the primary PAN.

Deployment and Node Settings

The **Deployment Nodes** window enables you to configure the Cisco ISE (PAN, PSN, and MnT) nodes and to set up a deployment.

Deployment Nodes List Window

The following table describes the fields in the **Deployment Nodes List** window, which you can use to configure Cisco ISE nodes in a deployment. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Table 10: Deployment Nodes List

Field Name	Usage Guidelines
Hostname	Displays the hostname of the node.

Field Name	Usage Guidelines
Personas	(Only appears if the node type is Cisco ISE) Lists the personas that a Cisco ISE node has assumed, for example, Administration, Policy Service, Monitoring, or pxGrid. For example, **Administration**, **Policy Service**, **Monitoring**, or **pxGrid**.
Role	Indicates the role (primary, secondary, or standalone) that the Administration and Monitoring personas have assumed, if these personas are enabled on this node. The role can be any one or more of the following: • **PRI(A)**: Refers to the primary PAN. • **SEC(A)**: Refers to the secondary PAN. • **PRI(M)**: Refers to the primary MnT. • **SEC(M)**: Refers to the secondary MnT.
Services	(Only appears if the Policy Service persona is enabled) Lists the services that run on this Cisco ISE node. Services can include any one of the following: • **Identity Mapping** • **Session** • **Profiling** • **All**
Node Status	Indicates the status of each Cisco ISE node in a deployment for data replication: • Green (Connected): Indicates that a Cisco ISE node, which is already registered in the deployment, is in sync with the primary PAN. • Red (Disconnected): Indicates that a Cisco ISE node is not reachable, is down, or data replication is not happening. • Orange (In Progress): Indicates that a Cisco ISE node is newly registered with the primary PAN, you have performed a manual sync operation, or the Cisco ISE node is not in sync (out of sync) with the primary PAN. For more information, click the quick view icon for each Cisco ISE node in the **Node Status** column.

Related Topics

Cisco ISE Distributed Deployment, on page 175
Cisco ISE Deployment Terminology, on page 171
Configure a Cisco ISE Node, on page 172
Register a Secondary Cisco ISE Node, on page 173

General Node Settings

The following table describes the fields on the **General Settings** window of a Cisco ISE node. In this window, you can assign a persona to a node and configure the services to be run on it. To view this window, click the

Menu icon (☰) and choose **Administration** > **System** > **Deployment** > **Deployment Node** > **Edit** > **General Settings**.

Table 11: General Node Settings

Field Name	Usage Guidelines
Hostname	Displays the hostname of the Cisco ISE node.
FQDN	Displays the fully qualified domain name of the Cisco ISE node, for example, ise1.cisco.com.
IP Address	Displays the IP address of the Cisco ISE node.
Node Type	Displays the node type.
Personas	
Administration	Enable this toggle button if you want a Cisco ISE node to assume the Administration persona. You can enable the Administration persona only on nodes that are licensed to provide the administrative services. **Role**: Displays the role that the Administration persona has assumed in the deployment. The persona can take one of these values—**Standalone**, **Primary**, or **Secondary**. **Make Primary**: Click this to make this node your primary Cisco ISE node. You can have only one primary Cisco ISE node in a deployment. The other options in this window will become active only after you make this node primary. You can have only two Administration nodes in a deployment. If the node has a **Standalone** role, the **Make Primary** button appears next to it. If the node has a **Secondary** role, the **Promote to Primary** button appears next to it. If the node has a **Primary** role, and there are no other nodes registered with it, the **Make Standalone** button appears next to it. Click the **Make Standalone** button to make your primary node a standalone node.

Field Name	Usage Guidelines
Monitoring	Click this toggle button if you want a Cisco ISE node to assume the Monitoring persona and function as your log collector. There must be at least one Monitoring node in a distributed deployment. At the time of configuring your primary PAN, you must enable the Monitoring persona. After you register a secondary Monitoring node in your deployment, you can edit the primary PAN and disable the Monitoring persona, if required. To configure a Cisco ISE node on a VMware platform as your log collector, use the following guidelines to determine the minimum amount of disk space that you need: 180 KB per endpoint in your network per day and 2.5 MB per Cisco ISE node in your network per day. You can calculate the maximum disk space that you need based on how many months of data you want to have in your Monitoring node. If there is only one Monitoring node in your deployment, it assumes the standalone role. If you have two Monitoring nodes in your deployment, Cisco ISE displays the name of the other Monitoring node too for you to configure the primary-secondary roles. To configure these roles, choose one of the following: • **Primary**: For the current node to be the primary Monitoring node. • **Secondary**: For the current node to be the secondary Monitoring node. • **None**: If you do not want the Monitoring nodes to assume the primary-secondary roles. If you configure one of your Monitoring nodes as primary or secondary, the other Monitoring node automatically becomes the secondary or primary node, respectively. Both the primary and secondary Monitoring nodes receive Administration and Policy Service logs. If you change the role for one Monitoring node to **None**, the role of the other Monitoring node also becomes **None**, thereby cancelling the high availability pair after you designate a node as a Monitoring node. You will find this node listed as a syslog target in the **Remote Logging Targets** window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Remote Logging Targets**.

Field Name	Usage Guidelines
Policy Service	

Field Name	Usage Guidelines
	Click this toggle button to enable any one or all of the following services: • **Enable Session Services**: Check this check box to enable network access, posture, guest, and client-provisioning services. From the **Include Node in Node Group** drop-down list, choose the group to which this Policy Service node belongs. Note that Certificate Authority (CA) and Enrollment over Secure Transport (EST) services can only run on a Policy Service node that has session services enabled on it. For **Include Node in Node Group**, choose **None** if you do not want this Policy Service node to be a part of a group. All the nodes within the same node group should be configured on the network access device (NAD) as RADIUS clients and authorized for CoA, because any one of them can issue a CoA request for the sessions that are established through any node in the node group. If you are not using a load balancer, the nodes in a node group should be the same as, or a subset of the RADIUS servers and clients configured on the NAD. These nodes would also be configured as RADIUS servers. While a single NAD can be configured with many Cisco ISE nodes as RADIUS servers and dynamic-authorization clients, it is not necessary for all the nodes to be in the same node group. The members of a node group should be connected to each other using high-speed LAN connection such as Gigabit Ethernet. The node group members need not be L2 adjacent, but L2 adjacency is highly recommended to ensure sufficient bandwidth and reachability. See the Create a Policy Service Node Group, on page 225 for more details. • **Enable Profiling Service**: Check this check box to enable the Profiling service. If you enable the Profiling service, you must click the **Profiling Configuration** tab and enter the details, as required. When you enable or disable any of the services that run on the Policy Service node or make any changes to this node, you will be restarting the application server processes on which these services run. Expect a delay while these services restart. You can determine when the application server has restarted on a node by using the **show application status ise** command from the CLI. • **Enable Threat-Centric NAC Service**: Check this check box to enable the Threat-Centric Network Access Control (TC-NAC) feature. This feature allows you to create authorization policies based on the threat and vulnerability attributes received from the threat and vulnerability adapters. Threat severity levels and vulnerability assessment results can be used to dynamically control the access level of an endpoint or a user. • **Enable SXP Service**: Check this check box to enable SXP service on the node. You must also specify the interface to be used for SXP service. If you have configured NIC bonding or teaming, the bonded interfaces are also listed along with the physical interfaces in the **Use Interface** drop-down list. • **Enable Device Admin Service**: Check this check box to create TACACS policy sets, policy results, and so on, to control and audit the configuration of network

Field Name	Usage Guidelines
	devices. • **Enable Passive Identity Service**: Check this check box to enable the Identity Mapping feature. This feature enables you to monitor users who are authenticated by a Domain Controller and not by Cisco ISE. In networks where Cisco ISE does not actively authenticate users for network access, you can use the Identity Mapping feature to collect user authentication information from the Active Directory Domain Controller.
pxGrid	Check this check box to enable the pxGrid persona. Cisco pxGrid is used to share the context-sensitive information from the Cisco ISE session directory to other policy network systems such as Cisco Adaptive Security Appliance (ASA). The pxGrid framework can also be used to exchange policy and configuration data between nodes, for example, sharing tags and policy objects between Cisco ISE and third-party vendors, and for non-Cisco ISE-related information exchanges such as threat information.

Related Topics

Personas in Distributed Cisco ISE Deployments, on page 172
Administration Node, on page 192
Policy Service Node, on page 200
Monitoring Node, on page 203
Cisco pxGrid Node, on page 210
Synchronize Primary and Secondary Cisco ISE Nodes, on page 224
Create a Policy Service Node Group, on page 225
Deploy Cisco pxGrid Node, on page 211
Change Node Personas and Services, on page 224
Configure MnT Nodes for Automatic Failover, on page 209

Profiling Node Settings

The following table describes the fields in the **Profiling Configuration** window, that you can use to configure the probes for the profiler service. To access this window, click the **Administration** > **System** > **Deployment** > **ISE Node** > **Edit** > **Profiling Configuration**.

Table 12: Profiling Node Settings

Field Name	Usage Guidelines
NetFlow	Click this toggle button to enable NetFlow for each Cisco ISE node that has assumed the Policy Service persona to receive NetFlow packets sent from the routers. Enter the required values for the following options: • **Interface**: Choose the interface on the Cisco ISE node. • **Port**: Enter the NetFlow listener port number on which NetFlow exports are received from the routers. The default port is 9996.

Field Name	Usage Guidelines
DHCP	Click this toggle button to enable DHCP for each Cisco ISE node that has assumed the Policy Service persona to listen for DHCP packets from the IP helper. Provide values for the following options: • **Interface**: Choose the interface on the Cisco ISE node. • **Port**: Enter the DHCP server UDP port number. The default port is 67.
DHCP SPAN	Click this toggle button to enable DHCP SPAN for each Cisco ISE node that has assumed the Policy Service persona to collect DHCP packets. • **Interface**: Choose the interface on the Cisco ISE node.
HTTP	Click this toggle button to enable HTTP per Cisco ISE node that has assumed the Policy Service persona to receive and parse HTTP packets. • **Interface**: Choose the interface on the Cisco ISE node.
RADIUS	Click this toggle button to enable the RADIUS server for each Cisco ISE node that has assumed the Policy Service persona to collect RADIUS session attributes as well as Cisco Device Protocol (CDP) and Link Layer Discovery Protocol (LLDP) attributes from the Cisco IOS Sensor-enabled devices.
Network Scan (NMAP)	Click this toggle button to enable the NMAP probe.
DNS	Click this toggle button to enable DNS for each Cisco ISE node that has assumed the Policy Service persona to perform a DNS lookup for the FQDN. Enter the **Timeout** period in seconds. **Note** For the DNS probe to work on a particular Cisco ISE node in a distributed deployment, you must enable one of these probes—DHCP, DHCP SPAN, HTTP, RADIUS, or SNMP. For DNS lookup, one of these probes must be started along with the DNS probe.
SNMP Query	Click this toggle button to enable SNMP query for each Cisco ISE node that has assumed the Policy Service persona to poll network devices at specified intervals. Enter values in **Retries**, **Timeout**, **Event Timeout** (mandatory), and **Description** (optional) fields. **Note** In addition to configuring the SNMP Query probe, you must also configure other SNMP settings in **Administration** > **Network Resources** > **Network Devices**. When you configure SNMP settings on the network devices, ensure that you enable CDP and LLDP globally on your network devices.

Field Name	Usage Guidelines
SNMP Trap	Click this toggle button to enable an SNMP Trap probe for each Cisco ISE node that has assumed the Policy Service Persona to receive linkUp, linkDown, and MAC notification traps from the network devices. Provide or enable the following information: • **Link Trap Query**: Enable this toggle button to receive and interpret the notifications received through the SNMP trap. • **MAC Trap Query**: Enable this toggle button to receive and interpret the MAC notifications received through the SNMP trap. • **Interface**: Choose an interface on the Cisco ISE node. • **Port**: Enter the UDP port of the host to use. The default port is 162.
Active Directory	Click this toggle button to scan the defined Active Directory servers for information about Windows users. • **Days before rescan**: Choose the days after which you want the scan to run again.
pxGrid	Click this toggle button to allow Cisco ISE to collect (profile) endpoint attributes over pxGrid.

Related Topics

Cisco ISE Profiling Service, on page 775
Network Probes Used by Profiling Service, on page 778
Configure Profiling Service in Cisco ISE Nodes, on page 778

Logging Settings

The following sections explain how to configure the severity of debug logs, create an external log target, and enable Cisco ISE to send log messages to these external log targets.

Remote Logging Target Settings

The following table describes the fields in the **Remote Logging Targets** window that you can use to create external locations (syslog servers) to store logging messages. To access this window, **Administration** > **System** > **Logging** > **Remote Logging Targets**, and click **Add**.

Table 13: Remote Logging Target Settings

Field Name	Usage Guidelines
Name	Enter a name for the new syslog target.
Target Type	Select the target type from the drop-down list. The default value is **UDP Syslog**.
Description	Enter a brief description of the new target.

Field Name	Usage Guidelines
IP Address	Enter the IP address or hostname of the destination machine that will store the logs. Cisco ISE supports IPv4 and IPv6 formats for logging.
Port	Enter the port number of the destination machine.
Facility Code	Choose the syslog facility code that must be used for logging, from the drop-down list. Valid options are Local0 through Local7.
Maximum Length	Enter the maximum length of the remote log target messages. Valid values are from 200 through 1024 bytes.
Include Alarms For this Target	When you check this check box, alarm messages are sent to the remote server as well.
Comply to RFC 3164	When you check this check box, the delimiters (, ; { } \ \) in the syslog messages sent to the remote servers are not escaped even if a backslash (\) is used.
Buffer Message When Server Down	This check box is displayed when you choose **TCP Syslog** or **Secure Syslog** from the **Target Type** drop-down list. Check this check box to allow Cisco ISE to buffer the syslog messages when a TCP syslog target or secure syslog target is unavailable. Cisco ISE retries sending messages to the target when the connection to the target resumes. After the connection resumes, messages are sent sequentially, starting with the oldest, and proceeding to the newest. Buffered messages are always sent before new messages. If the buffer is full, old messages are discarded.
Buffer Size (MB)	Set the buffer size for each target. By default, it is set to 100 MB. Changing the buffer size clears the buffer, and all the existing buffered messages for the specific target are lost.
Reconnect Timeout (Sec)	Enter the time (in seconds) to configure how long the TCP and secure syslogs are stored for before being discarded when the server is down.
Select CA Certificate	This drop-down list is displayed when you choose **Secure Syslog** from the **Target Type** drop-down list. Choose a client certificate from the drop-down list.
Ignore Server Certificate Validation	This check box is displayed when you choose **Secure Syslog** from the **Target Type** drop-down list. Check this check box for Cisco ISE to ignore server certificate authentication and accept any syslog server. By default, this option is set to Off unless the system is in FIPS mode when this is disabled.

Related Topics

Cisco ISE Logging Mechanism, on page 406
Cisco ISE System Logs, on page 407
Cisco ISE Message Catalogs, on page 409
Collection Filters, on page 410
Event Suppression Bypass Filter, on page 411
Configure Remote Syslog Collection Locations, on page 407
Configure Collection Filters, on page 411

Configure Logging Categories

The following table describes the fields that you can use to configure a logging category. Set a log severity level and choose the logging targets for the logs of a logging category. To access this window, choose **Administration** > **System** > **Logging** > **Logging Categories**.

Click the radio button next to the logging category that you want to view, and click **Edit**. The following table describes the fields that are displayed in the edit window of the logging categories.

Table 14: Logging Category Settings

Field Name	Usage Guidelines
Name	Displays the name of the logging category.
Log Severity Level	For some logging categories, this value is set by default, and you cannot edit it. For some logging categories, you can choose one of the following severity levels from a drop-down list: • **FATAL**: Emergency level. This level means that you cannot use Cisco ISE and you must immediately take the necessary action. • **ERROR**: This level indicates a critical error condition. • **WARN**: This level indicates a normal but significant condition. This is the default level set for many logging categories. • **INFO**: This level indicates an informational message. • **DEBUG**: This level indicates a diagnostic bug message.
Local Logging	Check this check box to enable logging events for a category on the local node.
Targets	This area allows you to choose the targets for a logging category by transferring the targets between the **Available** and the **Selected** areas using the left and right arrow icons. The **Available** area contains the existing logging targets, both local (predefined) and external (user-defined). The **Selected** area, which is initially empty, then displays the targets that have been chosen for the category.

Related Topics

Cisco ISE Message Codes, on page 409
Configure Remote Syslog Collection Locations, on page 407
Set Severity Levels for Message Codes, on page 409

Admin Access Settings

These sections enable you to configure access settings for administrators.

Administrator Password Policy Settings

The following table describes the fields in the **Password Policy** tab that you can use to define a criteria that administrator passwords should meet. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Authentication** > **Password Policy**.

Table 15: Administrator Password Policy Settings

Field Name	Usage Guidelines
Minimum Length	Specify the minimum length of the password (in characters). The default is six characters.
Password must not contain	**Admin name or its characters in reverse order**: Check this check box to restrict the use of the administrator username or its characters in reverse order as the password.
	Cisco or its characters in reverse order: Check this check box to restrict the use of the word "Cisco" or its characters in the reverse order as the password.
	This word or its characters in reverse order: Check this check box to restrict the use of any word that you define or its characters in the reverse order as the password.
	Repeated characters four or more times consecutively: Check this check box to restrict the use of repeated characters four or more times consecutively as the password.
	Dictionary words, their characters in reverse order, or their letters replaced with other characters: Check this check box to restrict the use of dictionary words, their characters in reverse order, or their letters replaced with other characters, as the password. Substitution of $ for s, @ for a, 0 for o, 1 for l, ! for i, 3 for e, and so on, is not permitted. For example, Pa$$w0rd is not permitted. • **Default Dictionary**: Choose this option to use the default Linux dictionary in Cisco ISE. The default dictionary contains approximately 480,000 English words. This option is selected by default. • **Custom Dictionary**: Choose this option to use your customized dictionary. Click **Choose File** to select a custom dictionary file. The text file must comprise newline-delimited (JSON format) words, .dic extension, and a size less than 20 MB.
Password must contain at least one character of each of the selected types	Check the check box for the type of characters an administrator's password must contain. Choose one or more of the following options: • **Lowercase alphabetic characters** • **Uppercase alphabetic characters** • **Numeric characters** • **Non-alphanumeric characters**

Field Name	Usage Guidelines
Password History	Specify the number of previous passwords from which the new password must be different, to prevent the repeated use of the same password. Check the **Password must be different from the previous *n*versions** check box, and enter the number in the corresponding field. Enter the number of days before which you cannot reuse a password. Check the **Cannot reuse password within *n* days** check box, and enter the number in the corresponding field.
Password Lifetime	Check the check boxes for the following options to force users to change passwords after a specified time period: • **Administrator passwords expire *n* days after creation or last change**: Time (in days) before the administrator account is disabled if the password is not changed. The valid range is 1 to 3650 days. • **Send an email reminder to administrators *n* days prior to password expiration**: Time (in days) before which administrators are reminded that their password will expire. The valid range is 1 to 3650 days.
Display Network Device-Sensitive Data	
Require Admin Password	Check this check box if you want the admin user to enter the login password to view network device-sensitive data such as shared secrets and passwords.
Password cached for *n* Minutes	The password that is entered by the admin user is cached for this time period. The admin user will not be prompted to enter the password again during this period to view the network device-sensitive data. The valid range is from 1 to 60 minutes.

Related Topics

Cisco ISE Administrators, on page 15

Create a New Administrator, on page 16

Session Timeout and Session Information Settings

The following table describes the fields in the **Session** window that you can use to define session timeout and terminate an active administrative session. To access this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Settings** > **Session**.

Table 16: Session Timeout and Session Information Settings

Field Name	Usage Guidelines
Session Timeout	
Session Idle Timeout	Enter the time, in minutes, that you want Cisco ISE to wait for, before it logs out the administrator if there is no activity. The default value is 60 minutes. The valid range is from 6 to 100 minutes.
Session Info	

Field Name	Usage Guidelines
Invalidate	Check the check box adjacent to the session ID that you want to terminate and click **Invalidate.**

Related Topics

Administrator Access Settings, on page 367

Configure Session Timeout for Administrators, on page 372

Terminate an Active Administrative Session, on page 372

Administration Node

A Cisco ISE node with the Administration persona allows you to perform all administrative operations on Cisco ISE. It handles all the system-related configurations that are related to functionalities such as authentication, authorization, auditing, and so on. In a distributed environment, you can have a maximum of two nodes running the Administration persona. The Administration persona can take on of these following roles—Standalone, Primary, or Secondary.

High Availability for Administrative Node

In a high-availability configuration, the primary Policy Administration Node (PAN) is in the Active state. The secondary PAN is in the Standby state, which means it receives all configuration updates from the primary PAN, but is not active in the Cisco ISE network.

Cisco ISE supports manual and automatic failover. With automatic failover, when the primary PAN goes down, an automatic promotion of the secondary PAN is initiated. Automatic failover requires a nonadministration secondary node, which is called a health check node. The health check node checks the health of the primary PAN. If the health check node detects that the primary PAN is down or unreachable, it initiates the promotion of the secondary PAN to take over the primary role.

To deploy the Automatic Failover feature, you must have at least three nodes, with two of them assuming the Administration persona, and one acting as the health check node. A health check node is a nonadministration node and can be a PSN, MnT, or pxGrid node, or a combination of these. If the primary and secondary PANs are in different data centers, you must have a health check node for each PAN.

The following table lists the features that are affected when the primary PAN goes down and the secondary PAN is yet to take over.

Table 17: Availability of Features

Feature Name	Available When Primary PAN is Down? (Yes/No)
Existing internal user RADIUS authentication	Yes
Existing or new AD user RADIUS authentication	Yes

Feature Name	Available When Primary PAN is Down? (Yes/No)
Existing endpoint with no profile change	Yes
Existing endpoint with profile change	No
New endpoint learned through profiling.	No
Existing guest: Local Web Authentication (LWA)	Yes
Existing guest: Central Web Authentication (CWA)	Yes (apart from flows enabled for device registration, such as Hotspot, BYOD, and CWA with automatic device registration)
Guest change password	No
Guest: AUP	No
Guest: Max Failed Login Enforcement	No
New Guest (Sponsored or Self-registered)	No
Posture	Yes
BYOD with Internal CA	No
Existing Registered Devices	Yes
MDM on-boarding	No
pxGrid Service	No
Log in to GUI of secondary nodes	Yes (The login process is delayed because a blocking call to the PAN is attempted to update the last login details. Login proceeds after this call times out.)

Note To support certificate provisioning with the internal CA, you must to import the root certificate of the original primary PAN and its key into the new primary node, after promotion. Certificate provisioning does not work after automatic failover for the PSN nodes that are added after the promotion of the secondary node to primary PAN.

High-Availability Health Check Nodes

The health check node for the Primary PAN is called the active health check node. The health check node for the Secondary PAN is called the passive health check node. The active health check node is responsible for checking the status of the Primary PAN, and managing the automatic failover of Administration nodes. We recommend that you use two nonadministrative ISE nodes as health check nodes, one for the Primary PAN and one for the Secondary PAN. If you use only one health check node, and that node goes down, automatic failover will not happen.

When both the PANs are in the same data center, you can use a single nonadministrative ISE node as the health check node for both the Primary PAN and the Secondary PAN. When a single health check node checks the health of both the Primary PAN and the Secondary PAN, it assumes both the active and passive roles.

A health check node is a nonadministration node, which means it can be a Policy Service, Monitoring, or pxGrid node, or a combination of these. We recommend that you designate PSN nodes as health check nodes in the same data center as the Administration nodes. However, in a small or a centralized deployment, where the two Administration nodes are not in the same location (LAN or data center), any node (PSN, pxGrid, or MnT) not having the Administration persona can be used as the health check node.

Note If you chose to not enable automatic failover, and rely on manually promoting the secondary node when the primary PAN fails, you do not need any check nodes.

Health Check Node for the Secondary PAN

The health check node for the Secondary PAN is a passive monitor. It does not take any action until the Secondary PAN has been promoted as the Primary PAN. When the Secondary PAN takes over the primary role, its associated health check node takes the active role for managing automatic failover of Administration nodes. The health check node of the previous Primary PAN becomes the health check node for the Secondary PAN now and monitors it passively.

Disabling and Restarting Health Check

When a node is removed from the health check role or auto failover configuration is disabled, the health check service is stopped on that node. When the auto failover configuration is enabled on the designated high-availability health check node, the node starts checking the health of Administration nodes again. Designating or removing the high-availability health check role of a node does not involve any application restart on that node; only the health check activities are started or stopped.

If the high-availability health check node is restarted, it ignores the previous downtimes of the Primary PAN and starts checking the health status afresh.

Health Check Nodes

The active health check node checks the health status of the primary PAN at a configured polling interval. It sends a request to the primary PAN, and if the response that it receives matches the configuration, the health check node considers the primary PAN to be in good health. If the health of the primary PAN is continuously poor for more than the configured failover period, the health check node initiates failover to the secondary PAN.

If, at any time during a health check, the health status is found to be good after being reported as poor previously within the failover period, the health check node marks the primary PAN status as good, and resets the health check cycle.

The response from the health check of the primary PAN is validated against the configuration values available on its health check node. If the response does not match, it raises an alarm. However, a promotion request is made to the secondary PAN.

Changing Health Nodes

You can change the Cisco ISE node that you are using for a health check, but there are some things to consider.

For example, assume that the health check node (H1) goes out-of-sync, and another node (H2) is made the health check node of the primary PAN. In such a case, after the primary PAN goes down, there is no way for H1 to know that another node (H2) is checking the same primary PAN. Later, if H2 goes down or goes out of the network, an actual failover is required. The secondary PAN, however, retains the right to reject the promotion request. So, after the secondary PAN is promoted to the primary role, a promotion request from H2 is rejected with an error. Even if a health check node for the primary PAN is out of sync, it continues to check the health of the primary PAN.

Automatic Failover to the Secondary PAN

You can configure Cisco ISE to automatically promote the Secondary PAN when the Primary PAN becomes unavailable. The configuration is done on the Primary PAN in the **Deployment** window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**. The failover period is defined as the number of times configured in **Number of Failure Polls Before Failover** times the number of seconds configured in **Polling Interval**. In the default configuration, that time is 10 minutes. Promotion of the Secondary PAN to Primary PAN takes another 10 minutes. So, by default, the total time from Primary PAN failure to secondary PAN working is 20 minutes.

When the Secondary PAN receives the failover call, it carries out the following validations before proceeding with the actual failover:

- The Primary PAN is not available in the network.
- The failover request came from a valid health check node.
- The failover request is for the Secondary PAN.

If all the validations pass, the Secondary PAN promotes itself to the primary role.

The following are some sample (but not limited to) scenarios where automatic failover of the Secondary PAN can be attempted:

- Health of the Primary PAN is consistently not good for the **Number of failure polls before failover** value during the polling period.

- Cisco ISE services on the Primary PAN are manually stopped, and remain stopped for the failover period.
- The Primary PAN is shut down using soft halt or reboot option, and remains shut down for the configured failover period.
- The Primary PAN goes down abruptly (power down), and remains down for the failover period.
- The network interface of the Primary PAN is down (network port shut or network service down), or it is not reachable by the health check node for any other reason, and remains down for the configured failover period.

Health Check Node Restarts

Upon restart, the high-availability health check node ignores the previous downtimes of the Primary PAN and checks the health status afresh.

Bring Your Own Device in Case of Automatic Failover to Secondary PAN

When the Primary PAN is down, authentication is not interrupted for the endpoints that already have certificates issued by the Primary PAN root CA chain. This is because all the nodes in the deployment have the entire certificate chain for trust and validation purposes.

However, until the Secondary PAN is promoted to Primary, new BYOD devices will not be onboarded. BYOD onboarding requires an active Primary PAN.

After the original primary PAN is brought back up or the Secondary PAN is promoted, new BYOD endpoints are onboarded without any issues.

If the Primary PAN that failed can not be rejoined as the Primary PAN, regenerate the root CA certificate on the newly promoted Primary PAN (the original secondary PAN).

For existing certificate chains, triggering a new root CA certificate results in the automatic generation of the subordinate CA certificates. Even when new subordinate certificates are generated, endpoint certificates that were generated by the previous chain continue to be valid.

Sample Scenarios when Automatic Failover is Avoided

The following are some sample scenarios that depict cases where automatic failover by the health check node might be avoided or a promotion request to the secondary node rejected:

- The node receiving the promotion request is not the secondary node.
- The promotion request received by the Secondary PAN does not have the correct Primary PAN information.
- The promotion request is received from an incorrect health check node.
- The promotion request is received, but the Primary PAN is up and in good health.
- The node receiving the promotion request goes out-of-sync.

Functionalities Affected by the PAN Automatic Failover Feature

The following table lists the functionalities that are blocked or require additional configuration changes if the PAN automatic failover configuration is enabled in your deployment.

Functionality	Affected Details
Operations that are Blocked	
Upgrade	Upgrade through the CLI is blocked. By default, this feature is disabled. To deploy the Automatic Failover feature, you must have at least three nodes, where two of the nodes assume the Administration persona, and one node acts as the health check node. (A health check node is a nonadministration node and can be a PSN, MnT, or pxGrid node, or a combination of these). If the PANs are in different data centers, you must have a health check node for each PAN.
Restore of Backup	Restore action through the CLI and user interface is blocked. If the PAN automatic failover configuration was enabled prior to restore, you must reconfigure it after a successful restore.
Change Node Persona	Change of the following node personas through the GUI is blocked: • Administration persona in both the Primary and Secondary PANs • Persona of the PAN • Deregistration of health check node after enabling the PAN Automatic Failover feature
Other CLI Operations	The following admin operations through the CLI is blocked: • Patch installation and rollback • DNS server change • IP address change of eth1, eth2, and eth3 interfaces • Host alias change of eth1, eth2, and eth3 interfaces • Time zone change
Other Administration Portal Operations	The following administrative operations through the GUI is blocked: • Patch installation and rollback • Change of HTTPS certificate • Change of admin authentication type from password-based authentication to certificate-based authentication and vice versa
Users with maximum connected devices cannot connect.	Some session data is stored on the failed PAN, and cannot be updated by the PSN.
Operations that Require PAN Automatic Failover to be Disabled	

Functionality	Affected Details
CLI Operations	The following administrative operations through the CLI display a warning message if the PAN automatic failover configuration is enabled. These operations may trigger automatic failover if a service or system is not restarted within the failover window. Hence, while performing the following operations, we recommend that you to disable the PAN automatic failover configuration: • Manually stopping the Cisco ISE service • Soft reload (reboot) of Cisco ISE using the admin CLI

Configure Primary PAN for Automatic Failover

Before you begin

To deploy the Automatic Failover feature, you must have at least three nodes, of which two nodes assume the Administration persona, and one node acts as the health check node. A health check node is a nonadministration node and can be a PSN, MnT, or pxGrid node, or a combination of these. If the PANs are in different data centers, you must have a health check node for each PAN.

Step 1 Log in to the Primary PAN GUI.

Step 2 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment** > **PAN Failover**.

Step 3 Check the **Enable PAN Auto Failover** check box to enable automatic failover of the primary PAN.

Note You can only promote a Secondary PAN to become the Primary PAN. Cisco ISE nodes that assume only the PSN, MnT, or pxGrid node, or a combination of these, cannot be promoted to become the Primary PAN.

Step 4 Choose the health check node for the primary PAN from the **Primary Health Check Node** drop-down list containing all the available secondary nodes.

We recommend that you have this node in the same location or data center as the primary PAN.

Step 5 Choose the health check node for the secondary PAN, from the **Secondary Health Check Node** drop-down list containing all the available secondary nodes.

We recommend that you have this node in the same location or data center as the secondary PAN.

Step 6 Provide the **Polling Interval** time after which the PAN status is checked. The valid range is 30 to 300 seconds.

Step 7 Provide the count for **Number of Failure Polls before Failover**.

Failover occurs if the status of the PAN is not good for the specified number of failure polls. The valid range is 2 to 60 counts.

Step 8 Click **Save**.

What to do next

After the promotion of the Secondary PAN to the Primary PAN, do the following:

- Manually sync the old Primary PAN to bring it back into the deployment.
- Manually sync any other secondary node that is outof sync, to bring it back into the deployment.

Manually Promote Secondary PAN to Primary

If the Primary PAN fails and you have not configured PAN automatic failover, you must manually promote the Secondary PAN to become the new Primary PAN.

Before you begin

Ensure that you have a second Cisco ISE node configured with the Administration persona to promote as your Primary PAN.

Step 1 Log in to the Secondary PAN GUI.

Step 2 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 3 In the **Edit Node** window, click **Promote to Primary**.

Note You can only promote a secondary PAN to become the primary PAN. Cisco ISE nodes that assume only the Policy Service or Monitoring persona, or both, cannot be promoted to become the primary PAN.

If the node that was originally the Primary PAN, comes back up, it will be demoted automatically and become the Secondary PAN. You must perform a manual synchronization on this node (that was originally the Primary PAN) to bring it back into the deployment.

In the **Edit Node** window of a secondary node, you cannot modify the personas or services because the options are disabled. You have to log in to the Admin portal to make changes.

Step 4 Click **Save**.

Reusing a Node of an Existing Cisco ISE Deployment as a Primary PAN for a New Cisco ISE Deployment

If you want to repurpose a node of an existing Cisco ISE deployment to the primary PAN of a new Cisco ISE deployment you must, perform these steps:

Step 1 Run the Cisco ISE Perform System Erase utility, as described in the *Cisco ISE Installation Guide* for your version of Cisco ISE. This document is available at: https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html

Step 2 Perform a fresh install of Cisco ISE, as described in the *Cisco ISE Installation Guide*.

Step 3 Configure the standalone node as a primary Policy Administration node, as described in Configure a Primary Policy Administration Node, on page 173.

Restoring Service to the Primary PAN

Cisco ISE does not support automatic fallback to the original primary PAN. After the automatic failover to the secondary PAN is initiated, if you bring the original primary PAN back into the network, you should configure it as the secondary PAN.

Support for Automatic Failover for the Administration Node

Cisco ISE supports automatic failover for the Administration persona. To enable the Automatic Failover feature, at least two nodes in your distributed setup should assume the Administration persona and one node should assume the nonadministration persona. If the Primary PAN goes down, an automatic promotion of the Secondary PAN is initiated. For this, a nonadministration secondary node is designated as the health check node for each of the PANs. The health check node checks the health of the primary PAN at configured intervals. If the health check response received for the primary PAN is not good for reasons, such as the device being down or unreachable, the health check node initiates the promotion of the secondary PAN to take over the primary role after waiting for the configured threshold value. Some features are unavailable after automatic failover of the secondary PAN. Cisco ISE does not support fallback to the original primary PAN. See High Availability for Administrative Node.

Policy Service Node

A Policy Service node (PSN) is a Cisco ISE node with the Policy Service persona, and provides network access, posture, guest access, client provisioning, and profiling services.

At least one node in your distributed setup should assume the Policy Service persona. This persona evaluates the policies and makes all the decisions. Typically, there is more than one PSN in a distributed deployment.

All the PSNs that reside in the same high-speed Local Area Network (LAN) or behind a load balancer can be grouped together to form a node group. If one of the nodes in a node group fails, the other nodes detect the failure and reset URL-redirected sessions, if any.

High Availability in Policy Service Nodes

To detect node failure and to reset all URL-redirected sessions on the failed node, two or more PSNs can be placed in the same node group. When a node that belongs to a node group fails, another node in the same node group issues a Change of Authorization (CoA) for all URL-redirected sessions on the failed node.

All the nodes within the same node group should be configured on the network access device (NAD) as RADIUS clients and authorized for CoA, because any one of them can issue a CoA request for the sessions that are established through any node in the node group. If you are not using a load balancer, the nodes in a node group should be the same as, or a subset of, the RADIUS servers and clients configured on the NAD. These nodes should also be configured as RADIUS servers.

Note While a single NAD can be configured with many Cisco ISE nodes as RADIUS servers and dynamicauthorization clients, it is not necessary for all the nodes to be in the same node group.

The members of a node group should be connected to each other using high-speed LAN connection such as Gigabit Ethernet. The node group members need not be L2 adjacent, but L2 adjacency is highly recommended to ensure sufficient bandwidth and reachability. See Create a Policy Service Node Group, on page 225 for more details.

Load Balancer to Distribute Requests Evenly Among PSNs

When you have multiple PSNs in the deployment, you can use a load balancer to distribute the requests evenly. The load balancer distributes the requests to the functional nodes behind it. See Cisco and F5 Deployment Guide: ISE Load Balancing using BIG-IP for more information, and to know about best practices when deploying PSNs behind a load balancer.

Session Failover in Policy Service Nodes

PSNs in a node group share session information. The nodes exchange heartbeat messages to detect node failures. If a node fails, one of its peers from the node group knows which sessions were on the failed PSN, and issues a CoA to disconnect those sessions. Most clients automatically reconnect, and establish a new session.

Some clients don’t automatically reconnect. For example, if a client connects through a VPN, then that client may not see the CoA. Clients that are IP phones, multihost 802.1X ports, or virtual machines may also not see or be able to respond to a CoA. URL-redirected clients (webauth) also can’t connect automatically. Those clients must manually reconnect.

Timing issues can also prevent reconnection, for example, if the posture state is pending at the time of PSN failover.

For more information about PSN session sharing, see Light Data Distribution, on page 201.

Number of Nodes in a Policy Service Node Group

The number of nodes that you can have in a node group depends on your deployment requirements. Node groups ensure that node failures are detected and that a peer issues a CoA for sessions that are authorized, but not yet postured. The size of the node group does not have to be very large.

If the size of the node group increases, the number of messages and heartbeats that are exchanged between the nodes increases significantly. As a result, traffic also increases. Having fewer nodes in a node group helps reduce the traffic and at the same time provides sufficient redundancy to detect PSN failures.

There is no hard limit on the number of PSNs that you can have in a node group cluster.

Light Data Distribution

Light Data Distribution is used to store user session information and replicate it across the PSNs in a deployment, thereby eliminating the need to be dependent on the PAN or MnT nodes for user session details.

Light Data Distribution consists of the following directories:

- RADIUS Session Directory
- Endpoint Owner Directory

In addition, you can configure the following options under **Advanced Settings**:

- **Batch Size**: The session updates can be sent in batches. This value specifies the number of records sent in each batch from a Light Data Distribution instance to the other PSNs in the deployment. If this field is set to 1, the session updates are *not* sent in batches. The default value is 10 records.
- **TTL**: This value specifies the maximum time a session will wait for a batch to complete before updating the Light Data Distribution. The default value is 1000 milliseconds.

In case of connectivity issues between the PSNs, for example, when a PSN is down, the session details are retrieved from the MnT session directory and stored for future use.

Large deployments can hold up to 2,000,000 session records. Small deployments can store 1,000,000 session records. When an accounting stop request is received for a session, the corresponding session data is deleted from all Light Data Distribution instances. When the number of stored records exceeds the maximum limit, the oldest sessions are deleted based on the timestamp.

Note

- If the IPv6 prefix length of a session is less than 128 bits and the interface ID is not specified, the IPv6 prefix is rejected, thereby preventing multiple sessions from having the same key.
- Light Data Distribution uses Cisco ISE messaging services for inter-node communication. Cisco ISE Release 3.0 and later support Certificate Signing Request generation for Cisco ISE Messaging Service. Thus, Cisco ISE Release 3.0 and later have both internal and external CA support for ISE Messaging Service. If you face issues with the Cisco ISE messaging service, you have to regenerate Cisco ISE messaging service certificate.
- 1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Certificate Management** > **Certificate Signing Requests**
  2. In the **Certificate(s) will be used for** section, select **ISE Messaging service**.
  3. Click **Generate ISE messaging service certificate**.

RADIUS Session Directory

The **RADIUS Session Directory** is used to store the user session information and replicate it across the PSNs in a deployment. This directory stores only the session attributes that are required for CoA.

This functionality is enabled by default from Cisco ISE Release 2.7. You can enable or disable this functionality, by checking or unchecking the **RADIUS Session Directory** check box in the **Light Data Distribution** window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Light Data Distribution**.

Endpoint Owner Directory

Until Cisco ISE Release 2.6, when an endpoint probe is received on a Policy Service node (PSN) that is different from the one that originally handled the requests for that specific endpoint, the endpoint owner is changed to the new PSN. This results in endpoint ownership flapping.

From Cisco ISE Release 2.7, the **Endpoint Owner Directory** is used to store the PSN FQDN of each MAC address connecting to Cisco ISE and to replicate this data across the PSNs in a deployment. This avoids endpoint ownership flapping because all the PSNs are now aware of all the endpoint owners. The endpoint ownership now changes only in case of a successful RADIUS authentication of that endpoint on another PSN.

In addition, the static endpoint assignments are prioritized over the attributes received by an incoming probe for the same endpoint, avoiding attribute override issues.

This feature is enabled by default from Cisco ISE Release 2.7. If required, you can disable it to fall back to the old mechanism of not using the endpoint owner directory. The **Endpoint Owner Directory** is also used in profiling, and disabling this option will use the legacy profiler owner's directory. You can enable or disable this feature by checking or unchecking the **Enable Endpoint Owner Directory** check box in the **Light Data Distribution** window. (To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Light Data Distribution**).

Monitoring Node

A Cisco ISE node with the Monitoring persona functions as the log collector and stores log messages from the PANs and PSNs in your network. This persona provides advanced monitoring and troubleshooting tools that you can use to effectively manage your network and resources. A node with this persona aggregates and correlates the data that it collects to provide you with meaningful information in the form of reports.

Cisco ISE allows you to have a maximum of two nodes with this persona that can take on primary or secondary roles for high availability. Both the primary and secondary MnT nodes collect log messages. If the primary MnT goes down, the primary PAN points to the secondary node to gather monitoring data. But the secondary node will not be promoted to primary automatically. This should be done by following the procedure described in Manually Modify the MnT Role.

At least one node in your distributed setup should assume the Monitoring persona. We recommend that you do not have the Monitoring and Policy Service personas enabled on the same Cisco ISE node, and that the node be dedicated solely to monitoring, for optimum performance.

You can access the Monitoring menu from the PAN in your deployment.

Note If you have enabled pxGrid, you must create a new certificate for the pxGrid node. Create the certificate template with digital signature usage and generate a new PxGrid certificate.

Manually Modify the MnT Role

You can manually modify MnT roles (both from primary to secondary and from secondary to primary) from the primary PAN.

Step 1 Log in to the primary PAN GUI.

Step 2 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 3 From the list of nodes, check the check box next to the MnT node for which you want to change the role.

Step 4 Click **Edit**.

Step 5 In the **Monitoring** section, change the role to **Primary** or **Secondary**.

You can enable the **Dedicated MnT** option if you want to disable all the other personas and services enabled on that node. When this option is enabled, the configuration data replication process is stopped on that node. This helps to improve the performance of the MnT node. When you disable this option, manual synchronization is triggered.

Step 6 Click **Save**.

Syslog over Cisco ISE Messaging Service

Cisco ISE, Release 2.6, offers MnT WAN survivability for the default, built-in UDP syslog collection targets, LogCollector and LogCollector2. This survivability can be enabled by the option **Use "ISE Messaging Service" for UDP Syslogs delivery to MnT** (In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **System** > **Logging** > **Log Settings**). After you enable this option, the UDP syslogs are protected by Transport Layer Security (TLS).

The **Use "ISE Messaging Service" for UDP Syslogs delivery to MnT** option is disabled by default in Cisco ISE, Release 2.6, First Customer Ship (FCS). This option is enabled by default in Cisco ISE, Release 2.6, Cumulative Patch 2 and later releases.

Using the Cisco ISE messaging service for UDP syslogs retains the operational data for a finite duration even when the MnT node is unreachable. The MnT WAN survivability period is approximately 2 hours and 30 mins.

This service uses TCP port 8671. Please configure your network accordingly and allow the connections to TCP port 8671 on each Cisco ISE node from all other Cisco ISE nodes in the deployment.

Note If your deployment uses TCP or secure syslogs for Cisco ISE deployment, the functionality remains same as the earlier releases.

We recommend defining the UDP syslog target using the IP address. This avoids the latencies encountered while defining UDP syslog targets using the DNS name or DNS server.

Queue Link Alarm

The Cisco ISE messaging service uses a different certificate, signed by the internal CA chain. You will get a `queue-link alarm` message in the **Alarms** dashlet in the Cisco ISE GUI dashboard. Ensure that the following are in place to resolve the alarm:

- All the nodes are connected and synced.
- All the nodes and Cisco ISE messaging services are functional.
- The Cisco ISE messaging services ports are not blocked by external entities such as firewalls.
- The Cisco ISE messaging certificate chain on each node is not broken, and the state of the certificate is good.

If the prerequisites listed above are met, the queue-link alarm might be triggered due to the upgrade process.

To resolve the queue link alarm, regenerate the Cisco ISE root CA chain:

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Certificate Management** > **Certificate Signing Requests**.

2. Click **Generate Certificate Signing Request (CSR)** and then select the **ISE Root CA** in the **Certificate(s) will be used for** drop-down list.
3. Click **Replace ISE root CA Certificate Chain**.

A **Queue Link Error** alarm is generated in the following scenarios:

- Timeout: A **Queue Link Error** alarm with the cause as **Timeout** occurs when there is a network issue between two nodes in the Cisco ISE deployment. Check the connectivity on port 8671 to troubleshoot this error.
- Unknown CA: A **Queue Link Error** alarm with the cause as **Unknown CA** occurs when when there is a broken Cisco ISE Messaging Certificate present in the **System Certificates** window (To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **System Certificates**.) This issue can be resolved by regenerating the Cisco ISE Messaging Certificate by choosing **Administration** > **System** > **Certificates** > **Certificate Management** > **Certificate Signing Requests** and then clicking on **Generate Certificate Signing Request (CSR)** on the Cisco ISE GUI.

Note Regeneration is not required if you have already replaced the Cisco ISE root CA certificate chain.

When you replace the Cisco ISE Root CA chain, the Cisco ISE Messaging Service certificate is also replaced. This is followed by the restart of the Cisco ISE Messaging service with a downtime of about two minutes. The syslogs are lost during this downtime. To avoid losing the syslogs during the downtime, the Cisco ISE Messaging Service can be disabled for a short period.

To enable or disable the Cisco ISE messaging service for UDP syslogs delivery to MnT, perform this procedure:

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **System** > **Logging** > **Log Settings**.

Step 2 Check or uncheck the **Use “ISE Messaging Service” for UDP Syslogs delivery to MnT** check box to enable or disable the use of the Cisco ISE Messaging Service.

Step 3 Click **Save**.

Cisco ISE Community Resource

For more information about the Queue Link alarm, see Queue Link Error.

Automatic Failover in MnT Nodes

MnT nodes do not offer high availablity, but do offer active standby. The PSN copies operational audit data to both the primary and secondary MnT nodes.

Automatic Failover Process

When a primary MnT node goes down, the secondary MnT node takes over all the monitoring and troubleshooting information.

To manually convert the secondary node to a primary node, see Manually Modify the MnT Role. If the primary node comes up again after the secondary node is promoted, the primary node takes on the secondary role. If the secondary node is not promoted, the primary MnT node resumes the primary role after it comes up again.

Caution When the primary node comes back up after a failover, back up of the secondary and restore the data to update the primary node.

Guidelines for Setting Up an Active Standby Pair of MnT Nodes

You can specify two MnT nodes on a Cisco ISE network, and configure them to be an active standby pair. We recommend that you back up the primary MnT node, and restore the data to the new secondary MnT node. This ensures that the history of the primary MnT node is synchronized with the new secondary node because the primary replicates new data. The following rules apply to an active standby pair:

- All changes are logged to the primary MnT node. The secondary node is read-only.
- Changes made to the primary node are automatically replicated on the secondary node
- Both the primary and secondary nodes are listed as log collectors, to which all other nodes send logs.
- The Cisco ISE dashboard is the main entry point for monitoring and troubleshooting. Monitoring information is displayed on the dashboard from the PAN . If the primary node goes down, monitoring information is available on the secondary node.
- Backing up and purging MnT data is not a part of a standard Cisco ISE node backup process. You must configure repositories for backup and data purging on both the primary and secondary MnT nodes, and use the same repositories for each.

MnT Node Failover Scenarios

The following scenarios apply to the active-standby or single-node configurations corresponding to the MnT nodes:

- In an active-standby configuration of the MnT nodes, the primary PAN always points to the primary MnT node to collect the monitoring data. After the primary MnT node fails, the PAN points to the standby MnT node. The failover from the primary node to the secondary node takes place after it is down for more than five minutes.

  However, after the primary node fails, the secondary node does not become the primary node. If the primary node comes up, the PAN starts collecting the monitoring data again from the resumed primary node.
- If the primary MnT node is down, and you want to promote the standby MnT node to active status, you can do so by following the procedure provided in Manually Modify the MnT Role or by deregistering the existing primary MnT node. When you deregister the existing primary MnT node, the standby node becomes the primary MnT node, and the PAN automatically points to the newly promoted primary node.
- In an active-standby pair, if you deregister the secondary MnT node, or if the secondary MnT node goes down, the existing primary MnT node remains the current primary node.
- If there is only one MnT node in the Cisco ISE deployment, then that node acts as the primary MnT node, and provides monitoring data to the PAN. However, when you register a new MnT node, and make

it the primary node in the deployment, the existing primary MnT node automatically becomes the standby node. The PAN points to the newly registered primary MnT node to collect monitoring data.

Monitoring Database

The rate and amount of data that is utilized by the monitoring functions requires a separate database on a dedicated node that is used for these purposes.

Like PSN, the MnT node has a dedicated database that requires you to perform maintenance tasks, as described in the topics covered in this section.

Back Up and Restore the Monitoring Database

The Monitoring database handles large volumes of data. Over time, the performance and efficiency of the MnT node depends on how well you manage that data. To increase efficiency, we recommend that you back up the data and transfer it to a remote repository on a regular basis. You can automate this task by scheduling automatic backups.

Note You should not perform a backup when a purge operation is in progress. If you start a backup during a purge operation, the purge operation stops or fails.

If you register a secondary MnT node, we recommend that you first back up the primary MnT node and then restore the data to the new secondary MnT node. This ensures that the history of the primary MnT node is in sync with the new secondary node when the new changes are replicated.

Monitoring Database Purge

The purging process allows you to manage the size of the Monitoring database by specifying the number of months to retain the data during a purge. The default is three months. This value is utilized when the disk space usage threshold for purging (80 percentage of the total disk space) is met. For this option, each month consists of 30 days. A default of three months equals 90 days.

Guidelines for Purging the Monitoring Database

Follow these guidelines for optimal Monitoring database disk usage:

- If the Monitoring database disk usage is greater than 80 percent of the threshold setting, that is 60 percent of total disk space, a critical alarm is generated, indicating that the database size is about to exceed the maximum amount of allocated disk size. If the disk usage is greater than 90 percent of the threshold setting, that is 70 percent of total disk space, another alarm is generated, indicating that the database size has exceeded the maximum amount of allocated disk size.

  A purge process runs, creating a status history report that you can view in the **Data Purging Audit** window. To view this window, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Reports** > **Audit** > **Data Purging Audit**. An information (INFO) alarm is generated after the purge is completed.

- Purging is also based on the percentage of consumed disk space for the database. When the consumed disk space for the Monitoring database is equal to or exceeds the threshold (the default is 80 percentage of the total disk space), the purge process starts. This process deletes only the oldest seven days' monitoring data, irrespective of what is configured in the Admin portal. It continues this process in a loop until the disk space is below 80 percent. Purging always checks the Monitoring database disk space limit before proceeding.

Operational Data Purging

Cisco ISE Monitoring Operational database contains information that is generated as Cisco ISE reports. Recent Cisco ISE (Cisco ISE Release 2.4 and above) releases have options to purge the monitoring operational data and reset the monitoring database when the **application configure ise** command is run.

The purge option is used to clean up the data and prompts you to enter the number of days for which to retain the data. The reset option is used to reset the database to the factory default, so that all the data that is backed up is permanently deleted. Specify the database if the files are consuming too much file system space.

Note The reset option causes Cisco ISE services to be temporarily unavailable.

The **Operational Data Purging** window contains the **Database Utilization** and **Purge Data Now** areas. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Maintenance** > **Operational Data Purging**. You can view the total available database space and the RADIUS and TACACS data stored in the **Database Utilization** area. Hover the mouse over the status bar to display the available disk space and the number of days the existing data is stored for in the database. Specify the period for which the RADIUS and TACACS data is supposed to be retained in the **Data Retention Period** area. Data is purged at 4 a.m. every day, and you can configure the export of data to a repository before it is purged, by specifying the number of retention days. Check the **Enable Export Repository** check box to select and create a repository, and specify an **Encryption Key**.

In the **Purge Data Now** area, you can purge all the RADIUS and TACACS data or specify the number of days beyond which data is supposed to be purged.

Note You must export RADIUS authentication and accounting, TACACS authorization and accounting, RADIUS errors, and misconfigured supplicants tables to a repository before purging.

Related Topics

Purge Older Operational Data, on page 208

Purge Older Operational Data

The operational data is collected in the server over a period of time. It can be purged either instantly or periodically. You can verify the success of the data purge by viewing the **Data Purging Audit** report.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Maintenance** > **Operational Data Purging**.

Step 2 Do one of the following:

- In the **Data Retention Period** area:
  a. Specify the time period, in days, for which RADIUS and TACACS data should be retained. All the data prior to the specified time period is exported to a repository.
  b. In the **Repository** area, check the **Enable Export Repository** check box to choose the repository to save data.
  c. In the **Encryption Key** field, enter the required password.
  d. Click **Save**.

     Note If the configured retention period is less than the existing retention thresholds corresponding to the diagnostics data, the configured value overrides the existing threshold values. For example, if you configure the retention period as three day,s and this value is less than the existing thresholds in the diagnostics tables (for example, a default of five days), the data is purged according to the value that you configure (three days) in this window.

- In the **Purge Data Now** area:
  a. Choose to purge all the data or to purge the data that is older than the specified number of days. Data is not saved in any repository.
  b. Click **Purge**.

Configure MnT Nodes for Automatic Failover

If you have two MnT nodes in a deployment, you can configure a primary-secondary pair for automatic failover to avoid downtime in the Cisco ISE Monitoring service. A primary-secondary pair ensures that a secondary MnT node automatically provides monitoring if the primary node fails.

Before you begin

- Before you configure MnT nodes for automatic failover, they must be registered as Cisco ISE nodes.
- Configure monitoring roles and services on both the nodes and name them for their primary and secondary roles, as appropriate.
- Configure repositories for backup and data purging on both the primary and secondary MnT nodes. For the backup and purging features to work properly, use the same repositories for both the nodes. Purging takes place on both the primary and secondary nodes of a redundant pair. For example, if the primary MnT node uses two repositories for backup and purging, you must specify the same repositories for the secondary node.

  Configure a data repository for a MnT node using the **repository** command in the system CLI.

Note For scheduled backup and purge to work properly on the nodes of a monitoring redundant pair, configure the same repository, or repositories, on both the primary and secondary nodes using the CLI. The repositories are not automatically synced between the two nodes.

From the Cisco ISE dashboard, verify that the MnT nodes are ready. The **System Summary** dashlet shows the MnT nodes with a green check mark to the left when their services are ready.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 2 In the **Deployment Nodes** window, check the check box next to the MnT node that you want to specify as primary, and click **Edit**.

Step 3 Click the **General Settings** tab and choose **Primary** from the **Role** drop-down list.

When you choose an MnT node as primary, the other MnT node automatically becomes secondary. In the case of a standalone deployment, primary and secondary role configuration is disabled.

Step 4 Click **Save**. Both the primary and secondary nodes restart.

Cisco pxGrid Node

You can use Cisco pxGrid to share the context-sensitive information from Cisco ISE session directory with other network systems such as Cisco ISE ecosystem, partner systems, and other Cisco platforms. The pxGrid framework can also be used to exchange policy and configuration data between nodes, such as sharing tags and policy objects between Cisco ISE and third-party vendors, and for other information exchanges. Cisco pxGrid also allows third-party systems to invoke adaptive network control actions (ANC) to quarantine users or devices or both in response to a network or security event. Cisco TrustSec information, such as tag definition, value, and description can be passed from Cisco ISE through the Cisco TrustSec topic to other networks. The endpoint profiles with Fully Qualified Names (FQNs) can be passed from Cisco ISE to other networks through an endpoint profile meta topic. Cisco pxGrid also supports bulk download of tags and endpoint profiles.

You can publish and subscribe to SXP bindings (IP-SGT mappings) through Cisco pxGrid. For more information about SXP bindings, see Security Group Tag Exchange Protocol .

The following logs are available for the Cisco pxGrid node:

- pxgrid.log: Provides state change notifications.
- pxgrid-cm.log: Displays updates on publisher or subscriber or both and data exchange activity between the client and the server.
- pxgrid-controller.log: Displays the details of client capabilities, groups, and client authorization.
- pxgrid-jabberd.log: Displays all the logs related to system state and authentication.
- pxgrid-pubsub.log: Displays all the information related to publisher and subscriber events.

Note

- You can enable Cisco pxGrid and Cisco pxGrid persona with the Cisco ISE Advantage license.
- Cisco pxGrid should be defined in order to work with the Passive ID Work Center. For more information, see PassiveID Work Center , on page 683

High Availability for pxGrid 2.0

pxGrid 2.0 nodes operate in an Active/Active configuration. For high availability, there should be at least two pxGrid nodes in the deployment. Large deployments can have up to four nodes for increased scale and redundancy. We recommend that you configure IP addresses for all the nodes, so that if one node goes down, that node's clients connect to the working node. When the PAN goes down, the pxGrid server stops handling the activations. Manually promote the PAN to activate the pxGrid server. For more information about pxGrid deployments, see **Performance and Scalability Guide for Cisco Identity Services Engine**

All the pxGrid service provider clients periodically reregister themselves with the pxGrid controller within a span of 7.5 minutes. If the client does not reregister, the PAN node assumes that the client is inactive and deletes the client. If the PAN node goes down for more than 7.5 minutes, when it comes back up, it deletes all the clients with timestamp values older than 7.5 minutes. All those clients must then register again with the pxGrid controller.

pxGrid 2.0 clients use WebSocket and REST-based APIs for pub/sub and query. These APIs are served by the ISE application server on port 8910. The pxGrid processes shown by `show logging application pxgrid` don’t apply to pxGrid 2.0.

Note All the references to pxGrid 1.0 processes in the GUI and the CLI have been removed.

Deploy Cisco pxGrid Node

You can enable Cisco pxGrid persona both on a standalone node and distributed deployment node.

Before you begin

- You must have a Cisco ISE Advantage license to enable the Cisco pxGrid persona. For licensing requirements, see ISE Licensing / Ordering.
- All nodes use the CA certificate for Cisco pxGrid service usage. If you used the default certificate for Cisco pxGrid service before the upgrade, the upgrade replaces that certificate with the internal CA certificate.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 2 In the **Deployment Nodes** window, check the check box next to the node for which you want to enable the Cisco pxGrid services, and click **Edit**.

Step 3 Click the **General Settings** tab and enable the **pxGrid** toggle button.

Step 4 Click **Save**.

Note When you upgrade from the previous version, the **Save** option might be disabled. This happens when the browser cache refers to the old files from the previous version of Cisco ISE. Clear the browser cache to enable the **Save** option.

Configure Cisco pxGrid Settings

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **pxGrid Services** > **Settings**.

Step 2 Check one of the following check boxes based on your requirements:

- **Automatically approve new certificate-based accounts**: Check this check box to automatically approve the connection requests from new Cisco pxGrid clients.
- **Allow password-based account creation**: Check this check box to enable username or password-based authentication for Cisco pxGrid clients. When this option is enabled, Cisco pxGrid clients cannot be automatically approved.

Step 3 Click **Save**.

Use the **Test** option in the Cisco pxGrid **Settings** window to run a health check on the Cisco pxGrid node. View the details in the pxgrid or pxgrid-test.log file.

Use the **PxGrid Client Auto Approval** API to:

- Enable automatic approval of certificate-based connection requests from new pxGrid clients. Enable this option only when you trust all the clients in your environment.
- Enable username or password-based authentication for the pxGrid clients. When this option is enabled, pxGrid clients cannot be automatically approved. A pxGrid client can register itself with the pxGrid controller by sending the username through a REST API. The pxGrid controller generates a password for the pxGrid client during client registration. An administrator can approve or deny the connection request.

For more information about the PxGrid Client Auto Approval API, see the “pxGrid Settings” section in the ERS SDK. You can access the ERS SDK at the following URL:

https://<*ISE-Admin-Node*>:9060/ers/sdk

Only users with ERS Admin role can access the ERS SDK.

Generate Cisco pxGrid Certificate

Before you begin

- You must not use the same certificate for Cisco ISE pxGrid server and pxGrid clients. You must use client certificates for the pxGrid clients. To generate client certificates, choose **Administration > System > Certificates**.
- Some versions of Cisco ISE have a certificate for Cisco pxGrid that uses NetscapeCertType. We recommend that you generate a new certificate.
- To perform the following task, you must be a Super Admin or System Admin.
- A Cisco pxGrid certificate must be generated from the primary PAN.
- If the Cisco pxGrid certificate uses the subject alternative name (SAN) extension, be sure to include the FQDN of the subject identity as a DNS name entry.
- Create a certificate template with digital signature usage and use that to generate a new Cisco pxGrid certificate.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **pxGrid Services** > **Client Management** > **Certificates**.

Step 2 From the **I want to** drop-down list, choose one of the following options:

- **Generate a single certificate (without a certificate signing request)**: You must enter the Common Name (CN) if you select this option.
- **Generate a single certificate (with a certificate signing request)**: You must enter the Certificate Signing Request details if you select this option.

Step 3 (Optional) Enter a description for this certificate.

Step 4 Click the **pxGrid_Certificate_Template** link to download and edit the certificate template based on your requirements.

Step 5 Enter the **Subject Alternative Name (SAN)**. You can add multiple SANs. The following options are available:

- **IP address**: Enter the IP address of the Cisco pxGrid client to be associated with the certificate.
- **FQDN**: Enter the FQDN of the pxGrid client.

Step 6 From the **Certificate Download Format** drop-down list, choose one of the following options:

- **Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)**: The root certificate, the intermediate CA certificates, and the end entity certificate are represented in the PEM format. PEM-formatted certificates are BASE64-encoded ASCII files. Each certificate starts with the `"--------BEGIN CERTIFICATE-----"` tag and ends with the `"-------END CERTIFICATE----"` tag. The end entity’s private key is stored using PKCS* PEM. It starts with the `"-----BEGIN ENCRYPTED PRIVATE KEY----"` tag and ends with the `"-----END ENCRYPTED PRIVATE KEY----"` tag.
- **PKCS12 format (including certificate chain; one file for both the certificate chain and key)**: A binary format to store the root CA certificate, the intermediate CA certificate, and the end entity's certificate and private key in one encrypted file.

Step 7 Enter the password for the certificate.

Step 8 Click **Create**.

You can view the certificate that you created in the **Issued Certificates** window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Certificate Authority** > **Issued Certificates**.

Note From Cisco ISE 2.4 patch 13 onwards, the certificate requirements have become stricter for the pxGrid service. If you are using the Cisco ISE default self-signed certificate as the pxGrid certificate, Cisco ISE might reject that certificate after applying Cisco ISE 2.4 patch 13 or later. This is because the earlier versions of that certificate have the **Netscape Cert Type** extension specified as **SSL Server**, which now fails (a client certificate is also required now).

Any client with a noncompliant certificate fails to integrate with Cisco ISE. Use a certificate issued by the internal CA, or generate a new certificate with proper usage extensions:

- The **Key Usage** extension in the certificate must contain the **Digital Signature** and **Key Encipherment** fields.
- The **Extended Key Usage** extension in the certificate must contain the **Client Authentication** and **Server Authentication** fields.
- The **Netscape Certificate Type** extension is not required. If you want to include that extension, add both **SSL Client** and **SSL Server** in the extension.
- If you are using a self-signed certificate, the **Basic Constraints CA** field must be set to **True**, and the **Key Usage** extension must contain the **Key Cert Sign** field.

Control Permissions for Cisco pxGrid Clients

You can create Cisco pxGrid authorization rules for controlling the permissions for the Cisco pxGrid clients. Use these rules to control the services that are provided to the Cisco pxGrid clients.

You can create different types of groups and map the services provided to the Cisco pxGrid clients to these groups. Use the **Groups** option in the **Client Management** window to add new groups. You can view the example authorization rules in the **Client Management** > **Policies** window. Note that you can update only the **Custom Operations** field for the predefined rules.

To create an authorization rule for pxGrid clients:

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **pxGrid Services** > **Client Management** > **Policy**.

Step 2 From the **Service** drop-down list, choose one of the following options:

- **com.cisco.ise.pubsub**
- **com.cisco.ise.config.anc**
- **com.cisco.ise.config.profiler**
- **com.cisco.ise.config.trustsec**
- **com.cisco.ise.service**

- **com.cisco.ise.system**
- **com.cisco.ise.radius**
- **com.cisco.ise.sxp**
- **com.cisco.ise.trustsec**
- **com.cisco.ise.mdm**

Step 3 From the **Operation** drop-down list, choose one of the following options:

- **<ANY>**
- **publish**
- **publish /topic/com.cisco.ise.session**
- **publish /topic/com.cisco.ise.session.group**
- **publish /topic/com.cisco.ise.anc**
- **<CUSTOM>**: You can specify a custom operation if you select this option.

See pxGrid Operations and Services Use Cases for more information.

Note The following additional attributes are published to the /topic/com.cisco.ise.session for REST ID store for Cisco ISE 3.0 patch 5 and later releases:

- identityProvider:Azure
- oid
- tenantID
- preferredUsername

Step 4 From the **Groups** drop-down list, choose the groups that you want to map to this service.

ANC and manually added groups are listed in this drop-down list.

Note Only the clients that belong to the groups included in the policy can subscribe to the service specified in that policy. For example, if you define a pxGrid policy for com.cisco.ise.pubsub service and assign the ANC group to this policy, only the clients that belong to the ANC group can subscribe to the com.cisco.ise.pubsub service.

pxGrid Operations and Services Use Cases

When creating a new pxGrid policy, note that some pxGrid operations are only applicable to specific services.

You can find the following pxGrid operations in the Cisco ISE GUI.

Operation <ANY>

When you use the <ANY> operation with a service and a particular user group, any operation related to that service is only accessible to the users in the chosen user group.

Consider the following example.

Service: com.cisco.ise.session; Operation: <ANY>; Groups: SessionUsers.

In this example, only pxGrid clients that are part of the ‘SessionUsers’ group will be able to perform any operation related to session topic (like subscribe/gets operations).

Operation publish

All the publish related operations are applicable only when com.cisco.ise.pubsub is chosen as the service. You can use the publish operation to create a pxGrid policy specifying that only a pxGrid client of a particular user group can publish a chosen topic or can publish all topics.

Operation <Custom>

You can use the <Custom> operation to specify an operation that is not provided in the Operation drop-down list. Currently, pxGrid supports the following operations but not all of them are listed in the Operation drop-down list:

1. 'sets' (applicable on all services and topics except pubsub) – You can use this to restrict access to REST API calls that perform a set operation.
2. 'gets' (applicable on all services and topics except pubsub) – You can use this to restrict access to REST API calls that perform a get operation.
3. 'publish' followed by a particular topic name (only applicable on pubsub service) – You can use this to restrict access to users who can publish a particular topic.

   For example, Service: com.cisco.ise.pubsub, Operation: publish/topic/com.cisco.ise.session.

   However, some rules with the same operation, service, and topic are incomprehensible and must be avoided. For example, Service: com.cisco.ise.session, Operation: publish /topic/com.cisco.ise.session.
4. subscribe' followed by topic name (only applicable on pubsub service) – You can use this to restrict access to users who can subscribe to a particular topic.

   For example, Service: com.cisco.ise.pubsub, Operation: publish /topic/com.cisco.ise.session

Cisco pxGrid Cloud Overview

Cisco pxGrid Cloud is a new Cisco cloud offer that extends pxGrid, ERS, and Open API access to cloud-based applications. Cisco ISE 3.1 patch 3 and later releases support Cisco pxGrid Cloud.

To allow connectivity between a Cisco ISE deployment and Cisco pxGrid Cloud, the **pxGrid Cloud** option must be enabled on one or more pxGrid nodes in the Cisco ISE deployment. If you have configured high availability for pxGrid nodes, one of the nodes acts as the Active node and the other one will be the Standby node. The Standby node takes over when the Active node goes down.

Only the Active node establishes connection to Cisco pxGrid Cloud and handles the traffic between the Cisco ISE deployment and Cisco pxGrid Cloud. No other Cisco ISE node interacts with Cisco pxGrid Cloud.

The pxGrid Cloud agent resides in Cisco ISE and serves as the bridge between Cisco ISE and Cisco pxGrid Cloud. A pxGrid Cloud application can subscribe to a pxGrid topic. The pxGrid Cloud agent in Cisco ISE learns about this subscription from Cisco pxGrid Cloud and establishes the actual subscription to the pxGrid service in Cisco ISE. When the agent receives a notification on the pxGrid topic, it forwards the notification to Cisco pxGrid Cloud over a logical channel dedicated to the pxGrid service. The pxGrid Cloud application can invoke pxGrid, ERS, and Open APIs in the Cisco ISE deployment. The pxGrid Cloud agent proxies a REST request from Cisco pxGrid Cloud to Cisco ISE, and returns the response back to Cisco pxGrid Cloud.

Cisco, its partners, and its customers can develop pxGrid Cloud-based applications and register them with the pxGrid Cloud offer. These applications use the pxGrid, ERS, and Open APIs to exchange information with Cisco ISE.

Cisco ISE customers who have a pxGrid Cloud subscription can register their Cisco ISE deployment with Cisco pxGrid Cloud and use the applications listed in the offer. To do this, they must:

1. Acquire and activate the pxGrid Cloud subscription.
2. Enable the pxGrid Cloud service on one or two pxGrid nodes in the Cisco ISE deployment.
3. Register the Cisco ISE deployment with Cisco pxGrid Cloud (associating it with the subscription) and receive an authentication token.
4. Enter the authentication token in the **Setup Connection** window in Cisco ISE (under **Administration** > **pxGrid Services** > **Client Management** > **pxGrid Cloud Connection**).

   This activates the pxGrid Cloud agent on the Active pxGrid Cloud node and establish a connection between the Cisco ISE deployment and Cisco pxGrid Cloud.
5. Select a pxGrid Cloud application from the offer and associate it with the subscription. The application will then have access to the Cisco ISE deployment.

Enable pxGrid Cloud Service in Cisco ISE

Before you begin

- Ensure that you install and activate the Advantage license in your Cisco ISE deployment.
- The pxGrid Cloud agent creates an outbound HTTPS connection to Cisco pxGrid Cloud. Therefore, you must configure Cisco ISE proxy settings if the customer network uses a proxy to reach the internet. To configure proxy settings in Cisco ISE, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Proxy**.
- The Cisco ISE Trusted Certificates Store must include the root CA certificate required to validate the server certificate presented by Cisco pxGrid Cloud. Ensure that the **Trust for Authentication of Cisco Services** option is enabled for this root CA certificate.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 2 Click the node in which you want to enable the pxGrid Cloud service.

Step 3 In the **General Settings** tab, click the toggle button to enable the **pxGrid** service.

Step 4 Check the **Enable pxGrid Cloud** check box.

The pxGrid Cloud service can be enabled on two nodes to enable high availability.

Note You can enable the **pxGrid Cloud** option only when the **pxGrid** service is enabled on that node.

Connect Cisco ISE to Cisco pxGrid Cloud

After the pxGrid Cloud service is enabled, you must connect the Cisco ISE deployment to Cisco pxGrid Cloud. You must register your Cisco ISE deployment in Cisco pxGrid Cloud and generate an authentication token.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **pxGrid Services** > **Client Management** > **pxGrid Cloud Connection**.

Step 2 Click **Setup Connection**.

Step 3 Enter the authentication token in the **Setup Connection** window, and then click **Connect**.

The connection setup includes the following steps:

a. **Enrollment**: A request is sent to Cisco pxGrid Cloud to enroll the Cisco ISE deployment using the authentication token. When this step is successfully completed, the pxGrid Cloud agent is started on the Active node in the Cisco ISE deployment.

b. **pxGrid Connection**: The pxGrid Cloud agent establishes a persistent connection to the pxGrid component running locally on the same Cisco ISE node. All pxGrid notifications from Cisco ISE are sent to the pxGrid Cloud agent using this connection.

c. **Cloud Connection**: The pxGrid Cloud agent establishes a persistent connection to Cisco pxGrid Cloud and sets up the logical channels. These logical channels are used to receive the pxGrid, ERS, and Open API requests from Cisco pxGrid Cloud, and to send the pxGrid notifications to Cisco pxGrid Cloud.

You can view the connection setup progress in the **pxGrid Cloud Connection** window. After all these steps are completed, the status is displayed as **Connected**, and the name of the Active pxGrid node is displayed.

To terminate the pxGrid Cloud connection, click **Disconnect** in the **pxGrid Cloud Connection** window. This disconnects the Cisco ISE deployment from Cisco pxGrid Cloud and terminates the pxGrid Cloud agent in the Active node.

After the Cisco ISE deployment is connected to Cisco pxGrid Cloud, the pxGrid Cloud agent (called HERMES process) is listed in the output of the **show application status ise** CLI command.

Disable pxGrid Cloud Service on Cisco ISE

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 2 Check the check box next to the corresponding pxGrid node and click **Edit**.

Step 3 Uncheck the **Enable pxGrid Cloud** check box.

This stops the pxGrid Cloud agent in the Cisco ISE deployment. You can re-enable the pxGrid Cloud service later when needed.

Configure a pxGrid Cloud Policy

By default, pxGrid Cloud applications are not permitted to access any pxGrid, ERS, or Open APIs in the Cisco ISE deployment. Access must be explicitly granted by configuring policies in Cisco ISE.

You can create a policy to specify what is allowed or denied between your Cisco ISE deployment and the pxGrid Cloud service. Authorization policies specific to each partner environment can be configured in the cloud portal. You will need the Cisco ISE Advantage license to configure a pxGrid Cloud policy.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **pxGrid Services** > **Client Management** > **pxGrid Cloud Policy**.

Step 2 In the **pxGrid Services** area, choose the required services from the list. You can enable one or more pxGrid services by clicking their names.

Step 3 In the **ERS APIs** area, click the toggle button enable the **ERS APIs** option to provide ERS API access to pxGrid Cloud applications.

Note The **ERS APIs** option is disabled here if the ERS service is disabled in Cisco ISE.

To enable this service in Cisco ISE, perform these steps:

a. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **API Settings** > **API Service Settings**.

b. Click the toggle button to enable the **ERS (Read/Write)** option.

Step 4 In the **Open APIs** area, click the toggle button to enable the **Open APIs** option to provide Open API access to pxGrid Cloud applications.

Note The **Open APIs** option is disabled here if the **Open API** option is disabled in Cisco ISE.

To enable this service in Cisco ISE, perform these steps:

a. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **API Settings** > **API Service Settings**.

b. Click the toggle button to enable the **Open API (Read/Write)** option.

Note

- By default, both ERS and Open API options are disabled in the **pxGrid Cloud Policy** window.
- When you enable the ERS or Open APIs option, the pxGrid Cloud applications are granted **Read Only** access by default (only HTTP GET operations can be performed). Click the toggle button to enable the **Read/Write** option in the **pxGrid Cloud Policy** window if you want to allow POST, PUT, and DELETE operations as well.

Cisco pxGrid Cloud Clients

To view the pxGrid Cloud applications, choose **Administration** > **pxGrid Services** > **Client Management** > **Clients** > **pxGrid Cloud Clients**.

The pxGrid Cloud offer provides a collection of registered applications that pxGrid Cloud subscribers can select and use. For example, if a subscriber registers Cisco ISE deployment in Cisco pxGrid Cloud and uses two applications, those two applications are listed in the **pxGrid Cloud Clients** tab. Note that you can only view the pxGrid Cloud applications in this tab. You cannot make any changes from this tab.

You can view the total number of pxGrid Cloud applications that are currently running on this deployment in the **Total Clients** pane in the **Summary** window (**Administration** > **pxGrid Services** > **Summary**).

High Availability for pxGrid Nodes

You can configure two or more pxGrid nodes to enable high availability. When the Cisco ISE deployment is successfully connected to Cisco pxGrid Cloud, one of the nodes is selected as the Active node and the pxGrid Cloud agent is started on that node. If the Active node is down, or if the network connectivity to the Active node is lost, the Standby node is moved to the Active state. The pxGrid Cloud agent is started on that node and the connectivity to Cisco pxGrid Cloud is established again.

Note The failover process might take around 30 seconds.

Table 18: Events that Trigger High-Availability Response

Event	High-Availability Response
pxGrid Cloud service disabled on Active node	Standby node immediately becomes the Active node
Active node restarted because of a crash or user-initiated sequence	Standby node becomes Active. When the restarted node comes up, this node becomes the Standby node and monitors the Active node.
Deployment upgrade (or standalone Cisco ISE node upgrade) with one pxGrid node	After the upgrade, the node functions as the Active node.
Upgrade deployment with Active and Standby nodes	After the upgrade, the Standby node remains as Standby and continues to monitor the Active node. When the Active node is upgraded, the Standby node takes over as the Active node. When the upgraded node comes up, it becomes Standby and monitors the Active node.
Network issue occurs between the Active and Standby nodes	Both the nodes operate in Active mode. When this occurs, the names of both the nodes are displayed in the **pxGrid Cloud Connection** window. After the connectivity between the nodes is restored, one of the nodes is selected as the Active node and the other node acts as the Standby node.
Add a new pxGrid node to the deployment	The new node initially acts as the Active node. After the node is fully synchronized and is able to communicate with its peer, one of the nodes is selected as the Active node.

The following configuration changes restart the pxGrid Cloud agent:

- Replacing the pxGrid system certificate
- Replacing the Admin system certificate
- Enabling or disabling the **Trust for authentication within ISE** or **Trust for authentication of Cisco Services** option for any trust certificate
- Changing Cisco ISE proxy settings
- Enabling or disabling the ERS service for Cisco pxGrid Cloud
- Enabling or disabling any pxGrid service in the **pxGrid Cloud Policy** window

Log Files Specific to pxGrid Cloud Service

You can check the following log files in the active pxGrid node if there is any issue related to pxGrid Cloud service:

Log File	Contents	Available Location
pxcloud.log	• pxGrid Cloud service configuration changes • pxGrid Cloud service connection status • High-availability status (selection of Active node, detection of failures, and so on)	Cisco ISE nodes where the pxGrid Cloud service is enabled.

hermes.log	All activities logged by the pxGrid Cloud agent including: • Cisco ISE and Cisco pxGrid Cloud connection status • pxGrid topic subscription status • Handling pxGrid, ERS, and Open API requests from Cisco pxGrid Cloud • Configuration changes made in Cisco ISE	Active pxGrid node **Note** If the Standby node was previously Active, hermes.log is retained in that node, but the log file is not updated after it moves to the Standby state.

These log files are included in the Cisco ISE support bundle when the **Include Debug Logs** option is enabled. To download these logs, choose **Operations** > **Troubleshoot** > **Download Logs** > **Debug Logs** > **Application Logs**.

Configure Debug Log Level for pxGrid Cloud Service

Perform this procedure to configure the level of detail included in the pxcloud.log and hermes.log files.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Debug Wizard** > **Debug Log Configuration**.

Step 2 Click the pxGrid node.

Step 3 Click **pxGrid Cloud**.

Step 4 Choose one of the following options from the **Log Level** drop-down list:

- **Trace**
- **Debug**
- **Info**
- **Warn**
- **Error**
- **Fatal**

The selected log level applies to both the pxcloud.log and the hermes.log.

Note The hermes.log supports only the **Debug**, **Info**, **Warn**, and **Error** log levels. Hence, if you choose **Trace**, the log level is set as **Debug** for the hermes.log. If you choose **Fatal**, the log level is set as **Error** for the hermes.log.

View Nodes in a Deployment

In the **Deployment Nodes** window, you can view all the Cisco ISE nodes, primary and secondary, that are a part of your deployment.

Step 1 Log in to the primary Cisco ISE Admin portal.

Step 2 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 3 Click **Deployment** in the navigation pane on the left.

All the Cisco ISE nodes that are a part of your deployment are listed.

Download Endpoint Statistical Data from MnT Nodes

You can download statistical data about the endpoints that connect to your network from the MnT nodes. Key Performance Metrics (KPM), which include the load, CPU usage, and authentication traffic data are available. You can use this data to monitor and troubleshoot issues in your network. From the Cisco ISE CLI, run the **application configure ise** command and choose Option 12 or Option 13 to download the daily KPM statistics or the KPM statistics for the last eight weeks.

The output of this command provides the following data about endpoints:

- Total endpoints in your network
- Number of endpoints that established a successful connection
- Number of endpoints that failed authentication
- Total number of new endpoints that have connected each day
- Total number of endpoints onboarded each day

The output also includes time stamp details, the total number of endpoints that connected through each of the Policy Service nodes (PSNs) in the deployment, total number of endpoints, active endpoints, load, and authentication traffic details.

See the Cisco Identity Services Engine CLI Reference Guide for more information on this command.

Database Crash or File Corruption Issues

Cisco ISE may crash if the Oracle database files are corrupted because of a power outage or other reasons, resulting in data loss. Based on the incident, follow these instructions to recover from data loss:

- In case of PAN corruption in the deployment, you should promote the Secondary PAN to Primary PAN. If the secondary PAN's promotion is not possible because the deployment is small or any other reason, restore the most recent available backup as described in Cisco Identity Services Engine CLI Reference Guide.
- In case of PSN corruption, follow the steps to deregister, reset config, and register, as described in the Cisco Identity Services Engine CLI Reference Guide.
- In case of a standalone device, restore the most recent backup that is available, as described in the Cisco Identity Services Engine CLI Reference Guide.

Note Obtain the backup from the standalone device regularly to avoid loss in the latest configuration changes.

Device Configuration for Monitoring

The MnT node receives and uses data from the devices on a network to populate the dashboard display. To enable communication between the MnT node and the network devices, the switches and NADs must be configured properly.

Synchronize Primary and Secondary Cisco ISE Nodes

You can make configuration changes to Cisco ISE only through the primary PAN. The configuration changes get replicated to all the secondary nodes. If, for some reason, this replication does not occur properly, you can manually synchronize the secondary PAN with the primary PAN.

Step 1 Log in to the primary PAN.

Step 2 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 3 Check the check box next to the node that you want to synchronize with the primary PAN, and click **Syncup** to force a full database replication.

Change Node Personas and Services

Note When you enable or disable any of the services that run on a PSN or make any changes to a PSN, you will be restarting the application server processes on which these services run. Expect a delay while these services restart. Because this delay in restarting services, automatic failover, if enabled in your deployment, might get initiated. To avoid this, make sure that the automatic failover configuration is turned off.

You can edit the Cisco ISE node configuration to change the personas and services that run on the node.

Step 1 Log in to the primary PAN.

Step 2 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 3 Check the check box next to the node whose personas or services you want to change, and then click **Edit**.

Step 4 Choose the personas and services that you want to modify.

Step 5 Click **Save**.

Step 6 Verify the receipt of an alarm on your primary PAN to confirm the persona or service change. If the persona or service change is not saved successfully, an alarm is not generated.

Effects of Modifying Nodes in Cisco ISE

When you make any of the following changes to a node in a Cisco ISE, that node restarts, which causes a delay:

- Register a node (Standalone to Secondary)
- Deregister a node (Secondary to Standalone)
- Change a primary node to Standalone (if no other nodes are registered with it; Primary to Standalone)
- Promote an Administration node (Secondary to Primary)
- Change the personas (when you assign or remove the Policy Service or Monitoring persona from a node)
- Modify the services in the Policy Service node (enable or disable the session and profiler services)
- Restore a backup on the primary and a sync up operation is triggered to replicate data from primary to secondary nodes

Note When you promote the secondary Administration node to the primary PAN position, the primary node will assume a secondary role. This causes both the primary and secondary nodes to restart, causing a delay.

Create a Policy Service Node Group

When two or more Policy Service nodes (PSNs) are connected to the same high-speed Local Area Network (LAN), we recommend that you place them in the same node group. This design optimizes the replication of endpoint profiling data by retaining less significant attributes that are local to the group and reducing the information that is replicated to the remote nodes in the network. Node group members also check on the availability of peer group members. If the group detects that a member has failed, it attempts to reset and recover all URL-redirected sessions on the failed node.

The node groups are used for the PSN failover in the sessions on which URL redirect (posture services, guest services, and MDM) is imposed.

Note We recommend that you put all the PSNs in the same local network and as a part of the same node group. PSNs need not be a part of a load-balanced cluster to join the same node group. However, each local PSN in a load-balanced cluster should typically be part of the same node group.

Node group members can communicate over TCP/7800.

Before you add PSNs as members to a node group, you must create the node group. You can create, edit, and delete PSN groups from the **Deployment** window of the Admin portal.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 2 Click the **Settings** icon at the top of the left navigation pane.

Step 3 Click **Create Node Group**.

Step 4 Enter a unique name for your node group.

Note We recommend that you do not configure a node group with the name **None**, because it may cause issues during node registration.

Step 5 (Optional) Enter a description for your node group.

Step 6 (Optional) Check the **Enable MAR Cache Distribution** check box and fill in the other options. Ensure that the MAR is enabled in the **Active Directory** window before checking this check box.

Step 7 Click **Submit** to save the node group.

After you save the node group, it should appear in the left navigation pane. If you do not see the node group in the left pane, it may be hidden. Click the **Expand** button on the navigation pane to view the hidden objects.

Add a node to a node group, or edit a node by choosing the corresponding node group from the **Include node in node group** drop-down list in the **Policy Service** area.

Remove a Node from Deployment

To remove a node from a deployment, you must deregister it. The deregistered node becomes a standalone Cisco ISE node.

It retains the last configuration that it received from the primary PAN and assumes the default personas of a standalone node, that is, Administration, Policy Service, or Monitoring. If you deregister an MnT node, this node will no longer be a syslog target.

When a Primary PSN is deregistered, the endpoint data is lost. If you want the PSN to retain the endpoint data after it becomes a standalone node, do one of the following:

- Obtain a backup from the primary PAN, and when the PSN becomes a standalone node, restore this data backup on it.
- Change the persona of the PSN to Administration (secondary PAN), synchronize the data in the **Deployment** window of the Admin portal, and then deregister the node. This node will now have all the data. You can then add a secondary PAN to the existing deployment.

You can view these changes in the **Deployment** window of the primary PAN. However, expect a delay of five minutes for the changes to take effect and appear in the **Deployment** window.

Before you begin

Before you remove a secondary node from a deployment, perform a backup of Cisco ISE configuration, which you can then restore later, if needed.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 2 Check the check box next to the secondary node that you want to remove, and click **Deregister**.

Step 3 Click **OK**.

Step 4 Verify the receipt of an alarm on your primary PAN to confirm that the secondary node is deregistered successfully. If the secondary node fails to deregister from the primary PAN, it means the alarm is not generated.

Shut Down a Cisco ISE Node

Before you run the **halt** command from the Cisco ISE CLI, we recommend that you stop the Cisco ISE application service and ensure that it is not performing a backup, restore, installation, upgrade, or remove operation. If you run the **halt** command while the Cisco ISE is performing any of these operations, you will get one of the following warning messages:

```
WARNING: A backup or restore is currently in progress! Continue with halt?
```

```
WARNING: An install/upgrade/remove is currently in progress! Continue with halt?
```

If no processes are running when you use the **halt** command, or if you enter `Yes` in response to the warning message displayed, then you must respond to the following question:

```
Do you want to save the current configuration?
```

If you enter `Yes` to save the existing Cisco ISE configuration, the following message is displayed:

```
Saved the running configuration to startup successfully.
```

Note We recommend that you stop the application process before rebooting the appliance.

We also recommend that you stop the application process before rebooting Cisco ISE. For more information, see the Cisco Identity Services Engine CLI Reference Guide.

Scenarios In Which Need to Reregister a Node

The following table summarizes some of the scenarios where you need to reregister a node when it is corrupted:

Scenarios	What needs to be done
If any of the nodes other than the Primary PAN is corrupted	1. Deregister the failed node from the deployment. 2. Reinstall Cisco ISE on the failed node. 3. Reregister the node in the existing deployment. **Note** You must import the old certificates to the node before or after the registration.
If the Primary PAN is corrupted	If, for example, there are two nodes, N1 (Primary PAN) and N2 (Secondary PAN): 1. Promote secondary PAN (N2) to Primary PAN. 2. Remove the failed node (N1) from the deployment. 3. Reinstall Cisco ISE on the failed node (N1). 4. Register the node (N1) as Secondary PAN to deployment. 5. Import the old certificates to the node (N1) after the registration is completed. 6. Promote the node (N1) back to Primary PAN to have similar deployment as earlier.
If both Primary PAN and Secondary PAN are corrupted	If, for example, there are two nodes, N1 (Primary PAN) and N2 (Secondary PAN): 1. Reinstall Cisco ISE on Primary PAN node (N1) and Secondary PAN node (N2). 2. Restore configuration backup in Primary PAN node (N1). 3. Import old certificates in Primary PAN node (N1). 4. Register the other node (N2) as Secondary PAN in the deployment. 5. Perform reset-config on other nodes and register the nodes in the deployment. 6. Import certificates to all the nodes. **Note** If the Primary PAN and Secondary PANs are VMs, reinstalling Cisco ISE might change the UDI. Hence, you must reinstall the licenses with the new UDIs.

Change the Hostname or IP Address of a Standalone Cisco ISE Node

You can change the hostname, IP address, or domain name of standalone Cisco ISE nodes. However, you cannot use **localhost** as the hostname for a node.

Before you begin

If a Cisco ISE node is a part of a distributed deployment, you must first remove it from the deployment and ensure that it is a standalone node.

Step 1 Change the hostname or IP address of the Cisco ISE node using the **hostname**, **ip address,** or **ip domain-name** command from the Cisco ISE CLI.

Step 2 Reset the Cisco ISE application configuration using the **application stop ise** command from the Cisco ISE CLI to restart all the services.

Step 3 Register the Cisco ISE node to the primary PAN if it is a part of a distributed deployment.

> **Note** If you are using the hostname while registering the Cisco ISE node, the fully qualified domain name (FQDN) of the standalone node that you are going to register, for example, *abc.xyz.com*, must be DNS-resolvable from the primary PAN. Otherwise, node registration fails. You must enter the IP addresses and FQDNs of the Cisco ISE nodes that are a part of your distributed deployment in the DNS server.

After you register the Cisco ISE node as a secondary node, the primary PAN replicates the change in the IP address, hostname, or domain name to the other Cisco ISE nodes in your deployment.

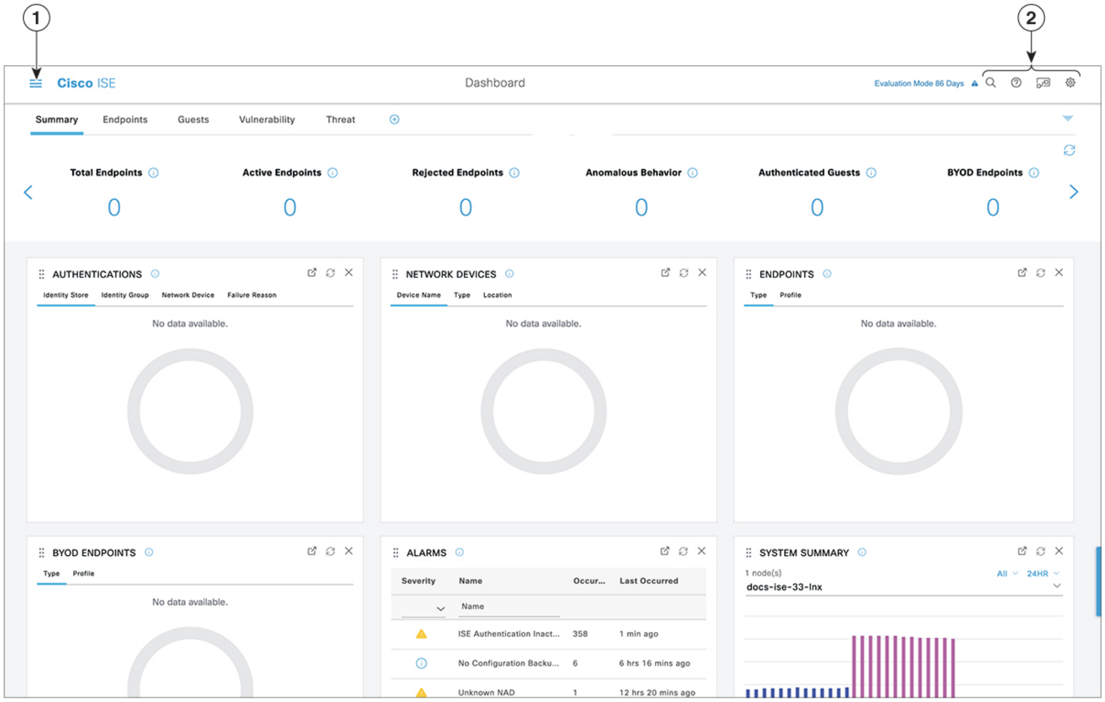
CHAPTER 5

Basic Setup

- Administration Portal, on page 232
- Cisco ISE Internationalization and Localization, on page 252
- MAC Address Normalization, on page 258
- Cisco ISE Deployment Upgrade, on page 259
- Administrator Access Console, on page 259
- Configure Proxy Settings in Cisco ISE, on page 260
- Ports Used by the Administration Portal, on page 261
- Set Up the Cisco ISE Application Programming Interface Gateway, on page 261
- Enable API Service, on page 262
- External RESTful Services Software Development Kit , on page 267
- Specify System Time and Network Time Protocol Server Settings, on page 267
- Change the System Time Zone, on page 269
- Configure SMTP Server to Support Notifications, on page 269
- Enable Secure Unlock Client Mechanism, on page 270
- Federal Information Processing Standards Mode Support, on page 272
- Secure SSH Key Exchange Using Diffie-Hellman Algorithm, on page 276
- Configure Cisco ISE to Send Secure Syslog, on page 276
- Default Secure Syslog Collector, on page 280
- Offline Maintenance, on page 281
- Configure Endpoint Login Credentials, on page 282
- Changing the Host Name in Cisco ISE, on page 282
- Certificate Management in Cisco ISE, on page 283
- Cisco ISE CA Service, on page 328
- OCSP Services, on page 360
- Configure Admin Access Policies, on page 367
- Administrator Access Settings, on page 367

Administration Portal

Figure 2: Cisco ISE Administration Portal


1
2
Cisco ISE
Dashboard
Evaluation Mode 86 Days
Summary
Endpoints
Guests
Vulnerability
Threat
Total Endpoints
0
Active Endpoints
0
Rejected Endpoints
0
Anomalous Behavior
0
Authenticated Guests
0
BYOD Endpoints
0
AUTHENTICATIONS
Identity Store
Identity Group
Network Device
Failure Reason
No data available.
NETWORK DEVICES
Device Name
Type
Location
No data available.
ENDPOINTS
Type
Profile
No data available.
BYOD ENDPOINTS
Type
Profile
No data available.
ALARMS
SYSTEM SUMMARY
1 node(s)
All
24HR
docs-ise-33-lnx

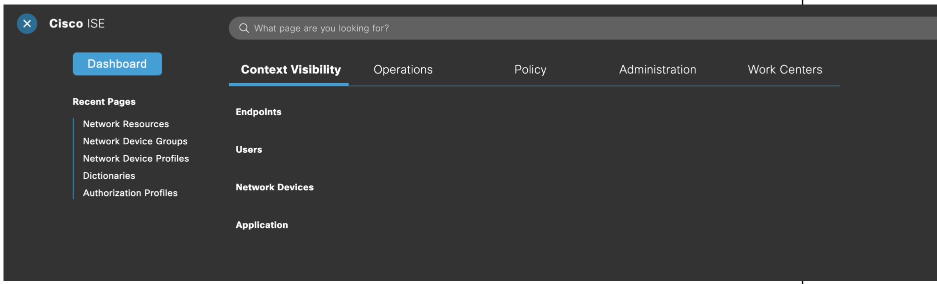
Severity	Name	Occur...	Last Occurred
	Name		
⚠	ISE Authentication Inact...	358	1 min ago
ⓘ	No Configuration Backu...	6	6 hrs 16 mins ago
⚠	Unknown NAD	1	12 hrs 20 mins ago

Table 19: Components of the Cisco ISE Administration Portal

1	Menu Icon	

Click the **Menu** icon (☰) for a slide-in window with the following menus. The slide-in Menu window also contains a search bar with which you can find the window that you need. Click **Dashboard** for the home page.

Figure 3: Cisco ISE Main Menu


Cisco ISE
What page are you looking for?
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Recent Pages
Network Resources
Network Device Groups
Network Device Profiles
Dictionaries
Authorization Profiles
Endpoints
Users
Network Devices
Application

The menu options on the left pane are:

- **Context Visibility**: The context visibility windows display information about endpoints, users, and network access devices (NAD). The context visibility information is grouped by features, applications, Bring Your Own Device (BYOD), and other categories, depending on the licenses you have registered. The context visibility windows use a central database and gather information from database tables, caches, and buffers. As a result, the content in the context visibility dashlets and lists gets updated quickly. The context visibility windows consist of dashlets at the top, and a list of information at the bottom. When you filter data by modifying the column attributes in the list, the dashlets get refreshed and display the modified content.
- **Operations**: Operations windows include tools to view RADIUS, TACACS+, and TC-NAC Live Logs, the Adaptive Network Control (ANC) policy, and troubleshooting options to diagnose and debug issues related to Cisco ISE deployments.
- **Policy**: Policy windows include tools for managing network security in the areas of authentication, authorization, profiling, posture, and client provisioning.
- **Administration**: Administration windows include tools for managing Cisco ISE nodes, licenses, certificates, network devices, users, endpoints, and guest services.
- **Work Centers**: Work Centers list the following expandable submenus. These submenus act as a single starting point for Cisco ISE administrators, to configure relevant features within a Cisco ISE deployment.
    - **Network Access**
    - **Guest Access**
    - **TrustSec**
    - **BYOD**
    - **Profiler**

		• **Posture** • **Device Administration** • **PassiveID**

2	Top-Right Menu Icons	

- 🔍

  Use this icon to search for endpoints and display their distribution by profiles, failures, identity stores, location, device type, and so on.

- ?

  Click the icon to view the Interactive Help menu that provides access to multiple resources.

- ⧉

  Click this icon to access the following options:

  - **PassiveID Setup**: The **PassiveID Setup** option launches the **PassiveID Setup** wizard to set up passive identity using Active Directory. Configure the server to gather user identities and IP addresses from external authentication servers and deliver the authenticated IP addresses to the corresponding subscriber.

  - **Visibility Setup**: **Visibility Setup** is a Proof of Value (PoV) service that collects endpoint data such as applications, hardware inventory, USB status, firewall status, and the overall compliance state of Windows endpoints. The collected data is then sent to Cisco ISE. When you launch the **ISE Visibility Setup** wizard, it allows you to specify an IP address range to run endpoint discovery for a preferred segment of the network or a group of endpoints.

    The PoV service uses the Cisco Stealth Temporal agent to collect endpoint posture data. Cisco ISE pushes the Cisco Stealth Temporal agent to computers running Windows with an Administrator account type, which automatically runs a temporary executable file to collect context. The agent then removes itself. To experience the optional debug capabilities of Cisco Stealth Temporal agent, check the **Endpoint Logging** check box (click the **Menu** icon (☰), and choose **Visibility Setup** > **Posture**) to save the debug logs in an endpoint or multiple endpoints. You can view the logs in either of the following locations:

    - C:\WINDOWS\syswow64\config\systemprofile\ (64-bit operating system)

    - C:\WINDOWS\system32\config\systemprofile\ (32-bit operating system)

  - **Run Endpoint Scripts**: Choose this option to run scripts on connected endpoints to carry out administrative tasks that comply with your organization’s requirements. This includes tasks like uninstalling obsolete software, starting or terminating processes or applications, and enabling or disabling specific services.

- ⚙

  Click this icon for a menu of system activities, including launching

		online help, and configuring account settings.

Interactive Help

The Interactive Help enables users to work effectively with Cisco ISE by providing tips and step-by-step guidance to complete tasks with ease.

This feature is enabled by default. To disable this feature, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Interactive Help**, and uncheck the **Enable Interactive Help** check box.

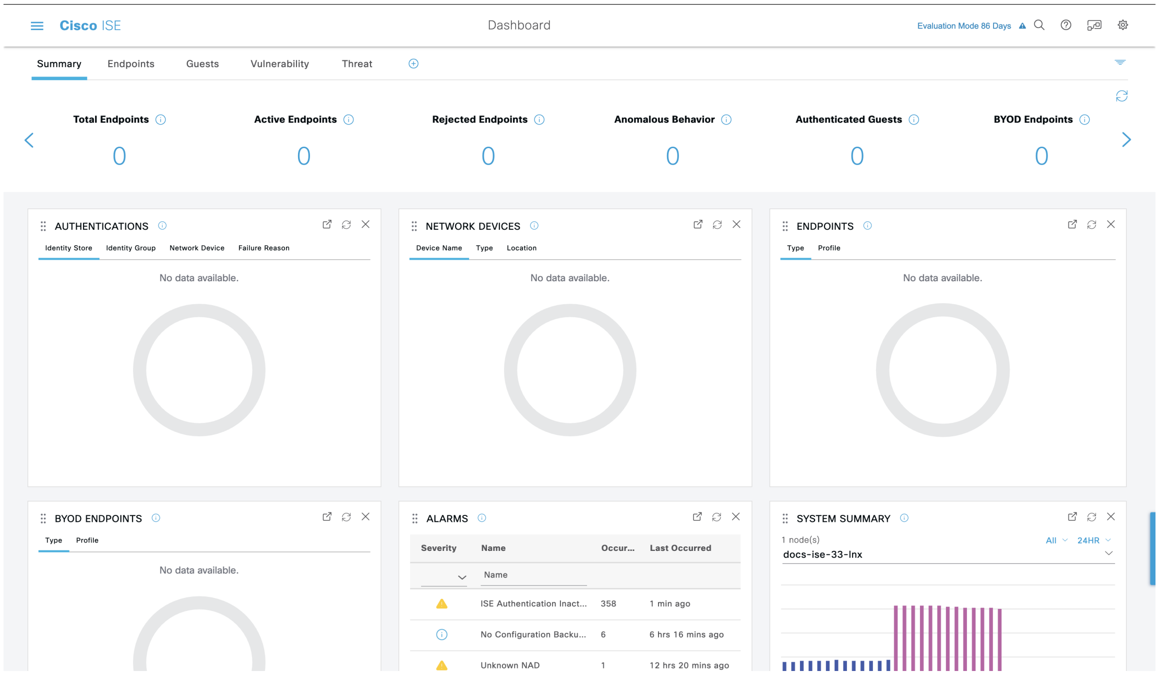
Click the **Show** button to view the Interactive Help menu.

If you access the Cisco ISE administrator portal through a Google Chrome Incognito window, you must enable third-party cookies to view and access Interactive Help. See Third-party cookie controls in Incognito mode.

Cisco ISE Home Dashboards

The Cisco ISE Home dashboard displays live consolidated and correlated statistical data that is essential for effective monitoring and troubleshooting. Dashboard elements typically display activity over 24 hours. The following figure is an example of the information available in a Cisco ISE dashboard. You can view the Cisco ISE dashboard data only in the primary Policy Administration node (PAN) portal.

Figure 4: Cisco ISE Home Dashboard


Cisco ISE
Dashboard
Evaluation Mode 86 Days
Summary
Endpoints
Guests
Vulnerability
Threat
Total Endpoints
0
Active Endpoints
0
Rejected Endpoints
0
Anomalous Behavior
0
Authenticated Guests
0
BYOD Endpoints
0
AUTHENTICATIONS
Identity Store
Identity Group
Network Device
Failure Reason
No data available.
NETWORK DEVICES
Device Name
Type
Location
No data available.
ENDPOINTS
Type
Profile
No data available.
BYOD ENDPOINTS
Type
Profile
No data available.
ALARMS
SYSTEM SUMMARY
1 node(s)
All
24HR
docs-ise-33-lnx

Severity	Name	Occur...	Last Occurred
⚠	ISE Authentication Inact...	358	1 min ago
ⓘ	No Configuration Backu...	6	6 hrs 16 mins ago
⚠	Unknown NAD	1	12 hrs 20 mins ago

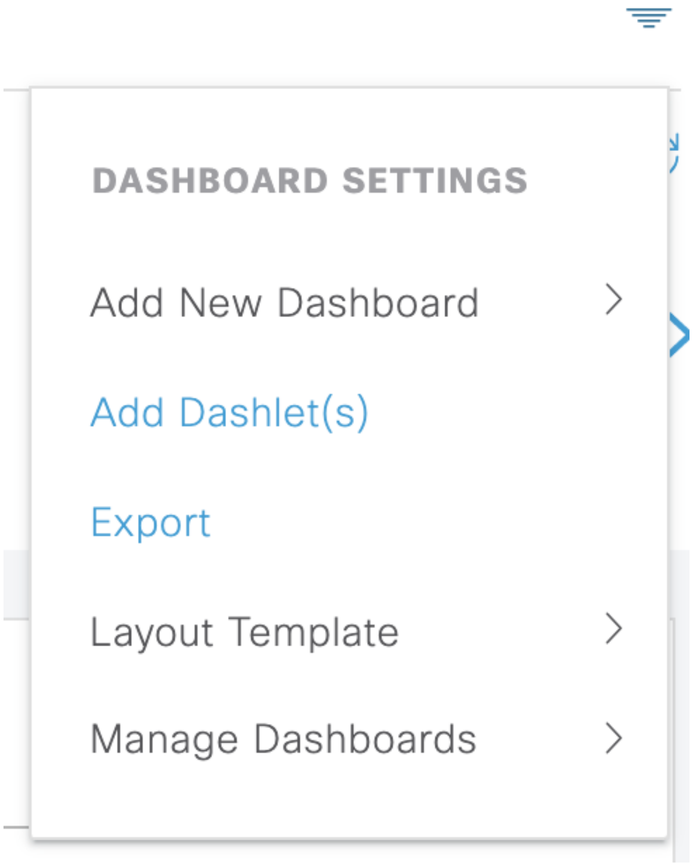
The home page has five default dashboards that display your Cisco ISE data. Each of these dashboards has several predefined dashlets.

- **Summary**: This dashboard contains a linear metrics dashlet, pie chart dashlets, and list dashlets. The metrics dashlet is not configurable. By default this dashboard contains the dashlets **Status Endpoints**, **Endpoint Categories**, and **Network Devices**.
- **Endpoints**: By default, this dashboard contains the dashlets **Status**, **Endpoints**, **Endpoint Categories**, and **Network Devices**.
- **Guests**: This dashboard contains dashlets that provide information on guest user type, log in failures, and location of acitivity.
- **Vulnerability**: This dashboard displays the information that vulnerability servers report to Cisco ISE.
- **Threat**: This dashboard displays information from the threat servers reports sent to Cisco ISE.

Configuring Home Dashboards

You can customize a home page dashboard by clicking the **Inverted Pyramid** icon in the top right corner of the window:

Figure 5: Customize A Dashboard



The following options are displayed in the drop-down list:

- **Add New Dashboard** allows you to add a new dashboard. Enter a value in the field that is displayed and click **Apply**.

- **Add Dashlet(s)** displays a dialog box with a list of dashlets available. Click **Add** or **Remove** next to the dashlet name to add or remove a dashlet from the dashboard.
- **Export** saves the selected home page view to a PDF.
- **Layout Template** configures the number of columns that are displayed in this view.
- **Manage Dashboards** contains two options:
    - **Mark As Default Dashboard**: Choose this option to make the current dashboard the default view when you choose Home.
    - **Reset All Dashboards**: Use this option to also reset all the dashboards and remove your configurations on all the Home dashboards.

Context Visibility Views

The structure of a **Context Visibility** window is similar to the home page, except that the Context Visibility windows:

- Retain your current context (browser window) when you filter the displayed data
- Are more customizable
- Focus on endpoint data

You can view the context visibility data only from the primary PAN.

Dashlets on the **Context Visibility** windows show information about endpoints, and endpoint connections to NADs. The information currently displayed is based on the content in the list of data below the dashlets on each window. Each window displays endpoint data, based on the name of the tab. As you filter the data, both the list and dashlets update. You can filter the data by clicking on parts of one or more of the circular graphs, by filtering rows on the table, or any combination those actions. As you select filters, the effects are additive, also referred to as cascading filter, which allows you to drill down to find the particular data you are looking for. You can also click an endpoint in the list, and get a detailed view of that endpoint.

We recommend that you enable the accounting settings on the network access devices (NADs) to ensure that the accounting start and update information is sent to Cisco ISE.

Cisco ISE can collect accounting information, such as the latest IP address, status of the session (Connected, Disconnected, or Rejected), the number of days an endpoint has been inactive, only if accounting is enabled. This information is displayed in the **Live Logs**, **Live Sessions** and **Context Visibility** windows in the Cisco ISE administration portal. When accounting is disabled on a NAD, there might be a missing, incorrect, or mismatched accounting information between the **Live Sessions**, **Live Logs** and **Context Visibility** windows.

There are four main menu options under **Context Visibility**:

- **Endpoints**: Filter the endpoints you want to view based on types of devices, compliance status, authentication type, hardware inventory, and more. See The Hardware Dashboard, on page 244 for additional information.

Note The **Visibility Setup** workflow that is available on the Cisco ISE administration portal home page allows you to add a list of IP address ranges for endpoints discovery. After this workflow is configured, Cisco ISE authenticates the endpoints, but the endpoints that are not included in the configured IP address ranges are not displayed in the **Context Visibility** > **Endpoints** window and the **Endpoints** listing page (**Work Centers** > **Network Access** > **Identities** > **Endpoints**).

- **Users**: Displays user-based information from user identity sources.

  If there is a change in the username or password attribute, it reflects in the **Users** window when there is a change in the authentication status.

  If the username is changed in the Microsoft Active Directory, the updated change is displayed in the **Users** window immediately after re-authentication.

  If any other attributes such as Email, Phone, Department, etc are changed in the Microsoft Active Directory, the updated attributes are displayed in the **Users** window 24 hours after re-authentication.

Note Updating User Attributes from AD depends on the interval configured under Active Directory Probe. For more information, see Active Directory Probe.

- **Network Devices**: This window displays the list of NADs that have endpoints connected to them. For any NAD, click the number of endpoints that is displayed in the corresponding **# of endpoints** column. A window that lists all the devices filtered by that NAD is displayed.

Note If you have configured your network device with SNMPv3 parameters, you cannot generate the **Network Device Session Status Summary** report that is provided by the Cisco ISE monitoring service (**Operations** > **Reports** > **Catalog** > **Network Device** > **Session Status Summary**). You can generate this report successfully if your network device is configured with SNMPv1 or SNMPv2c parameters.

- **Application**: Use this window to identify the number of endpoints that have a specific application installed. The results are displayed in graphical and table formats. The graphical representation helps you make a comparative analysis. For example, you can find out the number of endpoints with the Google Chrome software along with their Version, Vendor, and Category (Anti-phishing, Browser, and so on) in a table as well as a bar chart. For more information, see The Application Dashboard.

You can create a new tab in the **Context Visibility** windows and create a custom list for additional filtering. Dashlets are not supported in custom views.

Click a section of a circular graph in a dashlet to view a new window with filtered data from that dashlet in. From this new window, you can continue to filter the displayed data, as described in Filtering Displayed Data in a View, on page 247.

For more information about using Context Visibility windows to find endpoint data, see the following Cisco YouTube video https://www.youtube.com/watch?v=HvonGhrydfg.

Related Topics

The Hardware Dashboard, on page 244

Attributes in Context Visibility

The systems and services that provide attributes for Context Visibility sometimes have different values for the same attribute name. The following are a few examples:

For Operating System

- *OperatingSystem*: Posture operating system.
- *operating-system*: NMAP operating system.
- *operating-system-result*: Profiler consolidated operating system.

Note There might be some discrepancies in the endpoint operating system data that is displayed in the Context Visibility window when you enable multiple probes in Cisco ISE for an endpoint.

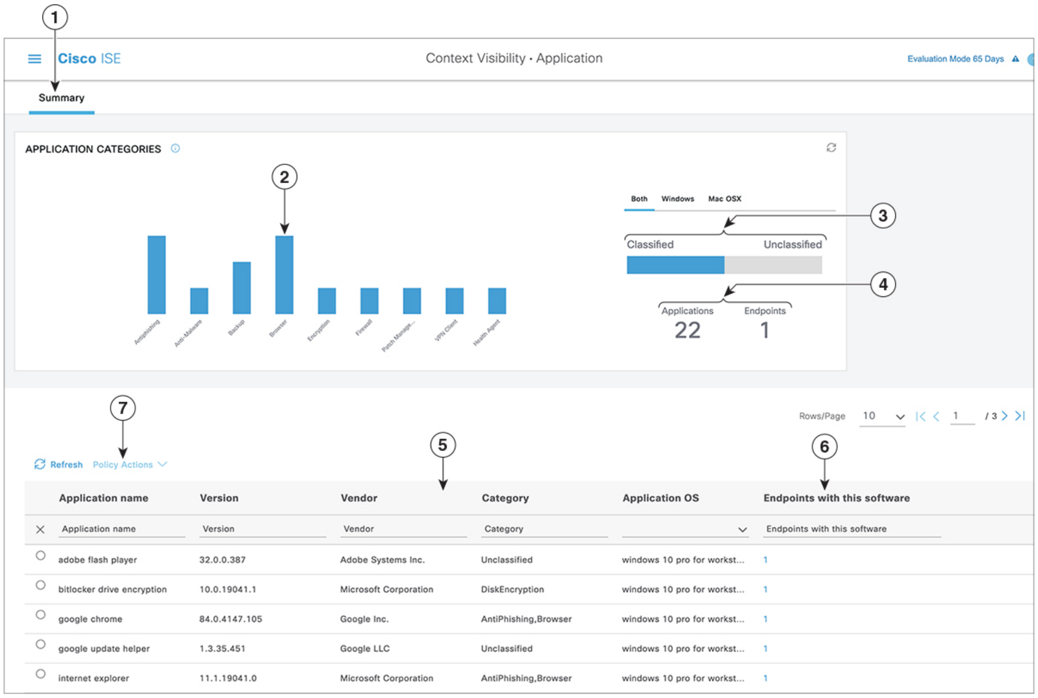
For Portal Name

- *Portal.Name*: Guest portal name when device registration is turned on.
- *PortalName*: Guest portal name when device registration is not turned on.

For Portal User

- *User-Name*: Username from RADIUS authentication.
- *GuestUserName*: Guest username.
- *PortalUser*: Portal username.

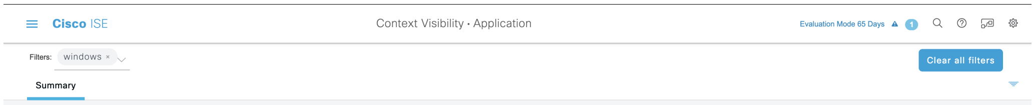
The Application Dashboard


1
Cisco ISE
Context Visibility · Application
Evaluation Mode 65 Days
Summary
APPLICATION CATEGORIES
2
Antiphishing
Anti-Malware
Backup
Browser
Encryption
Firewall
Patch Manage...
VPN Client
Health Agent
Both
Windows
Mac OSX
3
Classified
Unclassified
4
Applications
22
Endpoints
1
7
Rows/Page
10
1
/ 3
5
6
Refresh
Policy Actions

	Application name	Version	Vendor	Category	Application OS	Endpoints with this software
×	Application name	Version	Vendor	Category		Endpoints with this software
○	adobe flash player	32.0.0.387	Adobe Systems Inc.	Unclassified	windows 10 pro for workst...	1
○	bitlocker drive encryption	10.0.19041.1	Microsoft Corporation	DiskEncryption	windows 10 pro for workst...	1
○	google chrome	84.0.4147.105	Google Inc.	AntiPhishing,Browser	windows 10 pro for workst...	1
○	google update helper	1.3.35.451	Google LLC	Unclassified	windows 10 pro for workst...	1
○	internet explorer	11.1.19041.0	Microsoft Corporation	AntiPhishing,Browser	windows 10 pro for workst...	1

Table 20: Description of the Application Dashboard

Label	Description
1	The **Summary** tab is displayed by default on the home page. It displays the **Application Categories** dashlet, which contains a bar chart. Applications are classified into 13 categories. Applications that do not fall into any of these categories are grouped as **Unclassified**. The available categories are Anti-Malware, Antiphishing, Backup, Browser, Data Loss Prevention, Data Storage, Encryption, Firewall, Messenger, Patch Management, Public File Sharing, Virtual Machine, and VPN Client.
2	Each bar corresponds to a classified category. Hover over each bar to view the total number of applications and endpoints that correspond to the selected application category.
3	The applications and endpoints that fall under the Classified category are displayed in blue. Unclassified applications and endpoints are displayed in gray. Hover over the classified or unclassified category bars to view the total number of applications and endpoints that belong to that category. You can click **Classified** and view the results in the bar chart and table in the window. When you click **Unclassified**, the bar chart is disabled and the results are displayed in the table in the window.

<table>
<tr><th>Label</th><th colspan="6">Description</th></tr>
<tr><td>4</td><td colspan="6">The applications and endpoints are displayed based on the selected filter. You can view the breadcrumb trail as you click different filters. You can click Clear All Filters to remove all the applied filters.

 </td></tr>
<tr><td rowspan="5">5</td><td colspan="6">When you click multiple bars, the corresponding classified applications and endpoints are displayed in the table. For example, if you select the Antimalware and Patch Management categories, the following results are displayed:</td></tr>
<tr><td>Application Name</td><td>Version</td><td>Vendor</td><td>Category</td><td>Application OS</td><td>Endpoints With This Software</td></tr>
<tr><td>Gatekeeper</td><td>9.9.5</td><td>Apple Inc.</td><td>Antimalware</td><td>windows 7 64-bit,mac osx 10.10,mac osx 8,mac osx 9</td><td>5</td></tr>
<tr><td>Gatekeeper</td><td>10.9.5</td><td>Apple Inc.</td><td>Antimalware</td><td>Windows 8 64-bit, mac osx 10.10</td><td>3</td></tr>
<tr><td>Software Update</td><td>2.3</td><td>Apple Inc.</td><td>Patch Management</td><td>Windows 7 64 bit, mac osx 10.10,mac osx 8,mac osx 9</td><td>5</td></tr>
<tr><td>6</td><td colspan="6">Click an endpoint in the Endpoints With This Software column in the table to view the endpoint details, such as Mac address, NAD IP address, NAD port ID/SSID, IPv4 address, and so on.</td></tr>
<tr><td>7</td><td colspan="6">You can select an application name and choose the Create App Compliance option from the Policy Actions drop-down list to create application compliance condition and remediation.</td></tr>
</table>

The Hardware Dashboard

The endpoint hardware tab under context visibility helps you collect, analyze, and report endpoint hardware inventory information within a short time. You can gather information, such as finding endpoints with low memory capacity or finding the BIOS model/version in an endpoint. You can increase the memory capacity or upgrade the BIOS version based on these findings. You can assess the requirements before you plan the purchase of an asset. You can ensure timely replacement of resources. You can collect this information without installing any modules or interacting with the endpoint. In summary, you can effectively manage the asset lifecycle.

Note The hardware inventory data takes 120 seconds to be displayed in the ISE GUI. The hardware inventory data is collected for posture compliant and non-compliant states.

The **Context Visibility** > **Endpoints** > **Hardware** page displays the **Manufacturers** and **Endpoint Utilizations** dashlets. These dashlets reflect the changes based on the selected filter. The **Manufacturers** dashlet displays hardware inventory details for endpoints with Windows and Mac OS. The **Endpoint Utilizations** dashlet displays the CPU, Memory, and Disk utilization for endpoints. You can select any of the three options to view the utilization in percentage.

- Devices With Over n% CPU Usage.
- Devices With Over n% Memory Usage.
- Devices With Over n% Disk Usage.

Note

- The Quick Filters in the Hardware Visibility Page need at least 3 characters to take effect. Another way to make the Quick Filter work efficiently is to click on the filters of other column attributes after entering the characters.
- Some of the column attributes are greyed out as this table is only used to filter based on attributes related to hardware.
- The Operating System filter applies only to the **Manufacturers** Chart. It is not relevant to the table below it.

The hardware attributes of an endpoint and their connected external devices are displayed in a table format. The following hardware attributes are displayed:

- MAC Address
- BIOS Manufacturer
- BIOS Serial Number
- BIOS Model
- Attached Devices
- CPU Name
- CPU Speed (GHz)
- CPU Usage (%)
- Number of Cores
- Number of Processors
- Memory Size (GB)
- Memory Usage (%)
- Total Internal Disk(s) Size (GB)
- Total Internal Disk(s) Free Size (GB)
- Total Internal Disk(s) Usage (%)
- Number of Internal Disks

- NAD Port ID
- Status
- Network Device Name
- Location
- UDID
- IPv4 Address
- Username
- Hostname
- OS Types
- Anomalous Behavior
- Endpoint Profile
- Description
- Endpoint Type
- Identity Group
- Registration Date
- Identity Store
- Authorization Profile

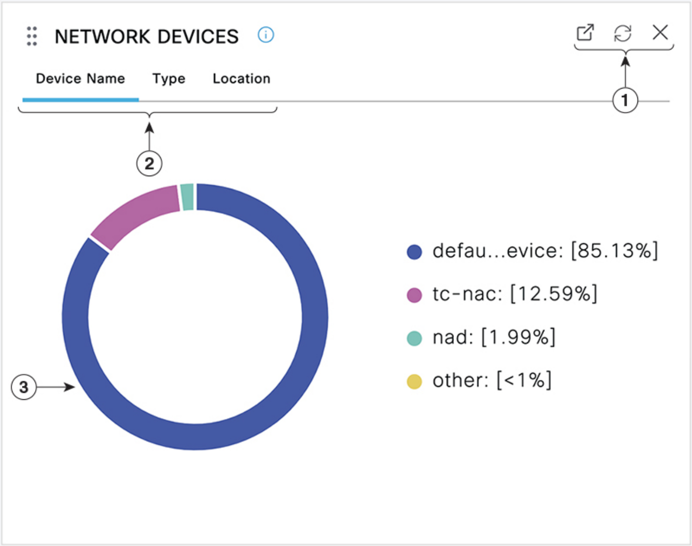
You can click the number in the **Attached Devices** column that corresponds to an endpoint to view the Name, Category, Manufacturer, Type, Product ID, and Vendor ID of the USB devices that are currently attached to the endpoint.

Note Cisco ISE profiles the hardware attributes of a client's system, however, there may be a few hardware attributes Cisco ISE does not profile. These hardware attributes may not appear in the Hardware Context Visibility page.

The hardware inventory data collection interval can be controlled in the **Administration** > **System** > **Settings** > **Posture** > **General Settings** page. The default interval is 5 minutes.

Dashlets

The following image is an example of a dashlet:



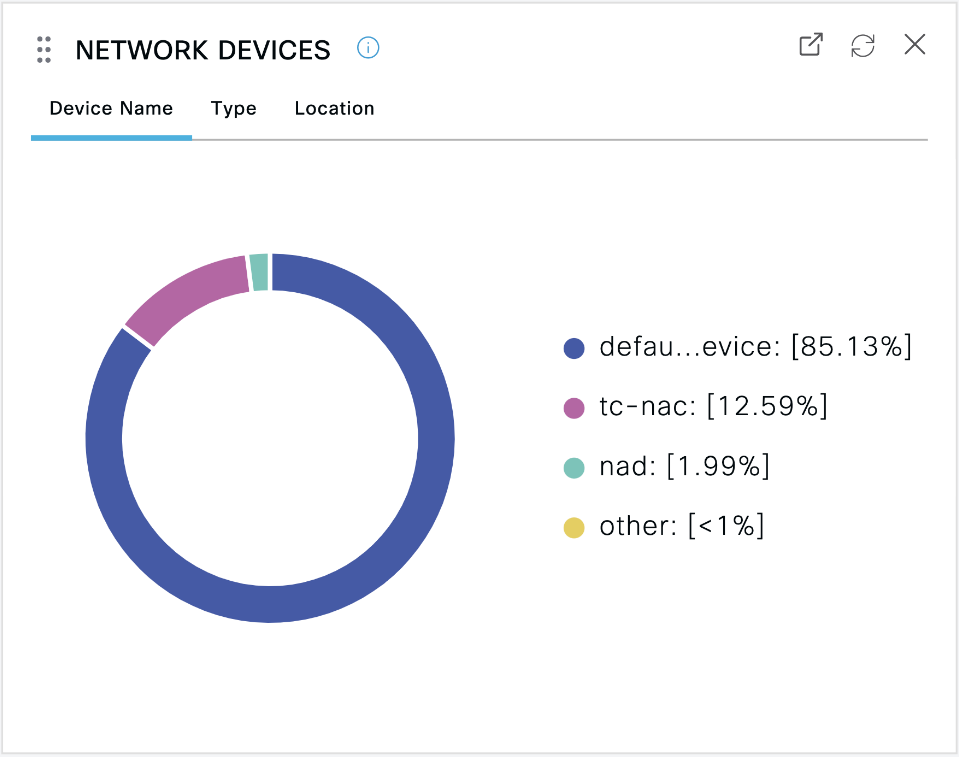
1. The Open New Window icon opens this dashlet in a new browser window. The pie chart refreshes. Click the **X** to delete this dashlet. This option is only available on the home page. You delete dashlets in Context Visibility windows using the gear symbol in the top-right corner of the screen.
2. Some dashlets have different categories of data. Click the category to see a pie chart with that set of data.
3. The pie chart shows the data that you have selected. Click one of the pie segments to open a new tab in with the filtered data, based on that pie segment.

Click a section of the pie chart in a home page dashboard to open the chart in a new browser window. The new window displays data that is filtered by the section of the pie chart that you clicked on.

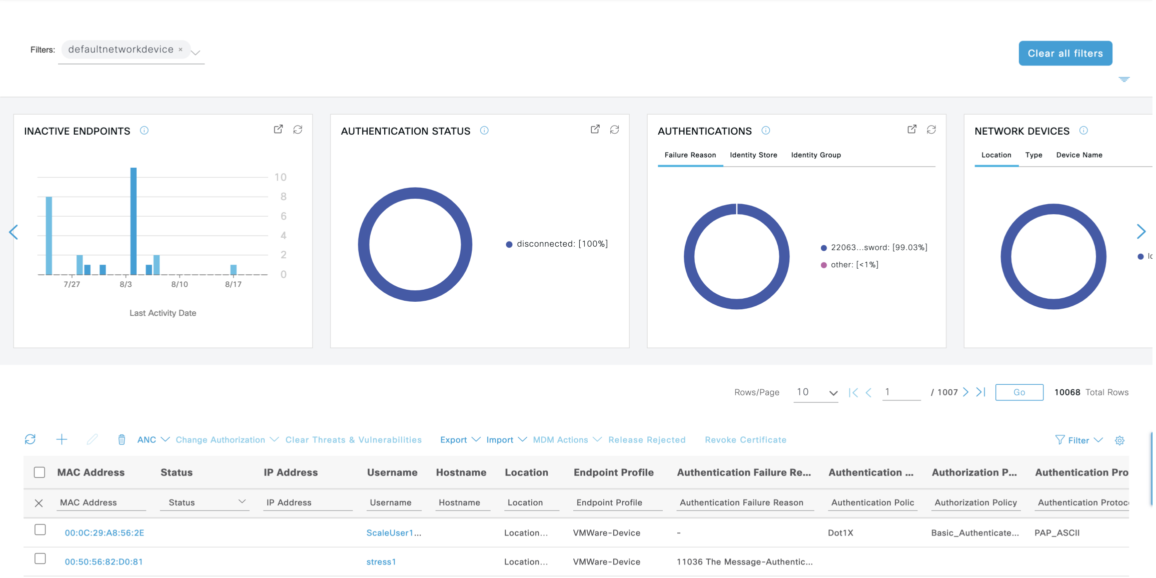
When you click a section of the pie chart in a Context Visibility window, the displayed data is filtered but context does not change. You view the filtered data in the same browser window.

Filtering Displayed Data in a View

When you click a dashlet in a Context Visibility window, the corresponding data is filtered by the item you click and displayed. For example, when you click a section of a pie chart, the data for the chosen section is filtered and displayed.


NETWORK DEVICES
Device Name
Type
Location
defau...evice: [85.13%]
tc-nac: [12.59%]
nad: [1.99%]
other: [<1%]

If you click **defau...evice** in the **Network Devices** dashlet, a new window displays the data, as shown in the following image:


Filters: defaultnetworkdevice ×
Clear all filters
INACTIVE ENDPOINTS
10
8
6
4
2
0
7/27
8/3
8/10
8/17
Last Activity Date
AUTHENTICATION STATUS
disconnected: [100%]
AUTHENTICATIONS
Failure Reason
Identity Store
Identity Group
22063...sword: [99.03%]
other: [<1%]
NETWORK DEVICES
Location
Type
Device Name
Rows/Page 10
1 / 1007
Go
10068 Total Rows
ANC
Change Authorization
Clear Threats & Vulnerabilities
Export
Import
MDM Actions
Release Rejected
Revoke Certificate
Filter

☐	MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authentication Failure Re...	Authentication ...	Authorization P...	Authentication Pro
×	MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authentication Failure Reason	Authentication Polic	Authorization Policy	Authentication Protoc
☐	00:0C:29:A8:56:2E			ScaleUser1...		Location...	VMWare-Device	-	Dot1X	Basic_Authenticate...	PAP_ASCII
☐	00:50:56:82:D0:81			stress1		Location...	VMWare-Device	11036 The Message-Authentic...			

Filter the data further by clicking more sections of the pie charts. You can also use the **Filter** drop-down list or the gear icon at the top-right corner of the list of data to manage the data displayed.

Save your custom filters.

Create Custom Filters

Create and save user-specific custom filters that are accessible only to you. Other users logging in to Cisco ISE cannot view the custom filters that you create. These custom filters are saved in the Cisco ISE database. You can access them from any computer or browser with which you log in to Cisco ISE.

Step 1 Click **Filter** and choose **Advanced Filter** from the drop-down list.

Step 2 Specify the search attributes, such as fields, operators, and values from the Filter menus.

Step 3 Click **+** to add more conditions.

Step 4 Click **Go** to display the entries that match the specified attributes.

Step 5 Click **Save** to save the filter.

Step 6 Enter a name and click **Save**. The filter now appears in the **Filter** drop-down list.

Filter Data by Conditions Using the Advanced Filter

The Advanced Filter allows you to filter information based on specified conditions, such as, First Name = Mike and User Group = Employee. You can specify more than one condition.

Step 1 Click **Filter** and choose **Advanced Filter** drop-down list.

Step 2 Specify search the search attributes, such as fields, operators, and values from the filter menus.

Step 3 Click **+** to add more conditions.

Step 4 Click **Go** to view the entries that match the specified attributes.

Filter Data by Field Attributes Using the Quick Filter

The Quick Filter allows you to enter a value for any of the field attributes displayed in the listing page, refreshes the page, and lists only those records that match your filter criteria.

Step 1 Click **Filter** and choose **Quick Filter** from the drop-down list.

Step 2 Enter search criteria in one or more of the attribute fields, and the entries that match the specified attributes display automatically.

Endpoint Actions in Dashlet Views

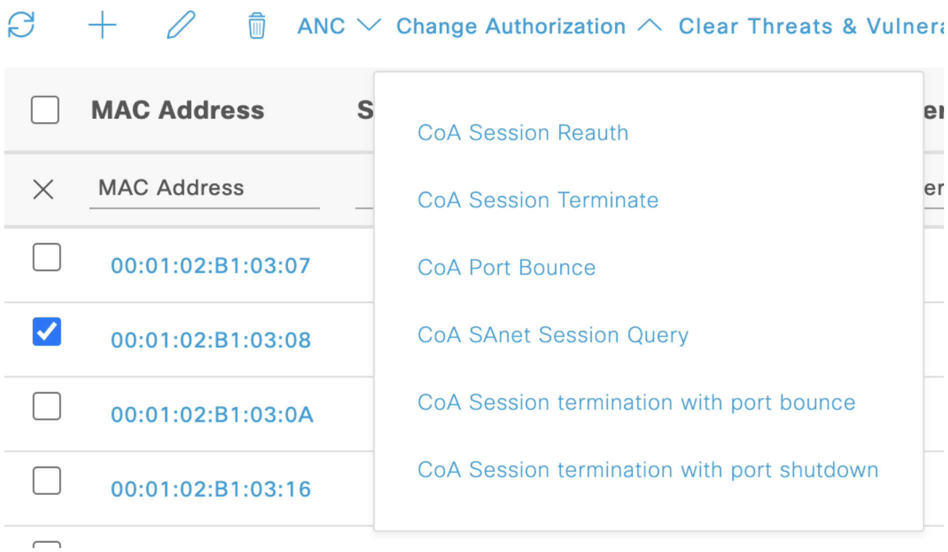
The toolbar at the top of the list allows you to act on endpoints in the list that you select. Not all actions are enabled for every list. Some actions depend on the feature that is enabled for use. The following list shows two endpoint actions that must be enabled in Cisco ISE before you can use them.

- **Adaptive Network Control Actions**

If you enable the Adaptive Network Control service, you can select endpoints in the list and assign or revoke network access. You can also issue a change of authorization.

When you click the pie chart on a home page dashlet, the new window that is displayed contains the options **ANC** and **Change Authorization**. Check the check box for the endpoint you want to perform an action on, and choose the necessary action from the drop-down lists of**ANC** and **Change Authorization**.

Figure 6: Endpoint Actions in Dashlet Views


ANC
Change Authorization
Clear Threats & Vulnera
MAC Address
MAC Address
☐ 00:01:02:B1:03:07
☑ 00:01:02:B1:03:08
☐ 00:01:02:B1:03:0A
☐ 00:01:02:B1:03:16
CoA Session Reauth
CoA Session Terminate
CoA Port Bounce
CoA SAnet Session Query
CoA Session termination with port bounce
CoA Session termination with port shutdown

- **MDM Actions**

  If you connect an MDM server to Cisco ISE, you can perform MDM actions on selected endpoints. Choose the necessary action from the **MDM Actions** drop-down list.

Cisco ISE Dashboard

The Cisco ISE dashboard or home page (click the **Menu** icon (☰) and choose **Dashboard**) is the landing page that you view after you log in to the Cisco ISE administration portal. The dashboard is a centralized management console consisting of metric meters along the top of the window, with dashlets below. The default dashboards are **Summary**, **Endpoints**, **Guests**, **Vulnerability**, and **Threat**. See Cisco ISE Home Dashboards, on page 238.

Note You can view this dashboard data only in the Cisco ISE primary PAN portal.

The dashboard's real-time data provides an at-a-glance status of the devices and users accessing your network, and an overview of the system's health.

Click the gear icon in the second level menu bar for a drop-down list of dashboard settings. The following table contains descriptions for the dashboard settings options available in the drop-down list:

Drop-Down List Option	Description
Add New Dashboard	You can have a maximum of 20 dashboards, including the five default dashboards.
Rename Dashboard	(This option is available only for custom dashboards) To rename a dashboard: **1.** Click **Rename Dashboard**. **2.** Specify a new name. **3.** Click **Apply**.
Add Dashlet	To add a dashlet to the home page dashboard: **1.** Click **Add Dashlet(s)**. **2.** In the **Add Dashlets** window, click **Add** next to the dashlets that you want to add. **3.** Click **Save**. **Note** You can add a maximum of nine dashlets per dashboard.
Export	You can export the dashboard data as a PDF or a CSV file. **1.** Click **Export**. **2.** In the **Export** dialog box, click the radio button next to one of the following file formats: • **PDF**: Choose the PDF format for a snapshot view of the selected dashlets. • **CSV**: Choose the CSV format to download the selected dashboard data as a zip file. **3.** In the **Export** dialog box, check the check boxes next to the dashlets you want to export. **4.** Click **Export**. The zip file contains individual dashlet CSV files for the selected dashboard. Data related to each tab in a dashlet is displayed as separate sections in the corresponding dashlet CSV file. When you export a custom dashboard, the zip file is exported with the same name. For example, if you export a custom dashboard that is named MyDashboard, then the exported file's name is MyDashboard.zip.

Drop-Down List Option	Description
Layout Template	You can change the layout of the template in which the dashlets are displayed. To change the layout: 1. Click **Layout Template**. 2. Select the required layout from the options available.
Manage Dashboards	Click **Manage Dashboards** and choose one of the following options: • **Mark as Default Dashboard**: Use this option to set a dashboard as your default dashboard (the home page). • **Reset all Dashboards**: Use this option to reset all the dashboards to their original settings.

You can delete a dashboard that you have created by clicking the close (**x**) icon next to the corresponding custom dashboard.

Note You cannot rename or delete a default dashboard.

Each dashlet has a toolbar at the top-right corner where you can perform the following operations:

- Detach: To view a dashlet in a separate window.
- Refresh: To refresh a dashlet.
- Remove: To remove a dashlet from the dashboard.

You can drag and drop the dashlet using the gripper icon that is present at the top-left corner of the dashlet.

The Alarms dashlet contains a quick filter for the **Severity** column. You can filter alarms by their severity by choosing **Critical**, **Warning**, or **Info** from the **Severity** drop-down list.

Cisco ISE Internationalization and Localization

Cisco ISE internationalization adapts the user interface to the supported languages. Localization of the user interface incorporates location-specific components and translated text. In Windows, MAC OSX, and Android devices, the native supplicant provisioning wizard can be used in any of the following supported languages.

In Cisco ISE, internalization and localization support focuses on support for non-English text in UTF-8 encoding to the end user-facing portals and on selective fields in the administration portal.

Supported Languages

Cisco ISE provides localization and internalization support for the following languages and browser locales.

Table 21: Supported Languages and Locales

Language	Browser Locale
Chinese traditional	zh-tw
Chinese simplified	zh-cn
Czech	cs-cz
Dutch	nl-nl
English	en
French	fr-fr
German	de-de
Hungarian	hu-hu
Italian	it-it
Japanese	ja-jp
Korean	ko-kr
Polish	pl-pl
Portuguese (Brazil)	pt-br
Russian	ru-ru
Spanish	es-es

End-User Web Portal Localization

The Guest, Sponsor, My Devices, and Client Provisioning portals are localized into all the supported languages and locales. This includes text, labels, messages, field names, and button labels. If a client browser requests a locale that is not mapped to a template in Cisco ISE, the portal displays content using the English template.

Using the administration portal, you can modify the fields that are used in the Guest, Sponsor, and My Devices portals for each language. You can also add other languages. Currently, you cannot customize these fields for the Client Provisioning portal.

You can further customize the Guest portal by uploading HTML pages to Cisco ISE. When you upload customized pages, you are responsible for the appropriate localization support for your deployment. Cisco ISE provides a localization support example with sample HTML pages, which you can use as a guide. Cisco ISE allows you to upload, store, and render custom internationalized HTML pages.

Note NAC and MAC agent installers, and WebAgent pages are not localized.

Support for UTF-8 Character Data Entry

Cisco ISE fields that are exposed to the end user (through the Cisco client agent or supplicants, or the Sponsor, Guest, My Devices, and Client Provisioning portals) support UTF-8 character sets for all languages. UTF-8 is a multibyte character encoding for the Unicode character set, which includes many different language character sets including Hebrew, Sanskrit, and Arabic.

Character values are stored in UTF-8 in the administration configuration database, and the UTF-8 characters display correctly in reports and user interface components.

UTF-8 Credential Authentication

Network access authentication supports UTF-8 username and password credentials. This includes RADIUS, Extensible Authentication Protocol (EAP), RADIUS proxy, RADIUS token, and web authentication from the Guest and administration portal login authentications. UTF-8 support for username and password applies to authentication against the local identity store and external identity stores.

UTF-8 authentication depends on the client supplicant that is used for network login. Some Windows native supplicants do not support UTF-8 credentials.

Note UTF-8 authentication with RSA is not supported as RSA does not support UTF-8 users. RSA servers, which are compatible with Cisco ISE, also do not support UTF-8.

UTF-8 Policies and Posture Assessment

Policy rules in Cisco ISE that are conditioned on attribute values may include UTF-8 text. Rule evaluation supports UTF-8 attribute values. You can also configure conditions with UTF-8 values through the administration portal.

Posture requirements are modified as File, Application, and Service conditions based on a UTF-8 character set.

UTF-8 Support for Messages Sent to Supplicant

RSA prompts and messages are forwarded to the supplicant using a RADIUS attribute REPLY-MESSAGE, or within EAP data. If the text contains UTF-8 data, it is displayed by the supplicant, based on the client's local operating system language support. Some Windows-native supplicants do not support UTF-8 credentials.

Cisco ISE prompts and messages may not be in synchrony with the locale of the client operating system on which the supplicant is running. You must align the end-user supplicant locale with the languages that are supported by Cisco ISE.

Reports and Alerts UTF-8 Support

Monitoring and troubleshooting reports and alerts support UTF-8 values for relevant attributes for the languages that are supported in Cisco ISE. The following activities are supported:

- Viewing live authentications.
- Viewing detailed pages of report records.
- Exporting and saving reports.
- Viewing the Cisco ISE dashboard.
- Viewing alert information.
- Viewing tcpdump data.

UTF-8 Character Support in the Portals

More character sets are supported in Cisco ISE fields (UTF-8) than are currently supported for localizations in portals and end-user messages. For example, Cisco ISE does not support right-to-left languages, such as Hebrew or Arabic, although the character sets themselves are supported.

The following table lists the fields in the Admin and end-user portals that support UTF-8 characters for data entry and viewing, with the following limitations:

- Cisco ISE does not support guest usernames and passwords with UTF-8 characters.
- Cisco ISE does not support UTF-8 characters in certificates.

Table 22: Administration Portal UTF-8 Character Fields

Administration Portal Element	UTF-8 Fields
Network access user configuration	• **Username** The usernames can contain any combination of upper and lowercase letters, numbers, space, and special characters (except `, %, ^, ;, :, [, {, |, },], \, ‘, “, =, <, >, ?, !, and control characters). You cannot submit usernames with only spaces. • **First Name** • **Last Name** • **Email**
User list	• All filter fields. • Values displayed in the User List window. • Values displayed in the left navigation quick view.

Administration Portal Element	**UTF-8 Fields**
User password policy	The passwords can contain any combination of upper and lowercase letters, numbers, and special characters (including !, @, #, $, ^, &, *, (, and). The password field accepts any characters including UTF-8 characters, but it does not accept control characters. Some languages do not have uppercase or lowercase alphabets. If your user password policy requires the user to enter a password with uppercase or lowercase characters and the user's language does not support these characters, the user cannot set a password. For the user password field to support UTF-8 characters, uncheck the following check boxes in the user password policy page (Click the **Menu** icon and choose**Administration** > **Identity Management** > **Settings** > **User Authentication Settings** > **Password Policy**): • **Lowercase alphabetic characters** • **Uppercase alphabetic characters** You cannot use dictionary words, their characters in reverse order, or their letters replaced with other characters.
Administrator list	• All filter fields. • Values that aredisplayed in the administrator list window. • Values that are displayed in the left navigation quick view.
Admin login page	• **Username**
RSA	• Messages • Prompts
RADIUS token	• Authentication tab > Prompt
Posture Requirement	• Name • Remediation action > Message shown to Agent User • Requirement list display
Posture conditions	The following fields in the **Policy** > **Policy Elements** > **Conditions** > **Posture** windows: • **File Condition** > **Add** > **File Path**. • **Application Condition** > **Add** > **Process Name**. • **Service Condition** > **Add** > **Service Name**. • Conditions list displays.

Administration Portal Element	UTF-8 Fields
Guest and My Devices settings	• Sponsor > Language Template: all supported languages, all fields. • Guest > Language Template: all supported languages, all fields. • My Devices >Language Template: all supported languages, all fields.
System settings	• SMTP Server > Default email address
Operations > Alarms > Rule	• Criteria > User • Notification > email notification user list
Operations > Reports	• Operations > Live Authentications > Filter fields • Operations > Reports > Catalog > Report filter fields
Operations > Troubleshoot	• General Tools > RADIUS Authentication Troubleshooting > Username
Policies	• Authentication > value for the antivirus expression within policy conditions • Authorization or posture or client provisioning > other conditions > value for the antivirus expression within policy conditions
Attribute value in policy library conditions	• Authentication > simple condition or compound condition > value for the antivirus expression • Authentication > simple condition list display • Authentication > simple condition list > left navigation quick view display • Authorization > simple condition or compound condition > value for the antivirus expression • Authorization > simple condition list > left navigation quick view display • Posture > Dictionary simple condition or dictionary compound condition > value for the antivirus expression • Guest > simple condition or compound condition > value for the antivirus expression

UTF-8 Support Outside the Cisco ISE User Interface

This section contains the areas outside the Cisco ISE user interface that provide UTF-8 support.

Debug Log and CLI-Related UTF-8 Support

Attribute values and posture condition details appear in some debug logs. All debug logs accept UTF-8 values. You can download debug logs containing raw UTF-8 data that can be viewed with a UTF-8-supported viewer.

Cisco Secure ACS Migration UTF-8 Support

Cisco ISE allows the migration of Cisco Secure Access Control Server (ACS) UTF-8 configuration objects and values. Migration of some UTF-8 objects may not be supported by Cisco ISE UTF-8 languages, which might render some of the UTF-8 data that is provided during migration unreadable using the administration portal or report methods. Convert the unreadable UTF-8 values (that are migrated from Cisco Secure ACS) into ASCII text. For more information about migrating from Cisco Secure ACS to Cisco ISE, see the Cisco Secure ACS to Cisco ISE Migration Tool for your version of Cisco ISE.

Support for Importing and Exporting UTF-8 Values

The administration and Sponsor portals support plaintext and CSV files with the UTF-8 values to use when importing user account details. Exported files are provided as CSV files.

UTF-8 Support on REST

External Representational State Transfer (REST) communication supports UTF-8 values. This applies to configurable items that have UTF-8 support in the Cisco ISE user interface, except for administrator authentication. Administrator authentication in REST requires ASCII text credentials for login.

UTF-8 Support for Identity Stores Authorization Data

Cisco ISE allows Microsoft Active Directory and Lightweight Directory Access Protocol (LDAP) to use UTF-8 data in authorization policies for policy processing.

MAC Address Normalization

Cisco ISE supports normalization of the MAC address that you enter in any of the following formats:

- 00-11-22-33-44-55
- 0011.2233.4455
- 00:11:22:33:44:55
- 001122334455
- 001122-334455

Provide full or partial MAC addresses in the following Cisco ISE windows:

- **Policy** > **Policy Sets**
- **Policy** > **Policy Elements** > **Conditions** > Authorization
- Authentications > Filters (Endpoint and Identity columns)
- Global search
- **Operations** > **Reports** > Report Filters
- **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **Endpoint Debug**

Provide full MAC addresses (six octets separated by ':' or '-' or '.') in the following Cisco ISE windows:

- Operations > Adaptive Network Control

- **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **RADIUS Authentication Troubleshooting**
- **Operations** > **Troubleshooting** > **Diagnostic Tools** > **General Tools** > **Posture Troubleshooting**
- Administration > Identities > Endpoints
- **Administration** > **System** > **Deployment**
- **Administration** > **Logging** > **Collection Filters**

REST APIs also support normalization of full MAC address.

The valid ranges for an octet are 0 to 9, a to f, or A to F.

Cisco ISE Deployment Upgrade

Cisco ISE offers a GUI-based centralized upgrade from the administration portal. The progress of the upgrade and the status of the nodes are displayed in the Cisco ISE GUI. For information on the preupgrade and postupgrade tasks you must carry out, see the *Cisco Identity Services Engine Upgrade Guide* for the Cisco ISE release that you want to upgrade to.

The upgrade **Overview** window (**Administration** > **System** > **Upgrade** > **Overview** lists all the nodes in your deployment, the personas that are enabled on them, the Cisco ISE version that is currently in use, and the status (whether a node is active or inactive) of each node. You can begin upgrade only if all the nodes are in the **Active** state.

Administrator Access Console

The following steps describe how to log in to the administrative portal.

Step 1 Enter the Cisco ISE URL in the address bar of your browser (for example, https://<ise hostname or ip address>/admin/).

Step 2 Enter the username and case-sensitive password that were specified and configured during the initial Cisco ISE setup.

Step 3 Click **Login** or press **Enter**.

If your login is unsuccessful, click the **Problem logging in?** link in the log in window and follow the instructions that are displayed.

Administrator Login Browser Support

The Cisco ISE administration portal supports the following HTTPS-enabled browsers:

- Mozilla Firefox 107 and earlier versions from version 82
- Mozilla Firefox ESR 102.4 and earlier versions
- Google Chrome 107 and earlier versions from version 86
- Microsoft Edge, the latest version and one version earlier than the latest version

ISE Community Resource

ISE Pages Fail to Fully Load When Adblock Plus is Used

Administrator Lockout Because of Login Attempts

If you enter an incorrect password for an administrator user ID enough times, the account is either suspended for a specified time or locked out (as configured). If Cisco ISE is configured to lock you out, the administration portal locks you out of the system. Cisco ISE adds a log entry in the Server Administrator Logins report and suspends the credentials for that administrator ID. Reset the password for that administrator ID as described in the Section "Reset a Disabled Password Due to Administrator Lockout" in the Cisco Identity Services Engine Installation Guide. The number of failed login attempts allowed before an administrator account is disabled is configured as described in the Section of the *Cisco Identity Services Engine Administrator Guide*. After an administrator user account is locked out, Cisco ISE sends an email to the associated user, if this information is configured.

Only an administrator with the role of Super Admin (including Microsoft Active Directory users) can configure the disable administrator access option.

Configure Proxy Settings in Cisco ISE

If your existing network topology requires you to use a proxy server to enable Cisco ISE to access external resources (such as the remote download site where you can find client provisioning and posture-related resources), use the administration portal to configure the proxy settings.

The proxy settings impact the following Cisco ISE functions:

- Partner Mobile Management
- Endpoint Profiler Feed Service Update
- Endpoint Posture Update
- Endpoint Posture Agent Resources Download
- Certificate Revocation List (CRL) Download
- Guest Notifications
- SMS Message Transmission
- Social Login
- Microsoft Entra ID
- pxGrid Cloud

The Cisco ISE proxy configuration supports basic authentication for proxy servers. NT LAN Manager (NTLM) authentication is not supported.

Note When you select OAuth Authentication Type for MDM configuration and integration , Cisco ISE uses NTLM authentication for proxy servers.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Proxy**.

Step 2 Enter the proxy IP address or DNS-resolvable hostname, and specify the port through which proxy traffic travels to and from Cisco ISE in the **Proxy host server : port** field.

Step 3 Check the **Password required** check box, if necessary.

Step 4 Enter the username and password that are used to authenticate to the proxy servers in the **User Name** and **Password** fields. Reenter the password in the **Confirm Password** field.

Step 5 Enter the IP address or the address range of hosts or domains that must be bypassed in the **Bypass proxy for these hosts and domain** text box.

Step 6 Click **Save**.

Ports Used by the Administration Portal

The administration portal uses HTTP port 80 and HTTPS port 443 and you cannot change these settings. You cannot configure any of the end user portals to use these ports, to reduce the risk to the administration portal.

Set Up the Cisco ISE Application Programming Interface Gateway

The Cisco ISE API Gateway is an API management solution that acts as a single entry point to multiple Cisco ISE service APIs to provide better security and traffic management. API requests from external clients are routed to the API Gateway in Cisco ISE. The requests are forwarded to the Cisco ISE nodes where service APIs are running, based on an internal algorithm.

From Cisco ISE Release 3.1 onwards, the MnT (Monitoring) APIs, the ERS APIs and the Open APIs all are routed through the API Gateway. The following ports need to opened between the API gateway node and all other nodes in the deployment for the respective APIs.

- MnT APIs: 9443
- Open APIs: 9070
- ERS APIs: 9060

You can choose the Cisco ISE nodes on which you want to enable the API Gateway. We recommend that you run the API Gateway on at least two nodes in your Cisco ISE deployment.

The API Gateway is always enabled on a standalone node even if the ERS and Open API services are disabled on that node. In case of a distributed deployment, the API Gateway is enabled by default on the primary PAN, provided the API Gateway is not enabled on any other node in the deployment.

Step 1 Log in to the primary PAN.

Step 2 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **API Settings** > **API Gateway Settings**.

Step 3 In the **ISE API Gateway Nodes List** area, check the check boxes next to the nodes on which you want to enable the API Gateway.

Step 4 Click **Enable**.

Troubleshooting

To troubleshoot issues that are related to the API Gateway, set the **Log Level** for the following components to **DEBUG** in the **Debug Log Configuration** window. (To view this window, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Debug Wizard** > **Debug Log Configuration**.)

- **ise-kong**
- **kong**

The logs can be downloaded from the **Download Logs** window. (To view this window, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Download Logs**.) You can choose to download either a support bundle from the **Support Bundle** tab (by clicking the **Download** button on the tab), or download the kong debug logs from the **Debug Logs** tab (by clicking the **Log File** value for **kong** debug log).

Verification

If you are able to log in to the Cisco ISE primary PAN successfully every time, the API Gateway setup is working as expected.

Note If REST APIs are accessed through API Gateway on a different tab in the same web browser where the GUI is logged in, the GUI gets logged out.

This happens only when the API is served by remote nodes other than API Gateway node.

From Cisco ISE 3.0 onwards, the UI services on port 443 are served through a docker service, which may result in behaviour change in cases that involve a multiple Network Interface Controller (NIC) scenario. You may need to adjust the routes to make sure the packets are routed through the intended interface or gateway based on the specific need, using the **ip route** command from the admin shell. For more information on using the **ip route** command, see the *Cisco ISE CLI Commands in Configuration Mode* section in the Cisco ISE CLI Reference Guide.

Enable API Service

The Cisco ISE API service provides a framework for developing and deploying web applications in the Cisco ISE environment. This feature documents the REST APIs, that can be used to generate code in different languages as well as share them across users for understanding the APIs. The Cisco ISE API service is based on OpenAPI specification, which is a broadly accepted industry standard for describing REST APIs.

The API Gateway must be enabled for accessing an API service. All API service requests enter Cisco ISE through the API Gateway in both standalone and distributed Cisco ISE deployments. The API Gateway receives API service requests through port 443.

In the standalone Cisco ISE node, after receiving the API request, the API Gateway forwards the request to the API service.

In a distributed environment, the read requests are forwarded to either a PSN or a primary PAN, but the write requests are forwarded only to the primary PAN. The primary PAN is the only node that has the write authority in the deployment environment.

Cisco ISE allows API access to manage Cisco ISE nodes through two sets of API formats:

- **External RESTtful Services APIs**

  External RESTful Services (ERS) APIs are REST APIs that are based on the HTTPS protocol and operate over the standard HTTPS port 443 (port 9060 can also be used). The ERS APIs support basic authentication. The authentication credentials are encrypted and are part of the request header. You can use any REST client such as JAVA, cURL Linux command, Python, or any other client to invoke External RESTful Services' API calls.

  Note

  - ERS APIs support TLS 1.1 and TLS 1.2, but not TLS 1.0 even if TLS 1.0 has been enabled in the **Security Settings** window (**Administration** > **System** > **Settings** > **Security Settings**). Enabling TLS 1.0 in the **Security Settings** window is related to only the EAP protocol and does not impact ERS APIs.
  - ERS session idle timeout is 60 sec. If several requests are sent during this period, the same session is used with the same Cross-Site Request Forgery (CSRF) token. If the session has been idle for more than 60 sec, the session is reset and a new CSRF token is used.
  - Cisco ISE admin passwords cannot be changed using REST APIs.

  For the SDK definition for ERS APIs, visit https://<*ise-ip*>:9060/ers/sdk or https://<ise-ip>/ers/sdk. You can also find this information in the **Overview** section of the **API Settings** window (**Administration** > **System** > **Settings** > **API Settings** > **Overview**).

  The ERS service is enabled by default when the Amazon Machine Image (AMI) version of Cisco ISE is deployed in the VMware Cloud environment. This helps in easy integration of Cisco ISE with other Cisco products and third-party applications, without the need to enable the ERS service from the Cisco ISE GUI.

  Note The userdata retrieval only works for Metadata version V1 (IMDSv1), it does not work with V2.

  Open API specification for ERS

  The Open API specification (JSON file) for ERS APIs is available for download in Cisco ISE in the **Overview** section of the **API Settings** window (**Administration** > **System** > **Settings** > **API Settings** > **Overview**). This Open API JSON file can be used for auto-generation of API client code using any programming language such as python, JAVA and so on. For additional information about Open API specifications and tools, see https://openapi.tools/.

- **Open APIs**

Open APIs are REST APIs based on HTTPS, operating in port 443. From Cisco ISE Release 3.1, newer APIs are available in the Open API format. For more information on Cisco ISE Open APIs, go to https://<*ise-ip*>/api/swagger-ui/index.html or Cisco ISE Open APIs.

Note In a Cisco ISE cloud setup, the firewall rule should be opened using iptables to access the API documentation page in AWS cloud.

The following Open APIs have been introduced in Cisco ISE, Release 3.1:

- **Repository:** These APIs provide the ability to manage the repositories. You can create, retrieve, update, and delete the repository configuration and list the files from the configured repositories.
- **Backup and Restore:** These APIs provide the ability to manage the backup and restore operations. They enable you to create, cancel, update, and restore the configuration backup, and also list the status of the last backup. Users can create and edit the backup schedule as well.
- **Certificate:** These APIs provide the ability to manage certificates. They enable you to create, retrieve, update, and delete system certificates, and trusted certificates, create Certificate Signing Requests (CSRs), and export and import certificates. Generate self-signed certificate API is available from Cisco ISE Release 3.1 Patch 1 onwards.
- **Policy:** These APIs provide the ability to manage policies. They are of two types:
    - **RADIUS Policy:** These APIs provide the ability to manage RADIUS policies. They enable you to get lists of all the required boundaries (Authorization Profile, SecurityGroup, IdentityStores, Profiles) and the Discovery Dictionary Filter Helper. These APIs allow Dictionaries and Attributes management, Conditions management (Library, Network, Time, and Date Conditions), and Policy Set management, including AuthN rules, Authz rules, Exception rules, and Global Exception rules.
    - **TACACS+ Policy:** These APIs provide the ability to manage TACACS+ Policies. They enable you to get lists of all the required boundaries (Command Sets, TACACS Profiles, IdentityStores, ServiceNames) and Discovery of Dictionary related to TACACS Helper. These APIs allow Conditions management (Library, Network, Time and Date Conditions), and Policy Set management including AuthN rules, Authz rules, Exception rules, and Global Exception rules.
- **TrustSec**: These APIs provide the ability to manage TrustSec related operations such as Virtual Networks(VNs), Security Group - Virtual Network mappings(SG-VN mappings), and VN-VLAN mappings.
- **Task Service**: These APIs provide the ability to monitor the status of various tasks carried out in Cisco ISE.
- **Deployment**: These APIs provide the ability to configure the Cisco ISE nodes and set up the deployment.
- **Patch and Hot Patch**: These APIs provide the ability to carry out patch related operations such as installing a patch, removing a patch, listing all the installed patches and so on.

Note This API works only when primary PAN services are up. If the primary PAN services are down, the API call on the secondary PAN fails.

- **License**: These APIs provide the ability to register, enable and manage smart licensing.
- **System Settings**: These APIs provide the ability to configure and update proxy settings and transport gateway settings in Cisco ISE.

Note The IP address present in the OpenAPI requests, and coming from a subnet is expected to be shown as a remote IP address from that network.

You must assign special privileges to a user operating on API services. API service users can be either internal users or belong to an external Microsoft Active Directory group. The internal users or the Active Directory group to which the external users belong must be mapped to either **ERS Admin** or **ERS Operator** groups:

- **ERS Admin**: These users can create, read, update, and delete External RESTful Services API requests. They have full access to all External RESTful Services APIs (GET, POST, DELETE, and PUT).
- **ERS Operator**: These users have read-only access (GET requests only).
- **MnT Admin**: These users can create, read, update, and delete Monitoring REST APIs.

Note A user with the Super Admin role can access all the API services.

In the **Authentication Method** window, from the **Identity Source** drop-down list, choose an option that will apply to the API authentication configuration you choose. However, certificate-based API authentication only supports the **Internal** identity source.

API services are disabled by default. If you evoke any API calls before you enable the API services in Cisco ISE, you receive an error message. Enable the Cisco ISE REST API feature for the applications developed for a Cisco ISE REST API to be able to access Cisco ISE. The ERS APIs use the standard HTTPS port 443 (port 9060 can also be used) and the Open APIs use the HTTPS port 9070. Both these ports are disabled by default. If the API services are not enabled in the Cisco ISE administration server, the client application receives a timeout error from the server for any guest REST API requests.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **API Settings** > **API Service Settings**.

Step 2 In the **API Service Settings for Primary Administration Node** area, click the **ERS (Read/Write)** toggle button to enable External RESTful Services in the Primary Administration Node (PAN), or click the **Open API (Read/Write)** toggle button to enable Open API services in the PAN.

Step 3 In the **API Service Settings for All Other Nodes** area, click the **ERS (Read/Write)** toggle button to enable External RESTful Services in all the other nodes, or click the **OpenAPI (Read/Write)** toggle button to enable Open API services in all the other nodes.

Step 4 In the **CSRF Check** area, click the radio button for one of the following options:

- **Use CSRF Check for Enhanced Security**: If this option is enabled, the External RESTful Services client must send a GET request to fetch the CSRF token from Cisco ISE and include the CSRF token in the requests that are sent to Cisco ISE. Cisco ISE will then validate a CSRF token when a request is received from the External RESTful Services client. Cisco ISE processes the request only if the token is valid. This option is not applicable for External RESTful Services clients in releases earlier than Cisco ISE Release 2.3.

- **Disable CSRF for ERS Request**: If this option is enabled, CSRF validation is not performed. This option can be used for External RESTful Services clients in releases earlier than Cisco ISE Release 2.3.

Step 5 Click **Save**.

Note When a Cisco ISE node is registered to PAN, the OpenAPI defaults to disabled from a prior-enabled state. Enable OpenAPI again in the Cisco ISE GUI following the procedure outlined above to maintain zero-touch OpenAPI deployment.

Cisco ISE provides different APIs for GET and UPDATE operations:

GET:

- **URL**: https://<*ise-node*>/admin/API/apiService/get
- **Response**: {"id": "1234","papIsEnabled":false,"psnsIsEnabled":true}

UPDATE:

- **URL**: https://<*ise-node*>/admin/API/apiService/update
- **Request Body**: {"papIsEnabled":false,"psnsIsEnabled":false}
- **Response**: {"id": "1234","papIsEnabled":false,"psnsIsEnabled":false}

Troubleshooting

All REST operations are audited and the logs are logged in the system logs. To troubleshoot issues that are related to the Open APIs, set the **Log Level** for the **apiservice** component to **DEBUG** in the **Debug Log Configuration** window. To troubleshoot issues relating to the ERS APIs, set the **Log Level** for the **ers** component to **DEBUG** in the **Debug Log Configuration** window (To view this window, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Debug Wizard** > **Debug Log Configuration**).

You can download the logs from the **Download Logs** window (To view this window, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Download Logs**). You can choose to download either a support bundle from the **Support Bundle** tab (by clicking the **Download** button under the tab), or download the **api-service** debug logs from the **Debug Logs** tab (by clicking the **Log File** value for the api-service debug log).

Verification

If you are able to access the API service GUI page, for example, https://<*iseip*>:<*port*>/api/swagger-ui/index.html or https://<*iseip*>/ers/sdk, the API service is working as expected.

Related Topics

External RESTful Services Software Development Kit , on page 267

Enable External Active Directory Access for API Services

Step 1 In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

Step 2 Add the Active Directory groups that the external user belongs to as an external identity source.

Step 3 Add user groups from the Active Directory.

Step 4 In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration** > **Admin Access** > **Authentication** > **Authentication Method**.

Step 5 From the **Identity Source** drop-down list, choose **AD: <Join Point Name>**.

Step 6 Choose either **Password Based** or **Client Certificate Based** authentication by clicking the corresponding radio button.

Step 7 Choose **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Groups**.

Step 8 Click **ERS Admin** group or **ERS Operator** from the list of administration groups.

Step 9 Click **Add** to add the external group to the administrator group as a member user.

Step 10 Click **Save**.

Note In Cisco ISE Release 3.1, if the external ID store is configured for Admin access in Cisco ISE GUI under **Administration > System > Admin Access > Authentication**, an Internal Admin user cannot be assigned the ERS Admin role. Only an External Admin user can be assigned the ERS Admin role.

External RESTful Services Software Development Kit

Use the External RESTful Services (ERS) software development kit (SDK) to build your own tools. You can access the External RESTful Services SDK with the URL https://<ISE-ADMIN-NODE>:9060/ers/sdk. Only users with the role **ERS Admin** can access the External RESTful Services SDK.

The SDK consists of the following components:

- Quick reference API documentation.
- A complete list of all available API operations.
- Schema files available for download.
- Sample application in Java available for download.
- Use cases in cURL script format.
- Use cases in Python script format.
- Instructions on using Chrome Postman.

Specify System Time and Network Time Protocol Server Settings

Cisco ISE allows you to configure up to three NTP servers. Use the NTP servers to maintain accurate time and synchronize time across different timezones. You can also specify whether Cisco ISE must use only authenticated NTP servers and enter one or more authentication keys for that purpose.

We recommend that you set all the Cisco ISE nodes to the Coordinated Universal Time (UTC) timezone, especially if your Cisco ISE nodes are installed in a distributed deployment. This procedure ensures that the timestamps of the reports and logs from the various nodes in your deployment are always synchronized.

Cisco ISE supports public key authentication for NTP servers. NTP Version 4 uses symmetric key cryptography and also provides a new Autokey security model that is based on public key cryptography. Public-key cryptography is considered to be more secure than symmetric key cryptography. This is because the security is based on a private value that is generated by each server and never revealed. With the Autokey security model, all the key distribution and management functions involve only public values, which simplify key distribution and storage considerably.

You can configure the Autokey security model for the NTP server from the Cisco ISE CLI in configuration mode. We recommend that you use the identification friend or foe (IFF) system because this system is most widely used.

Before you begin

You must have either the Super Admin or System Admin administrator role assigned to you.

If you have both primary and secondary Cisco ISE nodes in your deployment, log in to the user interface of each node and configure the system time and Network Time Protocol (NTP) server settings.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **System Time**.

Step 2 In the **NTP Server Configuration** area, enter the unique IP addresses (IPv4 or IPv6 or fully qualified domain name [FQDN] value) for your NTP servers.

Step 3 (Optional) To authenticate the NTP server using private keys, click the **NTP Authentication Keys** tab and specify one or more authentication keys if any of the servers that you specify require authentication through an authentication key. Carry out the following steps:

a) Click **Add**.
b) Enter the necessary values in the **Key ID** and **Key Value** fields. Choose the required Hashed Message Authentication Code (HMAC) value from the **HMAC** drop-down list.The **Key ID** field supports numeric values between 1 to 65535 and the **Key Value** field supports up to 15 alphanumeric characters.
c) Click **OK**.
d) Return to the **NTP Server Configuration** tab.

Step 4 (Optional) To authenticate the NTP server using public key authentication, configure the Autokey security model on Cisco ISE from the CLI. See the **ntp server** and **crypto** commands in the Cisco Identity Services Engine CLI Reference Guide for your Cisco ISE release.

Step 5 Click **Save**.

Note Use three or more NTP servers to ensure accurate time synchronization across your network, even if one of the servers fails or two of the servers are out of sync. See https://insights.sei.cmu.edu/blog/best-practices-for-ntp-services.

Change the System Time Zone

Once set, you cannot edit the time zone from the administration portal. To change the time zone setting, enter the following command in the Cisco ISE CLI:

clock timezone *timezone*

For more information about the **clock timezone** command, see Cisco Identity Services Engine CLI Reference Guide.

Note Cisco ISE uses Portable Operating System Interface (POSIX)-style signs in the time zone names and the output abbreviations. Therefore, zones west of Greenwich have a positive sign and zones east of Greenwich have a negative sign. For example, TZ='Etc/GMT+4' corresponds to 4 hours behind Universal Time (UT).

Caution When you change the time zone on a Cisco ISE appliance after installation, Cisco ISE services restart on that particular node. We recommend that you perform such changes within a maintenance window. Also, it is important to have all the nodes in a single Cisco ISE deployment that is configured to the same time zone. If you have Cisco ISE nodes located in different geographical locations or time zones, you should use a global time zone such as UTC on all the Cisco ISE nodes.

Configure SMTP Server to Support Notifications

Configure an SMTP server for Cisco ISE to be able to send email notifications for the following purposes:

- Alarms.
- For sponsors to send email notification to guests with their login credentials and password reset instructions.
- For guests to automatically receive their login credentials after they successfully register themselves, and for the actions that are required of them before their guest accounts expire.

The recipient of alarm notifications can be any internal admin user with the **Include system alarms in emails** option enabled. The sender's email address for sending alarm notifications is set as ise@<hostname> by default, but it can also be configured if needed. To configure the sender's email address, click on **Administration** > **System** > **Settings** > **Alarm Settings** > **Alarm Notification** and type in the **Enter sender e-mail:** field.

The following table shows which node in a distributed Cisco ISE environment sends emails.

Table 23: Cisco ISE Nodes that Send Emails

Purpose of Email	Node That Sends Email
Guest access expiration	Primary Policy Administration Node (PAN)
Alarms	Active Monitoring and Troubleshooting node (MnT)

Purpose of Email	Node That Sends Email
Sponsor and guest notifications from guest and sponsor portals	Policy Service node (PSN)
Password expirations	Primary PAN

To configure an Simple Mail Transfer Protocol (SMTP) server, click the **Menu** icon (☰) and **Administration** > **System** > **Settings** > **SMTP Server**. Configure the following fields:

- In the **SMTP Server Settings** area:
  - **SMTP Server**: Enter the hostname of the outbound SMTP server.
  - **SMTP Port**: Enter the SMTP port number. This port must be open to connect to the SMTP server.
  - **Connection Timeout**: Enter the maximum time that Cisco ISE waits for a connection to the SMTP server before starting a new connection. The timeout value is configured in seconds.
- In the **Encryption Settings** area, check the **Use TLS/SSL Encryption** check box to communicate with a secure SMTP server. If you use Secure Sockets Layer (SSL), add the root certificate of the SMTP server to Cisco ISE Trusted Certificates.
- In the **Authentication Settings** area, check the **Use Password Authentication** check box to use username and password for authentication instead of SSL.

Enable Secure Unlock Client Mechanism

The Secure Unlock Client mechanism provides root shell access on Cisco ISE CLI for a certain time. When you exit or close the session, the root access is also revoked.

The Secure Unlock Client feature is implemented using the Consent Token tool. Consent Token is a uniform multifactor authentication scheme to securely grant privileged access for Cisco products in a trusted manner, and only after mutual consent from both the customer and Cisco.

To enable root shell on Cisco ISE CLI, perform the following steps:

Step 1 In the Cisco ISE CLI, enter **permit rootaccess**:

```
ise/admin# permit rootaccess
1. Generate Challenge Token Request
2. Enter Challenge Response for Root Access
3. Show History
4. Exit
Enter CLI Option:
```

Step 2 Generate the Consent Token Challenge by choosing option **1**:

```
1. Generate Challenge Token Request
2. Enter Challenge Response for Root Access
3. Show History
4. Exit
```

```
Enter CLI Option:
1
Generating Challenge...................................
Challenge String (Please copy everything between the asterisk lines exclusively):
*****************************************************************************************
GLOX7gAAAQEBAAQAAAABAgAEAAAAAAAMAClmJxgub0hitBAAQiUwv+XeD3pnJ4HLnJy30YQUABAAADhAGAANUU0UHAAZJU0VfQ1QTAANUU0UUACcJIDU2NGQ5NjgwLTEmZmEtOWI0ZS0wZjY1LTdlZDllMGQ1M2UzNQo=
*****************************************************************************************
Starting background timer of 15mins
1. Generate Challenge Token Request
2. Enter Challenge Response for Root Access
3. Show History
4. Exit
Enter CLI Option:
```

Step 3 Send the Consent Token Challenge to the Cisco Technical Assistance Center (TAC):

Cisco TAC generates Consent Token Response using the Consent Token Challenge that you provide.

Step 4 Choose option **2** and then enter the Consent Token Response that is provided by Cisco TAC:

```
Enter CLI Option:
2
Please input the response when you are ready .........................
[illegible]
Response Signature Verified successfully !
Granting shell access
sh-4.2# ls
```

Note The privileged access is enabled if response signature verification is successful.

What to do next

To exit from the shell mode, run the **exit** command:

```
sh-4.2# exit
exit
Root shell exited
```

View the history of root access sessions by choosing option **3**:

```
1. Generate Challenge Token Request
2. Enter Challenge Response for Root Access
3. Show History
4. Exit
Enter CLI Option:
3
************************************
        SN No : 1
************************************
Challenge
3/WcyAAAAQEBAAQAAAABAgAEAAAAAAAMACMt89YhCTWWBAAQwo9lyianfhO4C5u1+v80AQUABAAADhAGAANUU0UHAAZJU0VfQ1QTAANUU0UUACcJIDU2NGQ5NjgwLTEmZmEtOWI0ZS0wZjY1LTdlZDllMGQ1M2UzNQo=
 generated at 2019-06-12 15:40:01.000
************************************
        SN No : 2
************************************
```

Federal Information Processing Standards Mode Support

Cisco ISE uses embedded Federal Information Processing Standards (FIPS) 140-2 validated cryptographic modules Cisco Common Cryptographic Module (Certificate #1643 and Certificate #2100). For details of the FIPS compliance claims, see FIPS Compliance Letter.

When the FIPS mode is enabled, the Cisco ISE administrator interface displays a FIPS mode icon at the left of the node name in the top-right corner of the window.

If Cisco ISE detects the use of a protocol or certificate that is not supported by the FIPS 140-2 standard, it displays a warning with the name of the protocol or certificate that is noncompliant, and the FIPS mode is not enabled. Ensure that you choose only FIPS-compliant protocols and replace non-FIPS compliant certificates before you enable the FIPS mode.

The certificates that are installed in Cisco ISE must be re-issued if the cryptographic algorithms or their parameters that are used in the certificates are not supported by FIPS.

When you enable the FIPS mode, the following functions are affected:

- Lightweight Directory Access Protocol (LDAP) over SSL

Cisco ISE enables FIPS 140-2 compliance via RADIUS shared secret and key management measures. When the FIPS mode is enabled, any function that uses a non-FIPS-compliant algorithm fails.

When you enable the FIPS mode:

- All non-FIPS compliant cipher suites are disabled for EAP-TLS, PEAP, TEAP, EAP-TTLS, and EAP-FAST.
- All non-FIPS compliant cipher suites are disabled in SSH.
- Certificates and private keys must use only FIPS-compliant hash and crytographic algorithms.
- RSA private keys must be 2048 bits or greater.
- ECDSA private keys must be 224 bits or greater.
- ECDSA server certificate works with only TLS 1.2.
- DHE ciphers work with DH parameters of 2048 bits or greater for all ISE TLS clients.
- 3DES ciphers are not allowed for Cisco ISE as a server
- SHA-1 is not allowed for generating certificates.
- SHA-1 is not allowed in client certificates.
- The anonymous PAC provisioning option in EAP-FAST is disabled.
- Local SSH server operates in FIPS mode.
- The following protocols are not supported for RADIUS:
  - EAP-MD5
  - PAP
  - CHAP

- MS-CHAPv1
- MS-CHAPv2
- LEAP

Once the FIPS Mode is enabled, all the nodes in the deployment are rebooted automatically. Cisco ISE performs a rolling restart by first restarting the primary PAN and then restarting each secondary node, one at a time. Hence, it is recommended that you plan for the downtime before changing the configuration.

Tip We recommend that you do not enable FIPS mode before completing the database migration process.

Enable Federal Information Processing Standards Mode in Cisco ISE

To enable the FIPS mode in Cisco ISE:

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **FIPS Mode**.

Step 2 Choose **Enabled** from the **FIPS Mode** drop-down list.

Step 3 Click **Save** and restart your machine.

What to do next

After you enable FIPS mode, enable and configure the following FIPS 140 compliant functions:

- Generate a Self-Signed Certificate, on page 296.
- Create a Certificate-Signing Request and Submit it to a Certificate Authority, on page 315.
- Configure RADIUS authentication settings as mentioned under Network Device Definition Settings, on page 905.

You may want to enable administrator account authorization using a Common Access Card function. Although using Common Access Card functions for authorization is not strictly a FIPS 140 requirement, it is a well-known secure-access measure that is used in several environments to bolster FIPS 140 compliance.

Configure Cisco ISE for Administrator Common Access Card Authentication

Before you begin

- (Optional) Enable the FIPS mode in Cisco ISE. FIPS mode is not required for certificate-based authentication, but the two security measures often go hand-in-hand. If you plan to deploy Cisco ISE in a FIPS 140 compliant deployment and use Common Access Card certificate-based authorization, enable the FIPS mode and specify the appropriate private keys and encryption/decryption settings first.
- Ensure that the domain name server (DNS) in Cisco ISE is set for Active Directory.
- Ensure that Active Directory user and user group memberships have been defined for each administrator certificate.

To ensure that Cisco ISE can authenticate and authorize an administrator based on the Common Access Card-based client certificate that is submitted from the browser, configure the following:

- The external identity source (Active Directory in the following example).
- The Active Directory user groups to which the administrator belongs.
- How to find the user's identity in the certificate.
- Active Directory user groups to Cisco ISE RBAC permissions mapping.
- The Certificate Authority (trust) certificates that sign the client certificates.
- A method to determine if a client certificate has been revoked by the certificate authority.

You can use a Common Access Card to authenticate credentials when logging in to Cisco ISE.

Step 1 When you enable FIPS mode, you are prompted to restart your system. You can defer the restart if you are going to import certificate authority certificates as well.

Step 2 Configure an Active Directory identity source in Cisco ISE and join all Cisco ISE nodes to Active Directory.

Step 3 Configure a certificate authentication profile according to the guidelines.

Be sure to select the attribute in the certificate that contains the administrator username in the **Principal Name X.509 Attribute** field. For Common Access Cards, the Signature Certificate on the card is normally used to look up the user in Active Directory. The Principal Name is found in this certificate in the **Subject Alternative Name** extension, specifically in the **Other Name** area of the extension. So the attribute selection here should be **Subject Alternative Name - Other Name**.

If the Active Directory record for the user contains the user's certificate, and you want to compare the certificate that is received from the browser against the certificate in Active Directory, check the **Binary Certificate Comparison** check box, and select the Active Directory instance name that was specified earlier.

Step 4 Enable Active Directory for password-based administrator authentication. Choose the Active Directory instance name that you connected and joined to Cisco ISE earlier.

Note You must use password-based authentication until you complete other configurations. Then, you can change the authentication type to client certificate based at the end of this procedure.

Step 5 Create an external administrator group and map it to an Active Directory group. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Groups**. Create an external system administrator group.

Step 6 Configure an administrator authorization policy to assign RBAC permissions to the external administrator groups.

Caution We strongly recommend that you create an external Super Admin group, map it to an Active Directory group, and configure an administrator authorization policy with Super Admin permissions (menu access and data access), and create at least one user in that Active Directory Group. This mapping ensures that at least one external administrator has Super Admin permissions once **Client Certificate-Based Authentication** is enabled. Failure to do this may lead to situations where the Cisco ISE administrator is locked out of critical functionality in the administration portal.

Step 7 **Administration** > **System** > **Certificates** > **Certificate Store** > **Trusted Certificates** to import certificate authority certificates into the Cisco ISE trusted certificates store.

Cisco ISE does not accept a client certificate unless the certificate authority certificates in the client certificate's trust chain are placed in the Cisco ISE Certificates store. You must import the appropriate certificate authority certificates in to the Cisco ISE Certificates store.

a) Click **Import** and click **Choose File** in the **Certificate File** area.
b) Check the **Trust for client authentication and Syslog** check box.
c) Click **Submit**.

Cisco ISE prompts you to restart all the nodes in the deployment after you import a certificate. You can defer the restart until you import all the certificates. However, after importing all the certificates, you must restart Cisco ISE before you proceed.

Step 8 Configure the certificate authority certificates for revocation status verification.

a) **Administration** > **System** > **Certificates** > **OSCP Client Profile**.
b) Click **Add**.
c) Enter the name of an OSCP server, an optional description, and the URL of the server in the corresponding fields.
d) **Administration** > **System** > **Certificates** > **Certificate Store**.
e) For each certificate authority certificate that can sign a client certificate, specify how to do the revocation status check for that certificate authority. Choose a certificate authority certificate from the list and click Edit. On the edit page, choose OCSP or certificate revocation list (CRL) validation, or both. If you choose OCSP, choose an OCSP service to use for that certificate authority. If you choose CRL, specify the CRL Distribution URL and other configuration parameters.

Step 9 Enable client certificate-based authentication. Choose **Administration** > **System** > **Admin Access** > **Authentication**.

a) In the **Authentication Method** tab, click the **Client Certificate Based** radio button.
b) Choose the certificate authentication profile that you configured earlier from the **Certificate Authentication Profile** drop-down list.
c) Select the Active Directory instance name from the **Identity Source** drop-down list.
d) Click **Save**.

Here, you switch from password-based authentication to client certificate-based authentication. The certificate authentication profile that you configured earlier determines how the administrator's certificate is authenticated. The administrator is authorized using the external identity source, which in this example is Active Directory.

The Principal Name attribute from the certificate authentication profile is used to look up the administrator in Active Directory.

Supported Common Access Card Standards

Cisco ISE supports U.S. government users who authenticate themselves using Common Access Card authentication devices. A Common Access Card is an identification badge with an electronic chip containing a set of X.509 client certificates that identify a particular employee. Access via the Common Access Card requires a card reader into which you insert the card and enter a PIN. The certificates from the card are then transferred into the Windows certificate store, where they are available to applications such as the local browser running Cisco ISE.

Common Access Card Operation in Cisco ISE

You can configure the administration portal so that Cisco ISE authentications occur only through a client certificate. Credentials-based authentication that requires user IDs or passwords is not permitted. In client certificate-based authentication, you insert a Common Access Card card, enter a PIN, and then enter the Cisco

ISE administration portal URL into the browser address field. The browser forwards the certificate to Cisco ISE, and Cisco ISE authenticates and authorizes your login session, based on the contents of the certificate. If this process is successful, the Cisco ISE Monitoring and Troubleshooting home page is displayed and you are given the appropriate RBAC permissions.

Secure SSH Key Exchange Using Diffie-Hellman Algorithm

Configure Cisco ISE to only allow Diffie-Hellman-Group14-SHA1 Secure Shell (SSH) key exchanges. Enter the following commands from the Cisco ISE CLI Configuration Mode:

service sshd key-exchange-algorithm diffie-hellman-group14-sha1

Here is an example:

```
ise/admin#conf t
```

```
ise/admin (config)#service sshd key-exchange-algorithm diffie-hellman-group14-sha1
```

Configure Cisco ISE to Send Secure Syslog

Before you begin

To configure Cisco ISE to send only TLS-protected secure syslog between the Cisco ISE nodes and to the monitoring nodes, perform the following tasks:

- Ensure that all the Cisco ISE nodes in your deployment are configured with appropriate server certificates. For your setup to be FIPS 140 compliant, the certificate keys must have a key size of 2048 bits or greater.
- Enable the FIPS mode in the administration portal.
- Ensure that the default network access authentication policy does not allow any version of the SSL protocol. Use the TLS protocol in the FIPS mode along with FIPS-approved algorithms.
- Ensure that all the nodes in your deployment are registered with the primary PAN. Also ensure that at least one node in your deployment has the Monitoring persona enabled on it to function as the secure syslog receiver (TLS server).
- Check the supported RFC standards for syslogs. See Cisco Identity Services Engine Network Component Compatibility guide for your Cisco ISE release.

Step 1 Configure a secure syslog remote logging target.

Step 2 Enable logging categories to send auditable events to the secure syslog remote logging target.

Step 3 Disable TCP Syslog and UDP syslog collectors. Only TLS-protected syslog collectors must be enabled.

Note Cisco ISE Release 2.6 and later releases include TLS-protected UDP syslogs if you enable the use of Cisco ISE Messaging Service for delivering UDP syslogs to MnT nodes.

Configure Secure Syslog Remote Logging Target

Cisco ISE system logs are collected and stored by log collectors for various purposes. To configure a secure syslog target, choose a Cisco ISE node with the Monitoring persona enabled on it as your log collector.

Step 1 Log in to the Cisco ISE administration portal.

Step 2 In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration** > **System** > **Logging** > **Remote Logging Targets**.

Step 3 Click **Add**.

Step 4 Enter a name for the secure syslog server.

Step 5 Choose **Secure Syslog** from the **Target Type** drop-down list.

Step 6 Choose **Enabled** from the **Status** drop-down list.

Step 7 Enter the hostname or IP address of the Cisco ISE monitoring node in your deployment, in the **Host / IP Address** field.

Step 8 Enter *6514* as the port number in the **Port** field. The secure syslog receiver listens on TCP port 6514.

Step 9 Choose the syslog facility code from the **Facility Code** drop-down list. The default value is **LOCAL6**.

Step 10 Check the following check boxes to enable the corresponding configurations:

a) **Include Alarms For This Target**
b) **Comply to RFC 3164**
c) **Enable Server Identity Check**

Step 11 Check the **Buffer Messages When Server Down** check box. If this option is checked, Cisco ISE stores the logs if the secure syslog receiver is unreachable, periodically checks the secure syslog receiver, and forwards the logs when the secure syslog receiver comes up.

a) Enter the buffer size in the **Buffer Size (MB)** field.
b) For Cisco ISE to periodically check the secure syslog receiver, enter the reconnect timeout value in the **Reconnect Time (Sec)** field. The timeout value is configured in seconds.

Step 12 Choose the CA certificate that Cisco ISE must present to the secure syslog server from the **Select CA Certificate** drop-down list.

Step 13 Ensure that the **Ignore Server Certificate validation** check box is not checked when configuring a Secure Syslog.

Step 14 Click **Submit**.

Remote Logging Target Settings

The following table describes the fields in the **Remote Logging Targets** window that you can use to create external locations (syslog servers) to store logging messages. To access this window, **Administration** > **System** > **Logging** > **Remote Logging Targets**, and click **Add**.

Table 24: Remote Logging Target Settings

Field Name	Usage Guidelines
Name	Enter a name for the new syslog target.
Target Type	Select the target type from the drop-down list. The default value is **UDP Syslog**.
Description	Enter a brief description of the new target.

Field Name	Usage Guidelines
IP Address	Enter the IP address or hostname of the destination machine that will store the logs. Cisco ISE supports IPv4 and IPv6 formats for logging.
Port	Enter the port number of the destination machine.
Facility Code	Choose the syslog facility code that must be used for logging, from the drop-down list. Valid options are Local0 through Local7.
Maximum Length	Enter the maximum length of the remote log target messages. Valid values are from 200 through 1024 bytes.
Include Alarms For this Target	When you check this check box, alarm messages are sent to the remote server as well.
Comply to RFC 3164	When you check this check box, the delimiters (, ; { } \ \) in the syslog messages sent to the remote servers are not escaped even if a backslash (\) is used.
Buffer Message When Server Down	This check box is displayed when you choose **TCP Syslog** or **Secure Syslog** from the **Target Type** drop-down list. Check this check box to allow Cisco ISE to buffer the syslog messages when a TCP syslog target or secure syslog target is unavailable. Cisco ISE retries sending messages to the target when the connection to the target resumes. After the connection resumes, messages are sent sequentially, starting with the oldest, and proceeding to the newest. Buffered messages are always sent before new messages. If the buffer is full, old messages are discarded.
Buffer Size (MB)	Set the buffer size for each target. By default, it is set to 100 MB. Changing the buffer size clears the buffer, and all the existing buffered messages for the specific target are lost.
Reconnect Timeout (Sec)	Enter the time (in seconds) to configure how long the TCP and secure syslogs are stored for before being discarded when the server is down.
Select CA Certificate	This drop-down list is displayed when you choose **Secure Syslog** from the **Target Type** drop-down list. Choose a client certificate from the drop-down list.
Ignore Server Certificate Validation	This check box is displayed when you choose **Secure Syslog** from the **Target Type** drop-down list. Check this check box for Cisco ISE to ignore server certificate authentication and accept any syslog server. By default, this option is set to Off unless the system is in FIPS mode when this is disabled.

Related Topics

Cisco ISE Logging Mechanism, on page 406
Cisco ISE System Logs, on page 407
Cisco ISE Message Catalogs, on page 409
Collection Filters, on page 410
Event Suppression Bypass Filter, on page 411
Configure Remote Syslog Collection Locations, on page 407
Configure Collection Filters, on page 411

Enable Logging Categories to Send Auditable Events to the Secure Syslog Target

Enable logging categories for Cisco ISE to send auditable events to the secure syslog target.

Step 1 In the Cisco ISE administration portal, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**.

Step 2 Click the radio button next to the **Administrative and Operational Audit** logging category, then click **Edit**.

Step 3 Choose **WARN** from the **Log Severity Level** drop-down list.

Step 4 In the **Targets** area, move the secure syslog remote logging target that you created earlier to the **Selected** area.

Step 5 Click **Save**.

Step 6 Repeat this task to enable the following logging categories. Both these logging categories have **INFO** as the default log severity level and you cannot edit it.

- **AAA Audit**.
- **Posture and Client Provisioning Audit**.

Configure Logging Categories

The following table describes the fields that you can use to configure a logging category. Set a log severity level and choose the logging targets for the logs of a logging category. To access this window, choose **Administration** > **System** > **Logging** > **Logging Categories**.

Click the radio button next to the logging category that you want to view, and click **Edit**. The following table describes the fields that are displayed in the edit window of the logging categories.

Table 25: Logging Category Settings

Field Name	Usage Guidelines
Name	Displays the name of the logging category.
Log Severity Level	For some logging categories, this value is set by default, and you cannot edit it. For some logging categories, you can choose one of the following severity levels from a drop-down list: • **FATAL**: Emergency level. This level means that you cannot use Cisco ISE and you must immediately take the necessary action. • **ERROR**: This level indicates a critical error condition. • **WARN**: This level indicates a normal but significant condition. This is the default level set for many logging categories. • **INFO**: This level indicates an informational message. • **DEBUG**: This level indicates a diagnostic bug message.

Field Name	Usage Guidelines
Local Logging	Check this check box to enable logging events for a category on the local node.
Targets	This area allows you to choose the targets for a logging category by transferring the targets between the **Available** and the **Selected** areas using the left and right arrow icons. The **Available** area contains the existing logging targets, both local (predefined) and external (user-defined). The **Selected** area, which is initially empty, then displays the targets that have been chosen for the category.

Related Topics

Cisco ISE Message Codes, on page 409
Configure Remote Syslog Collection Locations, on page 407
Set Severity Levels for Message Codes, on page 409

Disable TCP Syslog and UDP Syslog Collectors

For Cisco ISE to send only secure syslog between the nodes, you must disable the TCP and UDP syslog collectors, and enable only Secure Syslog collectors.

Note Cisco ISE Release 2.6 and later releases include TLS-protected UDP syslogs if you enable the use of Cisco ISE Messaging Service for delivering UDP syslogs to MnT nodes.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Remote Logging Targets**.

Step 2 Click the radio button next to a TCP or UDP syslog collector.

Step 3 Click **Edit**.

Step 4 Choose **Disabled** from the **Status** drop-down list.

Step 5 Click **Save**.

Step 6 Repeat this process until you disable all the TCP or UDP syslog collectors.

Default Secure Syslog Collector

Cisco ISE provides default secure syslog collectors for the MnT nodes. By default, no logging categories are mapped to these default secure syslog collectors. The default secure syslog collectors are named as follows:

- Primary MnT node: SecureSyslogCollector
- Secondary MnT node: SecureSyslogCollector2

You can view this information on the **Remote Logging Targets** window (**Administration** > **System** > **Logging** > **Remote Logging Targets**). You cannot delete the default syslog collectors and cannot update the following fields for the default syslog collectors:

- **Name**
- **Target Type**
- **IP/Host address**
- **Port**

During a fresh Cisco ISE installation, a certificate that is named **Default Self-signed Server Certificate** is added to the Trusted Certificates store. This certificate is marked for **Trust for Client authentication and Syslog** usage, making it available for secure syslog usage. While configuring your deployment or updating the certificates, you must assign relevant certificates to the secure syslog targets.

During a Cisco ISE upgrade, if there are any existing secure syslog targets pointing to MnT nodes on port 6514, the names and configurations of the target are retained. After the upgrade, you cannot delete these syslog targets and you cannot edit the following fields:

- **Name**
- **Target Type**
- **IP/Host address**
- **Port**

If no such targets exist at the time of upgrade, default secure syslog targets are created similar to the fresh installation scenario, without any certificate mapping. You can assign the relevant certificates to these syslog targets. If you try to map a secure syslog target that is not mapped to any certificate to a logging category, Cisco ISE displays the following message:

```
Please configure the certificate for log_target_name
```

Note You cannot create a new logging target using the hostname or IP address and port of an already existing target. Each logging target must have a unique hostname or IP address and port.

Offline Maintenance

If the maintenance time period is less than an hour, take the Cisco ISE node offline and perform the maintenance task. When you bring the node back online, the PAN node will automatically synchronize all the changes that happened during maintenance time period. If the changes are not synchronized automatically, you can manually synchronize it with the PAN.

If the maintenance time period is more than an hour, deregister the node at the time of maintenance and reregister the node when you add the node back to deployment.

We recommend that you schedule the maintenance at a time period during which the activity is low.

Note

1. Data replication issues may occur if the queue contains more than 1,000,000 messages or if the Cisco ISE node is offline for more than six hours.
2. If you are performing maintenance on the primary MnT node, we recommend that you take an operational backup of the MnT node before performing maintenance activities.

Configure Endpoint Login Credentials

The **Endpoint Login Configuration** window is where you configure login credentials so Cisco ISE can log in to clients. The login credentials that are configured in this window are used by the following Cisco ISE features:

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Endpoint Scripts** > **Settings**.

The following tabs are displayed:

- **Windows Domain User**: Configure the domain credentials that Cisco ISE must use to log in to a client via SSH. Click the **Plus** icon and enter as many Windows logins as you need. For each domain, enter the required values in the **Domain**, **Username**, and **Password** fields. If you configure domain credentials, the local user credentials that are configured in the **Windows Local User** tab are ignored.
- **Windows Local User**: Configure the local account that Cisco ISE uses to access the client via SSH. The local account must be able to run Powershell and Powershell remote.
- **MAC Local User**: Configure the local account that Cisco ISE uses to access the client via SSH. The local account must be able to run Powershell and Powershell remote. In the **Username** field, enter the Account Name of the local account. To view a Mac OS Account Name, run the following command in the Terminal:

  ```
  whoami
  ```

Changing the Host Name in Cisco ISE

In Cisco ISE, you can change the host name only through the CLI. For information on this, see the *Cisco Identity Services Engine CLI Reference Guide* for your version.

Considerations to keep in mind before changing the host name:

- All Cisco ISE services will undergo an automatic restart at the standalone node level if the host name is changed.
- If CA-signed certificates were used on this node, you must import them again with the correct host name.
- If this node will be joining a new Active Directory domain, you must leave your current Active Directory domain before changing the host name. If this node is already joined to an existing Active Directory domain, then it is strongly recommended that you rejoin all currently joined join-points to avoid possible mismatch between the current and previous host names and joined machine account name.
- If Internal-CA signed certificates are being used, you must regenerate the ISE root CA certificate.

- Changing the host name will cause any certificate using the old host name to become invalid. Therefore, a new self-signed certificate using the new host name will be generated now for use with HTTPs or EAP.

Note All the above considerations are applicable for any change in the domain name as well.

Certificate Management in Cisco ISE

A certificate is an electronic document that identifies an individual, a server, a company, or another entity, and associates that entity with a public key. A self-signed certificate is signed by its creator. Certificates can be self-signed or digitally signed by an external CA. A CA-signed digital certificate is considered an industry standard and more secure than a self-signed certificate.

Certificates are used in a network to provide secure access. Certificates identify a Cisco ISE node to an endpoint and secure the communication between that endpoint and the Cisco ISE node.

Cisco ISE uses certificates for:

- Communication between Cisco ISE nodes.
- Communication between Cisco ISE and external servers such as the syslog and feed servers.
- Communication between Cisco ISE and end user portals such as guest, sponsor and BYOD portals.

Manage certificates for all the nodes in your deployment through the Cisco ISE administration portal.

Configure Certificates in Cisco ISE to Enable Secure Access

Cisco ISE relies on public key infrastructure (PKI) to provide secure communication with both endpoints and administrators and between Cisco ISE nodes in a multinode deployment. PKI relies on X.509 digital certificates to transfer public keys for encryption and decryption of messages, and to verify the authenticity of other certificates representing users and devices. Through the Cisco ISE administration portal, you can manage two categories of X.509 certificates:

- System Certificates: These are server certificates that identify a Cisco ISE node to client applications. Every Cisco ISE node has its own system certificates that are stored on the node along with the corresponding private keys.

  Note Cisco ISE cannot import more than one certificate with the same private key. If the certificate is renewed and imported without changing the private key, then the existing certificate is replaced with the imported certificate.

- Trusted Certificates: These are CA certificates that are used to establish trust for the public keys that are received from users and devices. The Trusted Certificates store also contains certificates that are distributed by the Simple Certificate Enrollment Protocol (SCEP), which enables the registration of mobile devices into the enterprise network. Trusted certificates are managed on the primary PAN, and are automatically replicated to all the other nodes in a Cisco ISE deployment.

In a distributed deployment, you must import the certificate only into the Certificate Trust List (CTL) of the PAN. The certificate gets replicated to the secondary nodes.

To ensure certificate authentication in Cisco ISE is not impacted by minor differences in certificate-driven verification functions, use lowercase hostnames for all Cisco ISE nodes that are deployed in a network.

Certificate Usage

When you import a certificate into Cisco ISE, specify the purpose for which the certificate is to be used. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **System Certificates**, and click **Import**.

Choose one or more of the following uses:

- **Admin**: For internode communication and authenticating the administration portal.
- **EAP Authentication**: For TLS-based EAP authentication.
- **RADIUS DTLS**: For RADIUS DTLS server authentication.
- **Portal**: For communicating with all Cisco ISE end-user portals.
- **SAML**: For verifying that the SAML responses are being received from the correct identity provider.
- **pxGrid**: For communicating with the pxGrid controller.

Associate different certificates from each node for communicating with the administration portal (Admin usage), the pxGrid controller (pxGrid usage), and for TLS-based EAP authentication (EAP Authentication usage). However, you can associate only one certificate from each node for each of these purposes.

You must always use a new private key for each certificate that you import into Cisco ISE. When you reuse private keys across certificates, application initialization errors may occur due to a Red Hat NSS database limitation.

When a new certificate is imported into the Red Hat NSS database, any existing certificate that has the same private key is overridden. Cisco ISE application initialization is impacted if an admin certificate's private key is overridden.

With multiple PSNs in a deployment that can service a web portal request, Cisco ISE needs a unique identifier to identify the certificate that must be used for portal communication. When you add or import certificates that are designated for portal use, define a certificate group tag and associate it with the corresponding certificate on each node in your deployment. Associate this certificate group tag to the corresponding end-user portals (guest, sponsor, and personal devices portals). This certificate group tag is the unique identifier that helps Cisco ISE identify the certificate that must be used when communicating with each of these portals. You can only designate one certificate from each node for each of the portals.

Note An EAP-TLS client certificate should have KeyUsage=Key Agreement and ExtendedKeyUsage=Client Authentication for the following ciphers:

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384

An EAP-TLS client certificate should have KeyUsage=Key Encipherment and ExtendedKeyUsage=Client Authentication for the following ciphers:

- AES256-SHA256
- AES128-SHA256
- AES256-SHA
- AES128-SHA
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA
- ECDHE-RSA-AES128-SHA
- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- RC4-SHA
- RC4-MD5

To bypass this requirement, choose **Administration** > **System** > **Settings** > **Security Settings** and check the **Accept certificates without validating purpose** checkbox.

Certificate Matching in Cisco ISE

When you set up Cisco ISE nodes in a deployment, the nodes communicate with each other. The system checks the FQDN of each Cisco ISE node to ensure that they match (for example ise1.cisco.com and ise2.cisco.com or if you use wildcard certificates then *.cisco.com). In addition, when an external machine presents a certificate to a Cisco ISE server, the external certificate that is presented for authentication is checked (or matched) against the certificate in the Cisco ISE server. If the two certificates match, the authentication succeeds.

For Cisco , matching is performed between the nodes (if there are two), and between Cisco and pxGrid.

Cisco ISE checks for a matching subject name as follows:

1. Cisco ISE looks at the subject alternative name extension of the certificate. If the subject alternative name contains one or more DNS names, then one of the DNS names must match the FQDN of the Cisco ISE node. If a wildcard certificate is used, then the wildcard domain name must match the domain in the Cisco ISE node’s FQDN.
2. If there are no DNS names in the subject alternative name, or if the subject alternative name is missing entirely, then the common name in the **Subject** field of the certificate or the wildcard domain in the **Subject** field of the certificate must match the FQDN of the node.
3. If no match is found, the certificate is rejected.

Note X.509 certificates that are imported into Cisco ISE must be in privacy-enhanced mail (PEM) or distinguished encoding rule format. Files containing a certificate chain (a system certificate along with the sequence of trust certificates that sign it) can be imported, subject to certain restrictions.

Validity of X.509 Certificates

X.509 certificates are valid until a specific date. When a system certificate expires, the Cisco ISE functionality that depends on the certificate is impacted. Cisco ISE notifies you about the pending expiration of a system certificate when the expiration date is within 90 days. This notification appears in several ways:

- Colored expiration status icons appear in the **System Certificates** window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificate Management** > **System Certificates**.
- Expiration messages appear in the Cisco ISE System Diagnostic report. To view this window, click the **Menu** icon (☰) and choose**Operations** > **Reports** > **Reports** > **Diagnostics** > **System Diagnostic**.
- Expiration alarms are generated 90 days, 60 days, and 30 days before expiration. Expiration alarms are generated every day in the final 30 days before expiration.

If the expiring certificate is a self-signed certificate, you can extend its expiration date by editing the certificate. For a certificate authority-signed certificate, you must allow sufficient time to acquire the replacement certificate from your certificate authority.

Enable Public Key Infrastructure in Cisco ISE

PKI is a cryptographic technique that enables secure communication and verifies the identity of a user using digital signatures.

Step 1 Configure system certificates on each node in your deployment for the following:

- TLS-enabled authentication protocols such as EAP-TLS.
- Administration portal authentication.
- Allow browser and REST clients to access Cisco ISE web portals.
- Allow access to pxGrid controller.

By default, a Cisco ISE node is preinstalled with a self-signed certificate that is used for EAP authentication, and for access to administration portal, end user portals, and pxGrid controller. In a typical enterprise environment, this self-signed certificate is replaced with server certificates that are signed by a trusted CA.

Step 2 Populate the Trusted Certificates store with the CA-signed certificates that are used to establish trust with the user, and device certificates that will be presented to Cisco ISE.

To validate the authenticity of a user or device certificate with a certificate chain that consists of a root CA certificate and one or more intermediate CA certificates:

- Enable the relevant trust option for the root CA.

  In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** >**Certificates** > **Certificate Management** > **Trusted Certificates**. In this window, check the check box for the root CA certificate and click **Edit**. In the **Usage** area, check the necessary check boxes in the **Trusted For** area.

For inter-node communications, you must populate the Trusted Certificates store with the trust certificates that validate the Admin system certificate of each node in the Cisco ISE deployment. To use the default self-signed certificate for internode communication, export this certificate from the System Certificates window of each Cisco ISE node and import it into the Trusted Certificates store. If you replace the self-signed certificates with CA-signed certificates, it is only necessary to populate the Trusted Certificates store with the appropriate root CA and intermediate CA certificates. You cannot register a node in a Cisco ISE deployment until you complete this step.

If you use self-signed certificates to secure communication between a client and a PSN in a deployment, when BYOD users move from one location to another, EAP-TLS user authentication fails. For such authentication requests that have to be serviced between a few PSNs, you must secure communication between the client and the PSN with an externally-signed CA certificate or use wildcard certificates that are signed by an external CA.

If you intend to get a publicly signed certificate or if the Cisco ISE deployment is to be operated in FIPS mode, you must ensure that all system and trusted certificates are FIPS-compliant. This means that each certificate must have a minimum key size of 2048 bytes, and use SHA-1 or SHA-256 encryption.

Note After you obtain a backup from a standalone Cisco ISE node or the PAN, if you change the certificate configuration on one or more nodes in your deployment, you must obtain another backup to restore data. Otherwise, if you try to restore data using the older backup, communication between the nodes might fail.

Wildcard Certificates

A wildcard certificate uses a wildcard notation (an asterisk and period before the domain name) and the certificate can be shared across multiple hosts in an organization. For example, the **CN** value for the certificate subject would be a generic hostname such as aaa.ise.local and the SAN field would include the same generic hostname and a wildcard notation such as DNS.1=aaa.ise.local and DNS.2=*.ise.local.

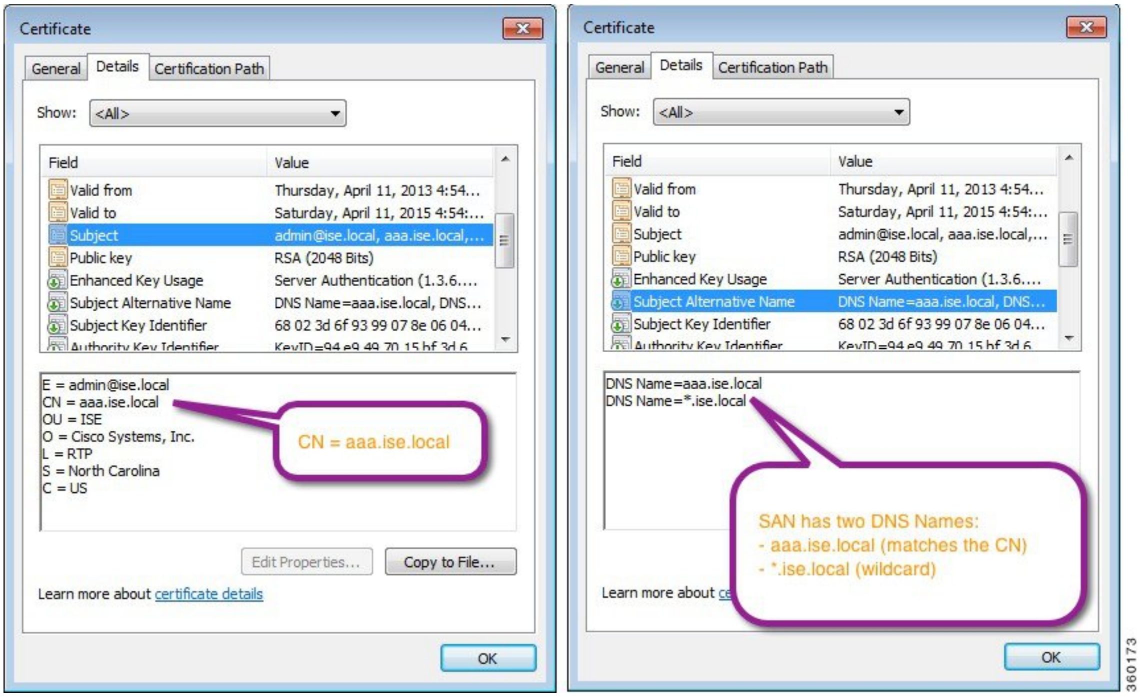
If you configure a wildcard certificate to use *.ise.local, you can use the same certificate to secure any other host whose DNS name ends with ".ise.local," such as :

- aaa.ise.local
- psn.ise.local
- mydevices.ise.local
- sponsor.ise.local

Wildcard certificates secure communication in the same way as a regular certificate, and requests are processed using the same validation methods.

The following figure is an example of a wildcard certificate that is used to secure a website.

Figure 7: Example of Wildcard Certificate



Field	Value
Valid from	Thursday, April 11, 2013 4:54...
Valid to	Saturday, April 11, 2015 4:54:...
Subject	admin@ise.local, aaa.ise.local,...
Public key	RSA (2048 Bits)
Enhanced Key Usage	Server Authentication (1.3.6....
Subject Alternative Name	DNS Name=aaa.ise.local, DNS...
Subject Key Identifier	68 02 3d 6f 93 99 07 8e 06 04...
Authority Key Identifier	KeyID=94 e9 49 70 15 bf 3d 6

E = admin@ise.local
CN = aaa.ise.local
OU = ISE
O = Cisco Systems, Inc.
L = RTP
S = North Carolina
C = US

CN = aaa.ise.local

Field	Value
Valid from	Thursday, April 11, 2013 4:54...
Valid to	Saturday, April 11, 2015 4:54:...
Subject	admin@ise.local, aaa.ise.local,...
Public key	RSA (2048 Bits)
Enhanced Key Usage	Server Authentication (1.3.6....
Subject Alternative Name	DNS Name=aaa.ise.local, DNS...
Subject Key Identifier	68 02 3d 6f 93 99 07 8e 06 04...
Authority Key Identifier	KeyID=94 e9 49 70 15 bf 3d 6

DNS Name=aaa.ise.local
DNS Name=*.ise.local

SAN has two DNS Names:
- aaa.ise.local (matches the CN)
- *.ise.local (wildcard)

Wildcard Certificate Support in Cisco ISE

Cisco ISE supports wildcard certificates. In earlier releases, Cisco ISE verified any certificate enabled for HTTPS to ensure the common name field matches the FQDN of the host exactly. If the fields did not match, the certificate could not be used for HTTPS communication.

In earlier releases, Cisco ISE used that common name value to replace the variable in the url-redirect A-V pair string. For all centralized web authentication, onboarding, posture redirection, and so on, the common name value was used.

Cisco ISE uses the hostname of the ISE node as the common name.

Wildcard Certificates for HTTPS and Extensible Authentication Protocol Communication

You can use wildcard server certificates in Cisco ISE for administration (web-based services) and EAP protocols that use SSL or TLS tunneling. When you use wildcard certificates, you do not need to generate a unique certificate for each Cisco ISE node. Also, you no longer have to populate the SAN field with multiple FQDN values to prevent certificate warnings. Use an asterisk (*) in the SAN field to share a single certificate across multiple nodes in a deployment and prevent certificate name mismatch warnings. However, the use of wildcard certificates is considered less secure than assigning a unique server certificate to each Cisco ISE node.

When assigning public wildcard certificates to the guest portal and importing sub-CA with root-CA certificates, the certificate chain is not sent until Cisco ISE services are restarted.

Note If you use wildcard certificates, we recommend that you partition your domain space for greater security. For example, instead of *.example.com, you can partition it as *.amer.example.com. If you do not partition your domain, it could lead to serious security issues.

Wildcard certificates use an asterisk (*) and a period before the domain name. For example, the common name value for a certificate's Subject Name would be a generic hostname such as aaa.ise.local and the SAN field would have the wildcard character such as *.ise.local. Cisco ISE supports wildcard certifications in which the wildcard character (*) is the left-most character in the presented identifier. For example, *.example.com or *.ind.example.com. Cisco ISE does not support certificates in which the presented identifier contains other characters along with the wildcard character. For example, abc*.example.com, or a*b.example.com, or *abc.example.com.

Note When generating a CSR on a node using the wildcard character (*) in the CN or SAN, the certificate will be considered as a wildcard. Cisco ISE adds it to the PAN and replicates it to all other nodes.

Fully Qualified Domain Name in URL Redirection

Authorization profile redirects are carried out for central web authentication, device registration web authentication, native supplicant provisioning, mobile device management, client provisioning, and posture services. When Cisco ISE builds an authorization profile redirect, the resulting cisco-av-pair includes a string similar to the following:

url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa

When processing this request, Cisco ISE substitutes actual values for some keywords in this string. For example, SessionIdValue is replaced with the actual session ID of the request. For an eth0 interface, Cisco ISE replaces the IP in the URL with the FQDN of the Cisco ISE node. For non-eth0 interfaces, Cisco ISE uses the IP address in the URL. You can assign a host alias (name) for interfaces eth1 through eth3, which Cisco ISE can then substitute in place of IP address during URL redirection.

To do this, use the **ip host** command in the configuration mode from the Cisco ISE CLI ISE /admin(config)# prompt:

ip host *IP_address host-alias FQDN-string*

Where *IP_address* is the IP address of the network interface (eth1 or eth2 or eth3) and *host-alias* is the name that you assign to the network interface. *FQDN-string* is the fully qualified domain name of the network interface. Using this command, you can assign a *host-alias* or an *FQDN-string* or both to a network interface.

Here is an example using the **ip host** command: ip host a.b.c.d sales sales.amerxyz.com

After you assign a host alias to the non-eth0 interface, restart the application services on Cisco ISE using the **application start ise** command.

Use the **no** form of this command to remove the association of the host alias with the network interface.

no ip host *IP_address host-alias FQDN-string*

Use the **show running-config** command to view the host alias definitions.

If you provide the *FQDN-string*, Cisco ISE replaces the IP address in the URL with the FQDN. If you provide only the host alias, Cisco ISE combines the host alias with the configured IP domain name to form a complete FQDN and replaces the IP address in the URL with the FQDN. If you do not map a network interface to a host alias, then Cisco ISE uses the IP address of the network interface in the URL.

When you use non-eth0 interfaces for client provisioning or native supplicant or guest flows, ensure that the IP address or host alias for non-eth0 interfaces are configured appropriately in the PSN certificate's SAN fields.

Advantages of Using Wildcard Certificates

- Cost savings: Certificates that are signed by third-party CAs are expensive, especially as the number of servers increases. Wildcard certificates can be used on multiple nodes in the Cisco ISE deployment.
- Operational efficiency: Wildcard certificates allow all PSNs to share the same certificate for EAP and web services. In addition to significant cost savings, certificate administration is also simplified by creating the certificate once and applying it on all the PSNs.
- Reduced authentication errors: Wildcard certificates address issues seen with Apple iOS devices when the client stores trusted certificates within the profile and does not follow the iOS keychain where the signing root is trusted. When an iOS client first communicates with a PSN, it does not explicitly trust the PSN certificate, although a trusted CA has signed the certificate. Using a wildcard certificate, the certificate is the same across all PSNs, so the user only has to accept the certificate once and successive authentications to different PSNs proceed without errors or prompts.
- Simplified supplicant configuration: For example, a Microsoft Windows supplicant with PEAP-MSCHAPv2 and a trusted server certificate requires that you specify each of the server certificate to trust, or the user may be prompted to trust each PSN certificate when the client connects using a different PSN. With wildcard certificates, a single server certificate can be trusted rather than individual certificates from each PSN.
- Wildcard certificates result in an improved user experience with less prompting and more seamless connectivity.

Disadvantages of Using Wildcard Certificates

The following are some of the security considerations that are related to the use of wildcard certificates:

- Loss of auditability and nonrepudiation.
- Increased exposure of the private key.
- Not common or understood by administrators.

Wildcard certificates are considered less secure than using a unique server certificate in each Cisco ISE node. But cost and other operational factors outweigh the security risk.

Security devices such as Cisco Adaptive Security Appliance also support wildcard certificates.

You must be careful when deploying wildcard certificates. For example, if you create a certificate with *.company.local and an attacker is able to recover the private key, that attacker can spoof any server in the company.local domain. Therefore, it is considered a best practice to partition the domain space to avoid this type of compromise.

To address this possible issue and to limit the scope of use, wildcard certificates may also be used to secure a specific subdomain of your organization. Add an asterisk (*) in the subdomain area of the common name where you want to specify the wildcard.

For example, if you configure a wildcard certificate for *.ise.company.local, that certificate may be used to secure any host whose DNS name ends in ".ise.company.local", such as:

- psn.ise.company.local
- mydevices.ise.company.local
- sponsor.ise.company.local

Wildcard Certificate Compatibility

Wildcard certificates are usually created with the wildcard listed as the common name of the certificate subject. Cisco ISE supports this type of construction. However, not all endpoint supplicants support the wildcard character in the certificate subject.

All the Microsoft native supplicants that were tested (including Windows Mobile which is now discontinued) do not support wildcard character in the certificate subject.

You can use another supplicant, such as Network Access Manager that might allow the use of wildcard characters in the Subject field.

You can also use special wildcard certificates such as DigiCert's Wildcard Plus that is designed to work with incompatible devices by including specific subdomains in the Subject Alternative Name of the certificate.

Although the Microsoft supplicant limitation appears to be a deterrent to using wildcard certificates, there are alternative ways to create the wildcard certificate that allow it to work with all the devices tested for secure access, including the Microsoft native supplicants.

To do this, instead of using the wildcard character in the Subject, you must use the wildcard character in the Subject Alternative Name field instead. The Subject Alternative Name field maintains an extension that is designed for checking the domain name (DNS name). See RFC 6125 and RFC 2128 for more information.

Certificate Hierarchy

In the administration portal, view the certificate hierarchy or the certificate trust chain of all endpoint, system, and trusted certificates. The certificate hierarchy includes the certificate, all the intermediate CA certificates, and the root certificate. For example, when you choose to view a system certificate from the the administration portal, the details of the corresponding system certificate are displayed. The certificate hierarchy is displayed at the top of the certificate. Click a certificate in the hierarchy to view its details. The self-signed certificate does not have any hierarchy or trust chain.

In the certificate listing windows, you will see one of the following icons in the **Status** column:

- Green icon: Indicates a valid certificate (valid trust chain).
- Red icon: Indicates an error (for example, trust certificate missing or expired).
- Yellow icon: Warns that a certificate is about to expire and prompts renewal.

System Certificates

Cisco ISE system certificates are server certificates that identify a Cisco ISE node to other nodes in the deployment and to client applications. System certificates are:

- Used for inter-node communication in a Cisco ISE deployment. Check the **Admin** check box in the **Usage** area of these certificates.
- Used by browser and REST clients who connect to Cisco ISE web portals. Check the **Portal** check box in the **Usage** area of these certificates.
- Used to form the outer TLS tunnel with PEAP and EAP-FAST. Check the **EAP Authentication** check box in the **Usage** area for mutual authentication with EAP-TLS, PEAP, and EAP-FAST.
- Used for RADIUS DTLS server authentication.
- Used to communicate with SAML identity providers. Check the **SAML** check box in the **Usage** area of this certificate. If you choose the SAML option, you cannot use this certificate for any other service.

  A SAML certificate is used by multiple Cisco ISE services such as Posture services and licensing communication between Cisco ISE and the Cisco Smart Software Manager. If you delete the SAML certificate from your Cisco ISE, the associated services are disrupted.
- Used to communicate with the pxGrid controller. Check the **pxGrid** check box in the **Usage** area of these certificates.

Install valid system certificates on each node in your Cisco ISE deployment. By default, two self-signed certificates and one signed by the internal Cisco ISE CA are created on a Cisco ISE node during installation time:

- A self-signed server certificate designated for EAP, Admin, Portal, and RADIUS DTLS (it has a key size of 2048 and is valid for one year).
- A self-signed SAML server certificate that can be used to secure communication with a SAML identity provider (it has a key size of 2048 and is valid for one year).
- An internal Cisco ISE CA-signed server certificate that can be used to secure communication with pxGrid clients (it has a key size of 4096 and is valid for one year).

When you set up a deployment and register a secondary node, the certificate that is designated for pxGrid controller is automatically replaced with a certificate that is signed by the primary node's CA. Thus, all pxGrid certificates become part of the same PKI trust hierarchy.

Note

- When you export a wildcard system certificate to be imported into the other nodes (for inter-node communication), ensure that you export the certificate and the private key, and specify an encryption password. During import, you will need the certificate, private key, and encryption password.
- Cisco ISE supports the use of RSASSA-PSS algorithm only for trusted certificates and endpoint certificates for EAP-TLS authentication. When you view the certificate, the signature algorithm is listed as 1.2.840.113549.1.1.10 instead of the algorithm name.

  Cisco ISE does not support system certificates that use RSASSA-PSS as the signature algorithm. This is applicable for the server certificate, root certificate, and intermediate CA certificate.
- When Cisco ISE is deployed on AWS using Cloud Formation Template (CFT), you might see DefaultISE.ise.com based certificates in the **System Certificates** window. This will not impact Cisco ISE functionality. After the CA certificates are regenerated, these additional certificates will not be active and can be ignored.

For supported key and cipher information for your release, see the appropriate version of the Cisco Identity Services Engine Network Component Compatibility guide.

We recommend that you replace the self-signed certificate with a CA-signed certificate for greater security. To obtain a CA-signed certificate, you must:

1. Create a Certificate-Signing Request and Submit it to a Certificate Authority, on page 315
2. Import a Root Certificate into the Trusted Certificate Store, on page 309
3. Bind a CA-Signed Certificate to a Certificate Signing Request, on page 316

ISE Community Resource

How To: Implement ISE Server-Side Certificates

Certificate Renewal on Cisco Identity Services Engine Configuration Guide

View System Certificates

The **System Certificate** window lists all the system certificates added to Cisco ISE.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration** > **System** > **Certificates** > **System Certificates**.

Step 2 The following columns are displayed in the **System Certificates** window:

- **Friendly Name**: Name of the certificate.
- **Usage**: The services for which this certificate is used.

- **Portal group tag**: Applicable only for certificates that are designated for portal use. This field specifies which certificate has to be used for portals.
- **Issued To**: Common Name of the certificate subject.
- **Issued By**: Common Name of the certificate issuer
- **Valid From**: Date on which the certificate was created, also known as the "Not Before" certificate attribute.
- **Valid To (Expiration)**: Expiration date of the certificate, also known as the "Not After" certificate attribute. The following icons are displayed next to the expiration date:
  - Green icon: Expiring in more than 90 days.
  - Blue icon: Expiring in 90 days or less.
  - Yellow icon: Expiring in 60 days or less.
  - Orange icon: Expiring in 30 days or less.
  - Red icon: Expired.

Import a System Certificate

You can import a system certificate for any Cisco ISE node from the administration portal.

Note Changing the certificate of the admin role certificate on a primary PAN node restarts services on all other nodes. The system restarts one node at a time, after the primary PAN restart is complete.

Before you begin

- Ensure that you have the system certificate and the private key file on the system that is running on the client browser.
- If the system certificate that you import is signed by an external CA, import the relevant root CA and intermediate CA certificates into the Trusted Certificates store (**Administration** > **System** > **Certificates** > **Trusted Certificates**).
- If the system certificate that you import contains basic constraints extension with the CA flag set to true, ensure that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set.
- To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration** > **System** > **Certificates** > **System Certificates**.

Step 2 Click **Import**.
The **Import Server Certificate** window is displayed.

Step 3 Enter the values for the certificate that you are going to import.

Step 4 Click **Submit**.

System Certificate Import Settings

The following table describes the fields in the **Import System Certificate** window that you can use to import a server certificate. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **System Certificates**. Click **Import**.

Table 26: System Certificate Import Settings

Field Name	Description
Select Node	(Required) Choose the Cisco ISE node on which you want to import the system certificate from the drop-down list.
Certificate File	(Required) Click **Choose File** and choose the certificate file from your local system.
Private Key File	(Required) Click **Choose File** and choose the private key file from your local system.
Password	(Required) Enter the password to decrypt the private key file.
Friendly Name	Enter a friendly name for the certificate. If you do not specify a name, Cisco ISE automatically creates a name in the following format: <common name> # <issuer> # <nnnnn> where <nnnnn> is a unique five-digit number.
Allow Wildcard Certificates	Check this check box if you want to import a wildcard certificate. A wildcard certificate uses a wildcard notation (an asterisk and period before the domain name). Wildcard certificates are shared across multiple hosts in an organization. If you check this check box, Cisco ISE imports this certificate to all the other nodes in the deployment.
Validate Certificate Extensions	Check this check box if you want Cisco ISE to validate the certificate extensions. If you check this check box and the certificate that you import contains a basic constraints extension with the CA flag set to true, ensure that the key usage extension is present. The keyEncipherment bit or the keyAgreement bit, or both, must also be set.

Field Name	Description
Usage	Choose the service for which this system certificate must be used: • **Admin**: Server certificate used to secure communication with the administration portal and between the Cisco ISE nodes in a deployment. **Note** Changing the certificate of the admin role certificate on the primary PAN restarts services on all other Cisco ISE nodes. • **EAP Authentication**: Server certificate used for authentications that use the EAP protocol for SSL or TLS tunneling. • **RADIUS DTLS**: Server certificate used for RADIUS DTLS authentication. • **pxGrid**: Client and server certificate to secure communication between the pxGrid client and the server. • **ISE Messaging Service**: Used by **Syslog Over Cisco ISE Messaging** feature, which enables MnT WAN survivability for built-in UDP syslog collection targets (LogCollector and LogCollector2). • **SAML**: Server certificate used to secure communication with the SAML identity provider. A certificate that is designated for SAML use cannot be used for any other service such as Admin, EAP authentication, and so on. • **Portal**: Server certificate used to secure communication with all Cisco ISE web portals

Note If the certificate is generated by other third-party tools and not Cisco ISE, you cannot import the certificate or its private key into Cisco ISE.

Related Topics

System Certificates, on page 292
View System Certificates, on page 293
Import a System Certificate, on page 294

Generate a Self-Signed Certificate

Add a new local certificate by generating a self-signed certificate. Cisco recommends that you only employ self-signed certificates for your internal testing and evaluation needs. If you plan to deploy Cisco ISE in a production environment, use CA-signed certificates whenever possible to ensure more uniform acceptance around a production network.

Note If you use a self-signed certificate and you want to change the hostname of your Cisco ISE node, log in to the administration portal of the Cisco ISE node, delete the self-signed certificate that has the old hostname, and generate a new self-signed certificate. Otherwise, Cisco ISE continues to use the self-signed certificate with the old hostname.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Self-Signed Certificate Settings

The following table describes the fields in the **Generate Self Signed Certificate** window. This window allows you to create system certificates for inter-node communication, EAP-TLS authentication, Cisco ISE web portals, and to communicate with the pxGrid controller. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **System Certificates**. Click **Generate Self Signed Certificate**.

Table 27: Self-Signed Certificate Settings

Field Name	Usage Guidelines
Select Node	(Required) Choose the node for which you want to generate the system certificate from the drop-down list.
Common Name (CN)	(Required if you do not specify a SAN) By default, the common name is the FQDN of the Cisco ISE node for which you are generating the self-signed certificate.
Organizational Unit (OU)	Organizational Unit name. For example, Engineering.
Organization (O)	Organization name. For example, Cisco.
City (L)	(Do not abbreviate) City name. For example, San Jose.
State (ST)	(Do not abbreviate) State name. For example, California.
Country (C)	Country name. Enter the two-letter ISO country code. For example, US.
Subject Alternative Name (SAN)	An IP address, DNS name, or Uniform Resource Identifier (URI) that is associated with the certificate.
Key Type	The algorithm to be used for creating the public key, either RSA or ECDSA.

Field Name	Usage Guidelines
Key Length	The bit size for the public key. Choose one of the following options from the drop-down list for RSA: • 512 • 1024 • 2048 • 4096 Choose one of the following options from the drop-down list for ECDSA: • 256 • 384 **Note** RSA and ECDSA public keys might have different key lengths for the same security level. Choose 2048 if you plan to get a public CA-signed certificate or deploy Cisco ISE as a FIPS-compliant policy management system.
Digest to Sign With	Choose one of the following hashing algorithms from the drop-down list: • SHA-1 • SHA-256
Certificate Policies	Enter the certificate policy OID or list of OIDs that the certificate should conform to. Use a comma or space to separate the OIDs.
Expiration TTL	Specify the number of days after which the certificate expires. Choose the value from the drop-down lists.
Friendly Name	Enter a friendly name for the certificate. If you do not specify a name, Cisco ISE automatically creates a name in the format <common name> # <issuer> # <nnnnn> where <nnnnn> is a unique five-digit number.
Allow Wildcard Certificates	Check this check box if you want to generate a self-signed wildcard certificate. A wildcard certificate uses a wildcard notation (an asterisk and period before the domain name) and allows the certificate to be shared across multiple hosts in an organization.

Field Name	Usage Guidelines
Usage	Choose the service for which this system certificate must be used: • **Admin**: Server certificate used to secure communication with the administration portal and between the Cisco ISE nodes in a deployment. • **EAP Authentication**: Server certificate used for authentications that use the EAP protocol for SSL or TLS tunneling. • **RADIUS DTLS**: Server certificate used for RADIUS DTLS authentication. • **pxGrid**: Client and server certificate to secure communication between the pxGrid client and the server. • **SAML**: Server certificate used to secure communication with the SAML identity provider. A certificate that is designated for SAML use cannot be used for any other service such as Admin, EAP authentication, and so on. • **Portal**: Server certificate used to secure communication with all Cisco ISE web portals.

Related Topics

System Certificates, on page 292

View System Certificates, on page 293

Generate a Self-Signed Certificate, on page 296

Edit a System Certificate

Use this window to edit a system certificate and to renew a self-signed certificate. When you edit a wildcard certificate, the changes are replicated to all the nodes in the deployment. If you delete a wildcard certificate, that wildcard certificate is removed from all the nodes in the deployment.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration** > **System** > **Certificates** > **System Certificates**.

Step 2 Check the check box next to the certificate that you want to edit, and click **Edit**.

Step 3 To renew a self-signed certificate, check the **Renewal Period** check box and enter the expiration Time to Live (TTL) in days, weeks, months, or years. Choose the required value from the drop-down lists.

Step 4 Click **Save**.

If the **Admin** check box is checked, then the application server on the Cisco ISE node restarts. In addition, if the Cisco ISE node is the PAN in a deployment, then the application server on all the other nodes in the deployment also restart. The system restarts one node at a time, after the primary PAN restart has completed.

For information on troubleshooting, see Launching a BYOD Portal using Google Chrome 65, on page 300Configuring Wireless BYOD setup using Mozilla Firefox 64, on page 300.

Launching a BYOD Portal using Google Chrome 65

When using Chrome 65 and above to launch Cisco ISE, it can cause BYOD portal or Guest portal to fail to launch in the browser although the URL is redirected successfully. This is because of a new security feature introduced by Google that requires all certificates to have a **Subject Alternative Name** field. For Cisco ISE Release 2.4 and later, you must fill the **Subject Alternative Name** field.

To launch BYOD portal with Chrome 65 and above, follow the steps below:

Step 1 Generate a new self-signed certificate from the Cisco ISE GUI by filling the Subject Alternative Name field. Both DNS and IP Address must be filled.

Step 2 Cisco ISE services restart.

Step 3 Redirect the portal in Chrome browser.

Step 4 From browser, **View Certificate** > **Details** > **Copy the certificate by selecting base-64 encoded**

Step 5 Install the certificate in Trusted path.

Step 6 Close the Chrome browser and try to redirect the portal.

Configuring Wireless BYOD setup using Mozilla Firefox 64

When configuring wireless BYOD setup for the browser Firefox 64 and later releases, with operating systems Win RS4 or RS5, you may not be able to add Certificate Exception. This behaviour is expected in case of fresh installs of Firefox 64 and later releases, and does not occur in case of upgrading to Firefox 64 and above from a previous version. The following steps allow you to add certificate exception in this case:

Step 1 Configure for BYOD flow single or dual PEAP or TLS.

Step 2 Configure CP Policy with Windows ALL option.

Step 3 Connect Dot1.x or MAB SSID in end client Windows RS4 or Windows RS5.

Step 4 Type any URL in FF64 browser for redirection to Guest or BYOD portal.

Step 5 Click **Add Exception** > **Unable to add certificate**, and proceed with flow.

As a workaround, add the certificate manually for Firefox 64. In the Firefox 64 browser, choose **Options** > **Privacy & Settings** > **View Certificates** > **Servers** > **Add Exception**.

Delete a System Certificate

It is safe to delete system certificates that are tagged as ***Not in use*** in **Administration** > **System** > **Certificates** > **System Certificates**.

Although you can delete multiple certificates from the System Certificates store at a time, you must have at least one certificate to use for Admin and EAP authentication. Also, you cannot delete any certificate that is in use for Admin, EAP Authentication, Portals, or pxGrid controller. However, you can delete the pxGrid certificate when the service is disabled.

If you choose to delete a wildcard certificate, the certificate is removed from all the Cisco ISE nodes in the deployment.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **System Certificates**.

Step 2 Check the check boxes next to the certificates that you want to delete, and click **Delete**.

A warning message is displayed.

Step 3 Click **Yes** to delete the certificate.

Export a System Certificate

You can export a system certificate or a certificate and its associated private key. If you export a certificate and its private key for backup purposes, you can reimport them later if needed.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **System Certificates**.

Step 2 Check the check box next to the certificate that you want to export and click **Export**.

Step 3 Choose whether to export only the certificate, or the certificate and its associated private key.

Tip We do not recommend exporting the private key that is associated with a certificate because its value may be exposed. If you must export a private key (for example, when you export a wildcard system certificate to be imported into the other Cisco ISE nodes for inter-node communication), specify an encryption password for the private key. You must specify this password while importing this certificate into another Cisco ISE node to decrypt the private key.

Step 4 Enter the password if you have chosen to export the private key. The password should be at least eight characters long.

Step 5 Click **Export** to save the certificate to the file system that is running your client browser.

If you export only the certificate, the certificate is stored in the PEM format. If you export both the certificate and private key, the certificate is exported as a .zip file that contains the certificate in the PEM format and the encrypted private key file.

Trusted Certificates Store

The Trusted Certificates store contains X.509 certificates that are used for trust and for Simple Certificate Enrollment Protocol (SCEP).

X.509 certificates imported to Cisco ISE must be in PEM or Distinguished Encoding Rule format. Files containing a certificate chain, a system certificate along with the sequence of trust certificates that sign it, are imported, subject to certain restrictions.

When assigning public wildcard certificates to the guest portal and importing sub-CA with root-CA certificates, the certificate chain is not sent until the Cisco ISE services restart.

The certificates in the Trusted Certificate store are managed on the primary PAN, and are replicated to every node in the Cisco ISE deployment. Cisco ISE supports wildcard certificates.

Cisco ISE uses the trusted certificates for the following purposes:

- To verify client certificates used for authentication by endpoints, and by Cisco ISE administrators accessing ISE-PICthe administration portal using certificate-based administrator authentication.
- To enable secure communication between Cisco ISE nodes in a deployment. The Trusted Certificates store must contain the chain of CA certificates needed to establish trust with the system certificate on each node in a deployment.
    - If a self-signed certificate is used for the system certificate, the self-signed certificate from each node must be placed in the Trusted Certificates store of the PAN.
    - If a CA-signed certificate is used for the system certificate, the CA root certificate, and any intermediate certificates in the trust chain, must be placed in the Trusted Certificates store of the PAN.
- To enable Secure LDAP authentication, a certificate from the certificate store must be selected when defining an LDAP identity source that will be accessed over SSL.
- To distribute to personal devices preparing to register in the network using the personal devices portals. Cisco ISE implements the SCEP on PSNs to support personal device registration. A registering device uses the SCEP protocol to request a client certificate from a PSN. The PSN contains a registration authority (RA) that acts as an intermediary. The RA receives and validates the request from the registering device and then forwards the request to an external CA or the internal Cisco ISE CA, which issues the client certificate. The CA sends the certificate back to the RA, which returns it to the device.

  Each SCEP CA used by Cisco ISE is defined by a SCEP RA profile. When a SCEP RA profile is created, two certificates are automatically added to the Trusted Certificates store:

    - A CA certificate (a self-signed certificate)
    - An RA certificate (a Certificate Request Agent certificate), which is signed by the CA.

  The SCEP protocol requires that these two certificates be provided by the RA to a registering device. By placing these two certificates in the Trusted Certificates store, they are replicated to all PSN nodes for use by the RA on those nodes.

Note When a SCEP RA profile is removed, the associated CA chain is also removed from the Trusted Certificates store. However, if the same certificates are referenced by secure syslog, LDAP, system, or trust certificates, only the SCEP profile is deleted.

ISE Community Resource

Install a Third-Party CA Certificate in ISE

Certificates in Trusted Certificates Store

The Trusted Certificate store is prepopulated with trusted certificates: manufacturing certificate, root certificate, and other trusted certificates. The Root certificate (Cisco Root CA) signs the Manufacturing (Cisco CA

Manufacturing) certificate. These certificates are disabled by default. If you have Cisco IP phones as endpoints in your deployment, enable the root and manufacturing certificates so the Cisco-signed client certificates for the phones are authenticated.

List of Trusted Certificates

The following table describes the columns in the **Trusted Certificates** window, where the list of trusted certificates that are added to the administration node is displayed. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Trusted Certificates**.

Table 28: Trusted Certificates Window Columns

Field Name	Usage Guidelines
Friendly Name	Displays the name of the certificate.
Status	This column displays **Enabled** or **Disabled**. If the certificate is disabled, Cisco ISE will not use the certificate for establishing trust.
Trusted for	Displays one or more of the following services for which the certificate is used. • **Infrastructure** • **Cisco Services** • **Endpoints**
Issued To	Displays the common name of the certificate subject.
Issued By	Displays the common name of the certificate issuer.
Valid From	Displays the date and time when the certificate was issued. This value is also known as the "Not Before" certificate attribute.
Expiration Date	Displays the date and time when the certificate expires. This value is also known as the "Not After" certificate attribute.
Expiration Status	Provides information about the status of the certificate expiration. There are five icons and categories of informational message that are displayed in this column: • **Green**: Expiring in more than 90 days • **Blue**: Expiring in 90 days or less • **Yellow**: Expiring in 60 days or less • **Orange**: Expiring in 30 days or less • **Red**: Expired

Related Topics

Trusted Certificates Store, on page 301
View Trusted Certificates, on page 305
Change the Status of a Certificate in Trusted Certificates Store, on page 305
Add a Certificate to Trusted Certificates Store, on page 305

Trusted Certificate Naming Constraints

A trusted certificate in CTL may contain a name constraint extension. This extension defines a namespace for values of all subject name and subject alternative name fields of subsequent certificates in a certificate chain. Cisco ISE does not check constraints that are specified in a root certificate.

Cisco ISE supports the following name constraints:

- Directory name

  The directory name constraint should be a prefix of the directory name in the subject or subject alternative name field. For example:

  - Correct subject prefix:

    CA certificate name constraint: Permitted: O=Cisco

    Client certificate subject: O=Cisco,CN=Salomon

  - Incorrect subject prefix:

    CA certificate name constraint: Permitted: O=Cisco

    Client certificate subject: CN=Salomon,O=Cisco

- DNS
- Email
- URI (The URI constraint must start with a URI prefix such as http://, https://, ftp://, or ldap://).

Cisco ISE does not support the following name constraints:

- IP Address
- OtherName

When a trusted certificate contains a constraint that is not supported and the certificate that is being verified does not contain the appropriate field, Cisco ISE rejects the certificate because it cannot verify unsupported constraints.

The following is an example of the name constraints definition within the trusted certificate:

```
X509v3 Name Constraints: critical
                Permitted:
                  othername:<unsupported>
                  email:.abcde.at
                  email:.abcde.be
                  email:.abcde.bg
                  email:.abcde.by
                  DNS:.dir
                  DirName: DC = dir, DC = emea
                  DirName: C = AT, ST = EMEA, L = AT, O = ABCDE Group, OU = Domestic
                  DirName: C = BG, ST = EMEA, L = BG, O = ABCDE Group, OU = Domestic
                  DirName: C = BE, ST = EMEA, L = BN, O = ABCDE Group, OU = Domestic
                  DirName: C = CH, ST = EMEA, L = CH, O = ABCDE Group, OU = Service Z100
                  URI:.dir
                  IP:172.23.0.171/255.255.255.255
                Excluded:
                  DNS:.dir
                  URI:.dir
```

An acceptable client certificate subject that matches the above definition is as follows:

```
          Subject: DC=dir, DC=emea, OU=+DE, OU=OU-Administration, OU=Users, OU=X1,
CN=cwinwell
```

View Trusted Certificates

The **Trusted Certificates** window lists all the trusted certificates that are available in Cisco ISE. To view the trusted certificates, you must be a Super Admin or System Admin.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 To view all the certificates, choose click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Trusted Certificates**. The Trusted Certificates window displayed, listing all the trusted certificates.

Step 2 Check the check box of the trusted certificate and click **Edit**, **View**, **Export**, or **Delete** to perform the required task.

Change the Status of a Certificate in Trusted Certificates Store

The status of a certificate must be enabled so that Cisco ISE can use the certificate for establishing trust. When a certificate is imported into the Trusted Certificates store, it is automatically enabled.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Trusted Certificates**.

Step 2 In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Certificates** > **Trusted Certificates**.

Step 3 Check the check box next to the certificate you want to enable or disable, and click **Edit**.

Step 4 Choose the status from the **Status** drop-down list.

Step 5 Click **Save**.

Add a Certificate to Trusted Certificates Store

The **Trusted Certificate** store window allows you to add CA certificates to Cisco ISE.

Before you begin

- To perform the following task, you must be a Super Admin or System Admin.
- The certificate that you want to add must be in the file system of the computer where your browser is running. The certificate must be in PEM or DER format.
- To use the certificate for Admin or EAP authentication, define the basic constraints in the certificate and set the CA flag to true.

Edit a Trusted Certificate

After you add a certificate to the Trusted Certificates store, you can further edit it by using the **Edit** options.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Trusted Certificates**.

Step 2 Check the check box next to the certificate that you want to edit, and click **Edit**.

Step 3 (Optional) Enter a name for the certificate in the **Friendly Name** field. If you do not specify a friendly name, a default name is generated in the following format:

common-name#issuer#nnnnn

Step 4 Define the usage of the certificate by checking the necessary check boxes in the **Trusted For** area.

Step 5 (Optional) Enter a description for the certificate in the **Description** field.

Step 6 Click **Save**.

Trusted Certificate Settings

The following table describes the fields in the **Edit** window of a Trusted Certificate. Edit the CA certificate attributes in this window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Trusted Certificates**. Check the check box for the Trusted Certificate you want to edit, and click **Edit**.

Table 29: Trusted Certificate Edit Settings

Field Name	Usage Guidelines
Certificate Issuer	
Friendly Name	Enter a friendly name for the certificate. This is an optional field. If you do not enter a friendly name, a default name is generated in the following format: *common-name#issuer#nnnnn*
Status	Choose **Enabled** or **Disabled** from the drop-down list. If the certificate is disabled, Cisco ISE will not use the certificate for establishing trust.
Description	(Optional) Enter a description.
Usage	
Trust for authentication within ISE	Check this check box if you want this certificate to verify server certificates (from other Cisco ISE nodes or LDAP servers).

Field Name	Usage Guidelines
Trust for client authentication and Syslog	(Applicable only if you check the **Trust for authentication within ISE** check box) Check the check box if you want this certificate to be used to: • Authenticate endpoints that connect to Cisco ISE using the EAP protocol. • Trust a Syslog server.
Trust for certificate based admin authentication	You can check this check box only when **Trust for client authentication and Syslog** is selected. Check this check box to enable usage for certificate-based authentications for admin access. Import the required certificate chains into the Trusted Certificate store.
Trust for authentication of Cisco Services	Check this check box if you want this certificate to be used to trust external Cisco services such as the Feed Service.
Certificate Status Validation	Cisco ISE supports two ways of checking the revocation status of a client or server certificate that is issued by a particular CA. The first way is to validate the certificate using the Online Certificate Status Protocol (OCSP), which makes a request to an OCSP service maintained by the CA. The second way is to validate the certificate against a CRL which is downloaded from the CA into Cisco ISE. Both of these methods can be enabled, in which case OCSP is used first and only if a status determination cannot be made then the CRL is used.
Validate Against OCSP Service	Check the check box to validate the certificate against OCSP services. You must first create an OCSP Service to be able to check this box.
Reject the request if OCSP returns UNKNOWN status	Check the check box to reject the request if certificate status is not determined by the OCSP service. If you check this check box, an unknown status value that is returned by the OCSP service causes Cisco ISE to reject the client or server certificate currently being evaluated.
Reject the request if OCSP Responder is unreachable	Check the check box for Cisco ISE to reject the request if the OCSP Responder is not reachable.
Download CRL	Check the check box for the Cisco ISE to download a CRL.
CRL Distribution URL	Enter the URL to download the CRL from a CA. This field is automatically populated if it is specified in the certificate authority certificate. The URL must begin with “http”, “https”, or “ldap.”
Retrieve CRL	The CRL can be downloaded automatically or periodically. Configure the time interval between downloads.
If download failed, wait	Configure the time interval that Cisco ISE must wait Cisco ISE tries to download the CRL again.
Bypass CRL Verification if CRL is not Received	Check this check box, for the client requests to be accepted before the CRL is received. If you uncheck this check box, all client requests that use certificates signed by the selected CA will be rejected until Cisco ISE receives the CRL file.

Field Name	Usage Guidelines
Ignore that CRL is not yet valid or expired	Check this check box if you want Cisco ISE to ignore the start date and expiration date and continue to use the not yet active or expired CRL and permit or reject the EAP-TLS authentications based on the contents of the CRL. Uncheck this check box if you want Cisco ISE to check the CRL file for the start date in the Effective Date field and the expiration date in the Next Update field. If the CRL is not yet active or has expired, all authentications that use certificates signed by this CA are rejected.

Related Topics

Trusted Certificates Store, on page 301

Edit a Trusted Certificate, on page 306

Delete a Trusted Certificate

You can delete trusted certificates that you no longer need. However, you must not delete Cisco ISE internal CA certificates. Cisco ISE internal CA certificates can be deleted only when you replace the Cisco ISE root certificate chain for the entire deployment.

Step 1 Choose **Administration** > **System** > **Certificates** > **Trusted Certificates**.

Step 2 Check the check boxes next to the certificates that you want to delete, and click **Delete**.

A warning message is displayed. To delete the Cisco ISE Internal CA certificates, click one of the following options:

- **Delete**: To delete the Cisco ISE internal CA certificates. All endpoint certificates that are signed by the Cisco ISE internal CA become invalid and the endpoints cannot join the network. To allow the endpoints on the network again, import the same Cisco ISE internal CA certificates into the Trusted Certificates store.
- **Delete & Revoke**: Deletes and revokes the Cisco ISE internal CA certificates. All endpoint certificates that are signed by the Cisco ISE internal CA become invalid and the endpoints cannot get on to the network. This operation cannot be undone. You must replace the Cisco ISE root certificate chain for the entire deployment.

Step 3 Click **Yes** to delete the certificate.

Export a Certificate from Trusted Certificates Store

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Note If you export certificates from the internal CA and plan to use the exported certificates to restore from backup, use the CLI command **application configure ise**. See Export Cisco ISE CA Certificates and Keys, on page 341.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Trusted Certificates**.

Step 2 Check the check box next to the certificate that you want to export, and click **Export**. You can export only one certificate at a time.

Step 3 The chosen certificate downloads in the PEM format into the file system that is running your client browser.

Import a Root Certificate into the Trusted Certificate Store

When you import the root CA and intermediate CA certificates, specify the services for which the trusted CA certificates are to be used.

When you import an external root CA certificate, enable the **Trust for certificate based admin authentication** usage option in Step 5 of the following task.

Before you begin

You must have the root certificate and other intermediate certificates from the CA that signed your certificate signing requests and returned the digitally signed CA certificates.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Trusted Certificates**.

Step 2 Click **Import**.

Step 3 In the **Import a new Certificate into the Certificate Store** window, click **Choose File** to select the root CA certificate that is signed and returned by your CA.

Step 4 Enter a **Friendly Name**.

If you do not enter a **Friendly Name**, Cisco ISE autopopulates this field with a name of the format *common-name#issuer#nnnnn*, where *nnnnn* is a unique number. You can also edit the certificate later to change the **Friendly Name**.

Step 5 Check the check boxes next to the services for which you want to use this trusted certificate.

Step 6 (Optional) In the **Description** field, enter a description for your certificate.

Step 7 Click **Submit**.

What to do next

Import the intermediate CA certificates into the Trusted Certificates store (if applicable).

Trusted Certificate Import Settings

The following table describes the fields in the Trusted Certificate Import window, which you can use to add CA certificates to Cisco ISE. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Trusted Certificates** > **Import**.

Table 30: Trusted Certificate Import Settings

Field Name	Description
Certificate File	Click **Browse** to choose the certificate file from the computer that is running the browser.
Friendly Name	Enter a friendly name for the certificate. If you do not specify a name, Cisco ISE automatically creates a name in the format <common name>#<issuer>#<nnnnn>, where <nnnnn> is a unique five-digit number.
Trust for authentication within ISE	Check the check box if you want this certificate to be used to verify server certificates (from other ISE nodes or LDAP servers).
Trust for client authentication and Syslog	(Applicable only if you check the Trust for authentication within ISE check box) Check the check box if you want this certificate to be used to: • Authenticate endpoints that connect to ISE using the EAP protocol • Trust a Syslog server
Trust for authentication of Cisco Services	Check this check box if you want this certificate to be used to trust external Cisco services such as the feed service.
Validate Certificate Extensions	(Only if you check both the Trust for client authentication and Enable Validation of Certificate Extensions options) Ensure that the “keyUsage” extension is present and the “keyCertSign” bit is set, and that the basic constraints extension is present with the CA flag set to true.
Description	Enter an optional description.

Related Topics

Trusted Certificates Store, on page 301

Certificate Chain Import, on page 310

Import a Root Certificate into the Trusted Certificate Store, on page 309

Certificate Chain Import

You can import multiple certificates from a single file that contains a certificate chain received from a Certificate store. All certificates in the file must be in the PEM format, and the certificates must be arranged in the following order:

- The last certificate in the file must be the client or server certificate issued by the CA.
- All preceding certificates must be the root CA certificate plus any intermediate CA certificates in the signing chain for the issued certificate.

Importing a certificate chain is a two-step process:

1. Import the certificate chain file into the Trusted Certificate store in the Cisco ISE administration portal. This operation imports all certificates from the file except the last one into the Trusted Certificates store.

2. Import the certificate chain file using the Bind a CA-Signed Certificate operation. This operation imports the last certificate from the file as a local certificate.

Install Trusted Certificates for Cisco ISE Inter Node Communication

When you set up the deployment, before you register a secondary node, you must populate the PAN's CTL with appropriate CA certificates that are used to validate the Admin certificate of the secondary node. The procedure to populate the CTL of the PAN is different for different scenarios:

- If the secondary node is using a CA-signed certificate to communicate with the Cisco ISE administration portal, you must import the CA-signed certificate of the secondary node, the relevant intermediate certificates (if any), and the root CA certificate (of the CA that signed the secondary node's certificate) into the CTL of the PAN.
- If the secondary node is using a self-signed certificate to communicate with the Cisco ISE administration portal, you can import the self-signed certificate of the secondary node into the CTL of the PAN.

Note

- If you change the Admin certificate on a registered secondary node, you must obtain appropriate CA certificates that can be used to validate the secondary node’s Admin certificate and import it into the CTL of the PAN.
- If you use self-signed certificates to secure communication between a client and PSN in a deployment, when BYOD users move from one location to another, EAP-TLS user authentication fails. For such authentication requests that have to be serviced between a few PSNs, you must secure communication between the client and the PSN with an externally-signed CA certificate or use wildcard certificates signed by an external CA.

Ensure that the certificate issued by the external CA has basic constraints defined and the CA flag is set to true. To install CA-signed certificates for inter-node communication:

Step 1 Create a Certificate-Signing Request and Submit it to a Certificate Authority, on page 315

Step 2 Import a Root Certificate into the Trusted Certificate Store, on page 309

Step 3 Bind a CA-Signed Certificate to a Certificate Signing Request, on page 316

Default Trusted Certificates in Cisco ISE

The Trusted Certificates store (click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Trusted Certificates**) in Cisco ISE includes some certificates that are available by default. These certificates are automatically imported into the store to meet security requirements. However, it is not mandatory for you to use all of them. Unless mentioned otherwise in the following table, you can use certificates of your choice instead of the ones that are already available.

Table 31: Default Trusted Certificates

Trusted Certificate Name	Serial Number	Purpose of Certificate	Cisco ISE Releases with Certificate
Baltimore CyberTrust Root CA	02 00 00 B9	This certificate can serve as the root CA certificate in CA chains used by cisco.com in some geographies. The certificate was also used in ISE 2.4 posture/CP update XML files when they hosted at https://s3.amazonaws.com.	Releases 2.4 and later.
DST Root CA X3 Certificate Authority	44 AF B0 80 D6 A3 27 BA 89 30 39 86 2E F8 40 6B	This certificate can serve as the root CA certificate for the CA chain used by cisco.com.	Releases 2.4 and later.
Thawte Primary Root CA	34 4E D5 57 20 D5 ED EC 49 F4 2F CE 37 DB 2B 6D	This certificate can serve as the root CA certificate for the CA chain used by cisco.com and perfigo.com.	Releases 2.4 and later.
VeriSign Class 3 Public Primary Certification Authority	18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A	This certificate serves as the root CA certificate for VeriSign Class 3 Secure Server CA-G3. You must use this certificate when configuring profiler feed services in Cisco ISE.	Releases 2.4 and later.
VeriSign Class 3 Secure Server CA - G3	6E CC 7A A5 A7 03 20 09 B8 CE BC F4 E9 52 D4 91	This is an intermediate CA certificate that expires on February 7, 2020. You do not need to renew this certificate. You can remove the certificate by following the task below.	Releases 2.4 and later.
Cisco CA Manufacturing	6A 69 67 B3 00 00 00 00 00 03	This certificate may be used by certain Cisco devices connecting to Cisco ISE. The certificate is disabled by default.	Releases 2.4 and 2.6.

Trusted Certificate Name	Serial Number	Purpose of Certificate	Cisco ISE Releases with Certificate
Cisco Manufacturing CA SHA2	02	This certificate can be used in CA chains for administrator authentications, endpoint authentications, and deployment infrastructure flows.	Releases 2.4 and later.
Cisco Root CA 2048	5F F8 7B 28 2B 54 DC 8D 42 A3 15 B5 68 C9 AD FF	This certificate can be used by certain Cisco devices connecting to Cisco ISE. The certificate is disabled by default.	Releases 2.4 and later.
Cisco Root CA M2	01	This certificate can be used in CA chains for administrator authentications, endpoint authentications, and deployment infrastructure flows.	Releases 2.4 and later.
DigiCert Root CA	02 AC 5C 26 6A 0B 40 9B 8F 0B 79 F2 AE 46 25 77	You must use this certificate for flows where guest login with Facebook is used.	Releases 2.4 and later.
DigiCert SHA2 High Assurance Server CA	04 E1 E7 A4 DC 5C F2 F3 6D C0 2B 42 B8 5D 15 9F	You must use this certificate for flows where guest login with Facebook is used.	Releases 2.4 and later.
HydrantID SSL ICA G2	75 17 16 77 83 D0 43 7E B5 56 C3 57 94 6E 45 63 B8 EB D3 AC	Trusted for Cisco services.	Releases 2.4 and 2.6.
QuoVadis Root CA 2	05 09	You must use this certificate in the profiler, posture, and client provisioning flows.	Releases 2.4 and later.
Cisco ECC Root CA	01	This certificate is part of the Cisco Trust root store bundle that is used in Cisco ISE.	Release 2.6.
Cisco Licensing Root CA	01	This certificate is part of the Cisco Trust root store bundle that is used in Cisco ISE.	Releases 2.6 and later.

Trusted Certificate Name	Serial Number	Purpose of Certificate	Cisco ISE Releases with Certificate
Cisco Root CA 2099	01 9A 33 58 78 CE 16 C1 C1	This certificate is part of the Cisco Trust root store bundle that is used in Cisco ISE.	Releases 2.6 and later.
Cisco Root CA M1	2E D2 0E 73 47 D3 33 83 4B 4F DD 0D D7 B6 96 7E	This certificate is part of the Cisco Trust Root Store bundle used in Cisco ISE.	Releases 2.6 and later.
Cisco RXC-R2	01	This certificate is part of the Cisco Trust root store bundle that is used in Cisco ISE.	Releases 2.6 and later.
DigiCert Global Root CA	08 3B E0 56 90 42 46 B1 A1 75 6A C9 59 91 C7 4A	This certificate is part of the Cisco Trust root store bundle that is used in Cisco ISE.	Releases 2.6 and later.
Cisco ECC Root CA 2099	03	This certificate is part of the Cisco Trust root store bundle that is used in Cisco ISE.	Releases 2.6 and later.

Remove a Default Trusted Certificate from Cisco ISE

- In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Trusted Certificates** to view all your trusted certificates.
- Export the certificate that you wish to delete and save it so that it can be imported again if needed.

  Check the check box against the certificate you wish to export, and click **Export** on the menu bar above. The key chain downloads to your system.
- Delete the certificate. Check the check box against the certificate you wish to delete, and click **Delete** on the menu bar above. You will not be allowed to delete the certificate if it is being used by any CA chain, Secure Syslog, or secure LDAP.
- Make the necessary configuration changes to remove the certificate from the CA chains, Secure Syslogs, and syslogs it is part of. Then, delete the certificate.
- After you delete the certificate, check that the related services (refer to the purpose of the certificate) are working as expected.

Stale System and Trusted Certificates

Stale certificates are certificates that don’t belong to any node in the deployment. These redundant certificates might accumulate in large numbers in the System and Trusted Certificate stores, leading to insufficient memory and latency issues. From with Cisco ISE Release 3.1, such redundant certificates carry a **Stale Certificate** status, enabling you to review and delete them.

Checking for Stale System and Trusted Certificates

The following checks are done to identify stale system and trusted certificates:

Stale System Certificates	Stale Trusted Certificates
• The **Issued To** field is checked to see if the hostname of any of the nodes in the deployment is a part of the issued system certificate. If there are no matches, the system certificate is considered to be stale. • The **SAN Extension** field of an issued system certificate must match the FQDN of a node in the deployment. If there are no matches, the system certificate is considered to be stale. • The **Subject Name Alternative (SAN)** field is checked for a wildcard entry. In the absence of a wildcard character, the system certificate is considered to be stale. **Note** Stale certificate checks are run for certificates signed by third-party CAs or the Cisco ISE CA. Self-signed certificates are exempt from these checks.	• When checking the internal CA certificate status, if the status is displayed as **Inactive** and the **StatusChangeReason** is **CertSuperseded**, the trusted certificate is considered to be stale. • The **Issued To** field is checked to see if the hostname of any of the nodes in the deployment is a part of the issued trusted certificate. If there are no matches, the trusted certificate is considered to be stale.

Certificate-Signing Requests

For a CA to issue a signed certificate, you must create a certificate signing request and submit it to the CA.

The list of certificate-signing requests that you have created is available in the **Certificate-Signing Requests** window. To view this window, click the **Menu** icon (☰) and choose**Administration** > **System** > **Certificates** > **Certificate-Signing Requests**. To obtain signatures from a CA, you must export the certificate-signing request and then send the certificates to the CA. The CA signs and returns your certificates.

You can manage the certificates centrally from the Cisco ISE administration portal. You can create certificate-signing requests for all the nodes in your deployment and export them. Then, you should submit the certificate-signing requests to a CA, obtain the signed certificates from the CA, import the root and intermediary CA certificates given by the CA into the Trusted Certificates store, and bind the CA-signed certificates to the certificate-signing requests.

Create a Certificate-Signing Request and Submit it to a Certificate Authority

You can generate a certificate-signing request to obtain a CA-signed certificate for the nodes in your deployment. You can generate the certificate-signing request for a specific node in the deployment or for all the nodes in your deployment.

Step 1 Choose **Administration** > **System** > **Certificates** > **Certificate-Signing Requests**.

Step 2 Click **Generate Certificate-Signing Requests (CSR)** to generate the certificate-signing request.

Step 3 Enter the values for generating a certificate-signing request. See Trusted Certificate Settings, on page 306 for information on each of the fields in the window displayed.

Step 4 (Optional) Check the check box of the signing request that you want to download and and click **Export** to download the request.

Step 5 Copy all the text from "**-----BEGIN CERTIFICATE REQUEST-----**" through "**-----END CERTIFICATE REQUEST-----.**" and paste the contents of the request in the certificate request of the chosen CA.

Step 6 Download the signed certificate.

Some CAs might email the signed certificate to you. The signed certificate is in the form of a .zip file that contains the newly issued certificate and the public signing certificates of the CA that you must add to the Cisco ISE trusted certificates store. The digitally-signed CA certificate, root CA certificate, and other intermediate CA certificate (if applicable) can be downloaded to the local system running your client browser.

Bind a CA-Signed Certificate to a Certificate Signing Request

After the CA returns the digitally signed certificate, you must bind it to the certificate-signing request. You can perform the bind operation for all the nodes in your deployment, from the Cisco ISE administration portal.

Before you begin

- You must have the digitally signed certificate, and the relevant root intermediate CA certificates sent by the CA.
- Import the relevant root and intermediate CA certificates to the Trusted Certificates store (click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Trusted Certificates**).

Step 1 Choose **Administration** > **System** > **Certificates** > **Certificate-Signing Requests**.

Step 2 Check the check box next to the certificate signing request you must bind with the CA-signed certificate.

Step 3 Click **Bind Certificate**.

Step 4 In the **Bind CA Signed Certificate** window displayed, click **Choose File** to choose the CA-signed certificate.

Step 5 Enter a value in the **Friendly Name** field.

Step 6 Check the **Validate Certificate Extensions** check box if you want Cisco ISE to validate certificate extensions.

If you enable the **Validate Certificate Extensions** option, and the certificate that you import contains a basic constraints extension with the CA flag set to True, ensure that the key usage extension is present, and that the keyEncipherment bit or the keyAgreement bit, or both, are also set.

Note Cisco ISE requires EAP-TLS client certificates to have digital signature key usage extension.

Step 7 (Optional) Check the services for which this certificate will be used in the **Usage** area.

This information is autopopulated if you have enabled the **Usage** option while generating the certificate signing request. You can also choose to edit the certificate at a later time to specify the usage.

Changing the **Admin** usage certificate on a primary PAN restarts the services on all the other nodes. The system restarts one node at a time, after the primary PAN restarts.

Step 8 Click **Submit** to bind the certificate-signing request with the CA-signed certificate.

If this certificate is marked for Cisco ISE internode communication usage, the application server on the Cisco ISE node restarts.

Repeat this process to bind the certificate-signing request with the CA-signed certificate on the other nodes in the deployment.

What to do next

Import a Root Certificate into the Trusted Certificate Store, on page 309

Export a Certificate-Signing Request

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration** > **System** > **Certificates** > **Certificate-Signing Requests**.

Step 2 Check the check box next to the certificates that you want to export, and click **Export**.

Step 3 The certificate-signing request is downloaded to your local file system.

Certificate-Signing Request Settings

Cisco ISE allows you to generate certificate-signing requests for all the nodes in your deployment from the administration portal in a single request. Also, you can choose to generate the certificate signing request for a single node or multiple both nodes in the deployment. If you choose to generate a certificate signing request for a single node, ISE automatically substitutes the Fully Qualified Domain Name (FQDN) of that particular node in the CN field of the certificate subject. If you enter a domain name other than the FQDN of that node in the CN field, Cisco ISE rejects authentication with that certificate. If you choose to include an entry in the Subject Alternative Name (SAN) field of the certificate, you must enter the FQDN of the ISE node in addition to other SAN attributes. If necessary, you can also add additional FQDNs in the SAN field. If you choose to generate certificate signing requests for all the nodes in your deployment, check the Allow Wildcard Certificates check box and enter the wildcard FQDN notation in the SAN field (DNS name), for example, *.amer.example.com. If you plan to use the certificate for EAP Authentication, do not enter the wildcard value in the CN= field.

With the use of wildcard certificates, you no longer have to generate a unique certificate for each Cisco ISE node. Also, you no longer have to populate the SAN field with multiple FQDN values to prevent certificate warnings. Using an asterisk (*) in the SAN field allows you to share a single certificate across multiple both nodes in a deployment and helps prevent certificate name mismatch warnings. However, use of wildcard certificates is considered less secure than assigning a unique server certificate for each Cisco ISE node.

The following table describes the fields in the certificate-signing request window, which you can use to generate a certificate-signing request that can be signed by a Certificate Authority (CA). To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Certificate Management** > **Certificate-Signing Request**.

Table 32: Certificate-Signing Request Settings

Field	Usage Guidelines
Certificate(s) will be used for	

Field	Usage Guidelines

	Choose the service for which you are going to use the certificate:
	Cisco ISE Identity Certificates
	• **Multi-Use**: Used for multiple services (Admin, EAP-TLS Authentication, pxGrid, and Portal). Multi-use certificates use both client and server key usages. The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties:
	  • **Key Usage**: Digital Signature (Signing)
	  • **Extended Key Usage**: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) and TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)
	• **Admin**: Used for server authentication (to secure communication with the Admin portal and between ISE nodes in a deployment). The certificate template on the signing CA is often called a Web Server certificate template. This template has the following properties:
	  • **Key Usage**: Digital Signature (Signing)
	  • **Extended Key Usage**: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)
	• **EAP Authentication**: Used for server authentication. The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties:
	  • **Key Usage**: Digital Signature (Signing)
	  • **Extended Key Usage**: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)
	Note Digital signature key usage is required for EAP-TLS client certificates.
	• **RADIUS DTLS**: Used for RADIUS DTLS server authentication. This template has the following properties:
	  • **Key Usage**: Digital Signature (Signing)
	  • **Extended Key Usage**: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)
	• **ISE Messaging Service**: Used by the feature Syslog Over Cisco ISE Messaging, which enables MnT WAN survivability for built-in UDP syslog collection targets (LogCollector and LogCollector2).
	  • **Key Usage**: Digital Signature (Signing)
	  • **Extended Key Usage**: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)
	• **Portal**: Used for server authentication (to secure communication with all ISE web portals). The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties:
	  • **Key Usage**: Digital Signature (Signing)
	  • **Extended Key Usage**: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)
	• **pxGrid**: Used for both client and server authentication (to secure communication between the pxGrid client and server). The certificate template on the signing CA is often called a Computer or Machine

Field	Usage Guidelines

	certificate template. This template has the following properties:
	  • **Key Usage**: Digital Signature (Signing)
	  • **Extended Key Usage**: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) and TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)
	• **SAML**: Server certificate used to secure communication with the SAML Identity Provider (IdP). A certificate designated for SAML use cannot be used for any other service such as Admin, EAP authentication, and so on.
	  • **Key Usage**: Digital Signature (Signing)
	  • **Extended Key Usage**: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)
	Note We recommend that you do not use a certificate that contains the value of 2.5.29.37.0 for the Any Purpose object identifier in the Extended Key Usage attribute. If you use a certificate that contains the value of 2.5.29.37.0 for the Any Purpose object identifier in the Extended Key Usage attribute, the certificate is considered invalid and the following error message is displayed:
	`source=local ; type=fatal ; message="unsupported certificate"`
	Cisco ISE Certificate Authority Certificates
	• **ISE Root CA**: (Applicable only for the internal CA service) Used for regenerating the entire internal CA certificate chain including the root CA on the Primary PAN and subordinate CAs on the PSNs.
	• **ISE Intermediate CA**: (Applicable only for the internal CA service when ISE acts as an intermediate CA of an external PKI) Used to generate an intermediate CA certificate on the Primary PAN and subordinate CA certificates on the PSNs. The certificate template on the signing CA is often called a Subordinate Certificate Authority. This template has the following properties:
	  • **Basic Constraints**: Critical, Is a Certificate Authority
	  • **Key Usage**: Certificate Signing, Digital Signature
	  • **Extended Key Usage**: OCSP Signing (1.3.6.1.5.5.7.3.9)
	• **Renew ISE OCSP Responder Certificates**: (Applicable only for the internal CA service) Used to renew the ISE OCSP responder certificate for the entire deployment (and is not a certificate signing request). For security reasons, we recommend that you renew the ISE OCSP responder certificates every six months.

Allow Wildcard Certificates	Check this check box to use a wildcard character (*) in the CN and/or the DNS name in the SAN field of the certificate. If you check this check box, all the nodes in the deployment are selected automatically. You must use the asterisk (*) wildcard character in the left-most label position. If you use wildcard certificates, we recommend that you partition your domain space for greater security. For example, instead of *.example.com, you can partition it as *.amer.example.com. If you do not partition your domain, it might lead to security issues.
Generate CSRs for these Nodes	Check the check boxes next to the nodes for which you want to generate the certificate. To generate a CSR for select nodes in the deployment, you must uncheck the Allow Wildcard Certificates option.

Field	Usage Guidelines
Common Name (CN)	By default, the common name is the FQDN of the ISE node for which you are generating the certificate signing request. $FQDN$ denotes the FQDN of the ISE node. When you generate certificate signing requests for multiple nodes in the deployment, the Common Name field in the certificate signing requests is replaced with the FQDN of the respective ISE nodes.
Organizational Unit (OU)	Organizational Unit name. For example, Engineering.
Organization (O)	Organization name. For example, Cisco.
City (L)	(Do not abbreviate) City name. For example, San Jose.
State (ST)	(Do not abbreviate) State name. For example, California.
Country (C)	Country name. You must enter the two-letter ISO country code. For example, US.
Subject Alternative Name (SAN)	An IP address, DNS name, Uniform Resource Identifier (URI), or Directory Name that is associated with the certificate. • **DNS Name**: If you choose the DNS name, enter the fully qualified domain name of the ISE node. If you have enabled the Allow Wildcard Certificates option, specify the wildcard notation (an asterisk and a period before the domain name). For example, *.amer.example.com. • **IP Address**: IP address of the ISE node to be associated with the certificate. • **Uniform Resource Identifier**: A URI that you want to associate with the certificate. • **Directory Name**: A string representation of distinguished name(s) (DNs) defined per RFC 2253. Use a comma (,) to separate the DNs. For “dnQualifier” RDN, escape the comma and use backslash-comma “\,” as separator. For example, CN=AAA,dnQualifier=O=Example\,DC=COM,C=IL
Key Type	Specify the algorithm to be used for creating the public key: RSA or ECDSA.
Key Length	Specify the bit size for the public key. The following options are available for RSA: • 512 • 1024 • 2048 • 4096 The following options are available for ECDSA: • 256 • 384 **Note** RSA and ECDSA public keys might have different key length for the same security level. Choose 2048 or greater if you plan to get a public CA-signed certificate or deploy Cisco ISE as a FIPS-compliant policy management system.

Field	Usage Guidelines
Digest to Sign With	Choose one of the following hashing algorithm: SHA-1 or SHA-256.
Certificate Policies	Enter the certificate policy OID or list of OIDs that the certificate should conform to. Use comma or space to separate the OIDs.

Related Topics

Certificate-Signing Requests, on page 315
Create a Certificate-Signing Request and Submit it to a Certificate Authority, on page 315
Bind a CA-Signed Certificate to a Certificate Signing Request, on page 316

Set Up Certificates for Portal Use

With multiple PSNs in a deployment that can service a web portal request, Cisco ISE needs a unique identifier to identify the certificate that must be used for portal communication. When you add or import certificates that are designated for portal use, define a certificate group tag and associate it with the corresponding certificate on each node in your deployment. Associate this certificate group tag to the corresponding end-user portals (guest, sponsor, and personal devices portals). This certificate group tag is the unique identifier that helps Cisco ISE identify the certificate that must be used when communicating with each of these portals. You can only designate one certificate from each node for each of the portals.

Note Cisco ISE presents the Portal certificate on TCP port 8443 (or the port that you have configured for portal use).

Step 1 Create a Certificate-Signing Request and Submit it to a Certificate Authority, on page 315.

You must choose a Certificate Group Tag that you have already defined or create a new one for the portal. For example, mydevicesportal.

Step 2 Import a Root Certificate into the Trusted Certificate Store, on page 309.

Step 3 Bind a CA-Signed Certificate to a Certificate Signing Request, on page 316.

Reassign Default Portal Certificate Group Tag to CA-Signed Certificate

By default, all Cisco ISE portals use the self-signed certificate. If you want to use a CA-signed certificate for portals, you can assign the default portal certificate group tag to a CA-signed certificate. You can use an existing CA-signed certificate or generate a CSR and obtain a new CA-signed certificate for portal use. You can reassign any portal group tag from one certificate to another.

Note When you add a new certificate, you can reassign the portal group tag from the Default Portal Certificate Group tag to a different portal group tag. This will change all the portals that are associated with the certificate by default, to those that are mapped to that portal group tag only. The system displays a list of these portals. When you edit an existing certificate, if the portal tag that is associated with the certificate is already in use by any of the portals, then you cannot reassign the Default Portal Certificate Group tag or any other portal group tag to this certificate.

The following procedure describes how to reassign the default portal certificate group tag to a CA-signed certificate.

Step 1 Choose **Administration** > **System** > **Certificates** > **System Certificates**.

Hover the mouse over the i icon next to the Default Portal Certificate Group tag to view the list of portals that use this tag. You can also view the ISE nodes in the deployment that have portal certificates which are assigned this tag.

Step 2 Check the check box next to the CA-signed certificate that you want to use for portals, and click **Edit**.

Be sure to choose a CA-signed certificate that is not in use by any of the portals.

Step 3 Under the **Usage** area, check the **Portal** check box and choose the Default Portal Certificate Group Tag.

Step 4 Click **Save**.

A warning message appears.

Step 5 Click **Yes** to reassign the default portal certificate group tag to the CA-signed certificate.

Associate Portal Certificate Tag Before You Register a Node

If you use the "Default Portal Certificate Group" tag for all the portals in your deployment, before you register a new ISE node, ensure that you import the relevant CA-signed certificate, choose "Portal" as a service, and associate the "Default Portal Certificate Group" tag with this certificate.

When you add a new node to a deployment, the default self-signed certificate is associated with the "Default Portal Certificate Group" tag and the portals are configured to use this tag.

After you register a new node, you cannot change the Certificate Group tag association. Therefore, before you register the node to the deployment, you must do the following:

Step 1 Create a self-signed certificate, choose "Portal" as a service, and assign a different certificate group tag (for example, tempportaltag).

Step 2 Change the portal configuration to use the newly created certificate group tag (tempportaltag).

Step 3 Edit the default self-signed certificate and remove the Portal role.

This option removes the Default Portal Certificate Group tag association with the default self-signed certificate.

Step 4 Do one of the following:

Option	Description
Generate a CSR	When you generate the CSR:

Option	Description
	a. Choose "Portal" as a service for which you will use this certificate and associate the "Default Portal Certificate Group" tag. **b.** Send the CSR to a CA and obtain the signed certificate. **c.** Import the root and any other intermediate certificates of the CA that signed your certificate in to the Trusted Certificates store. **d.** Bind the CA-signed certificate with the CSR.
Import the private key and the CA-signed certificate	When you import the CA-signed certificate: **a.** Choose "Portal" as a service for which you will use this certificate and associate the "Default Portal Certificate Group" tag. **b.** Import the root and any other intermediate certificates of the CA that signed your certificate in to the Trusted Certificates store.
Edit an existing CA-signed certificate.	When you edit the existing CA-signed certificate: Choose "Portal" as a service for which you will use this certificate and associate the "Default Portal Certificate Group" tag.

Step 5 Register the ISE node to the deployment.
The portal configuration in the deployment is configured to the "Default Portal Certificate Group" tag and the portals are configured to use the CA-signed certificate associated with the "Default Portal Certificate Group" tag on the new node.

User and Endpoint Certificate Renewal

By default, Cisco ISE rejects a request that comes from a device whose certificate has expired. However, you can change this default behavior and configure ISE to process such requests and prompt the user to renew the certificate.

If you choose to allow the user to renew the certificate, Cisco recommends that you configure an authorization policy rule which checks if the certificate has been renewed before processing the request any further. Processing a request from a device whose certificate has expired may pose a potential security threat. Hence, you must configure appropriate authorization profiles and rules to ensure that your organization’s security is not compromised.

Some devices allow you to renew the certificates before and after their expiry. But on Windows devices, you can renew the certificates only before it expires. Apple iOS, Mac OSX, and Android devices allow you to renew the certificates before or after their expiry.

Dictionary Attributes Used in Policy Conditions for Certificate Renewal

Cisco ISE certificate dictionary contains the following attributes that are used in policy conditions to allow a user to renew the certificate:

- Days to Expiry: This attribute provides the number of days for which the certificate is valid. You can use this attribute to create a condition that can be used in authorization policy. This attribute can take a value from 0 to 15. A value of 0 indicates that the certificate has already expired. A value of 1 indicates that the certificate has less than 1 day before it expires.

- Is Expired: This Boolean attribute indicates whether a certificate has expired or not. If you want to allow certificate renewal only when the certificate is near expiry and not after it has expired, use this attribute in authorization policy condition.

CWA Redirect to a Renew Certificate

If a user certificate is revoked before its expiry, Cisco ISE checks the CRL published by the CA and rejects the authentication request. In case, if a revoked certificate has expired, the CA may not publish this certificate in its CRL. In this scenario, it is possible for Cisco ISE to renew a certificate that has been revoked. To avoid this, before you renew a certificate, ensure that the request gets redirected to Central Web Authentication (CWA) for a full authentication. You must create an authorization profile to redirect the user for CWA.

Configure Cisco ISE to Allow Users to a Renew Certificate

You must complete the tasks listed in this procedure to configure Cisco ISE to allow users to renew certificates.

Before you begin

Configure a limited access ACL on the WLC to redirect a CWA request.

Step 1 Update the Allowed Protocol Configuration, on page 325

Step 2 Create an Authorization Policy Profile for CWA Redirection, on page 326

Step 3 Create an authorization policy rule to renew the certificate.

Step 4 Enable BYOD Settings in Guest Portal, on page 326

Update the Allowed Protocol Configuration

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **Authentication** > **Allowed Protocols** > **Default Network Access**.

Step 2 Check the **Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy** check box under the EAP-TLS protocol and EAP-TLS inner methods for PEAP and EAP-FAST protocols.

Requests that use the EAP-TLS protocol will go through the NSP flow.

For PEAP and EAP-FAST protocols, you must manually install and configure Cisco AnyConnect for Cisco ISE to process the request.

Step 3 Click **Submit**.

What to do next

Create an Authorization Policy Profile for CWA Redirection, on page 326

Create an Authorization Policy Profile for CWA Redirection

Before you begin

Ensure that you have configured a limited access ACL on the WLC.

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.

Step 2 Click **Add**.

Step 3 Enter a name for the authorization profile. For example, CertRenewal_CWA.

Step 4 Check the **Web Redirection (CWA, DRW, MDM, NSP, CPP)** check box in the Common Tasks area.

Step 5 Choose **Centralized Web Auth** from the drop-down list and the limited access ACL.

Step 6 Check the **Display Certificates Renewal Message** check box.

The URL-redirect attribute value changes and includes the number of days for which the certificate is valid.

Step 7 Click **Submit**.

Enable BYOD Settings in Guest Portal

For a user to be able to renew a personal device certificate, you must enable the BYOD settings in the chosen guest portal.

Step 1 Choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals**.

a) Select the chosen CWA portal and click **Edit**.

Step 2 From BYOD Settings, check the **Allow employees to use personal devices on the network** check box.

Step 3 Click **Save**.

Certificate Renewal Fails for Apple iOS Devices

When you use ISE to renew the endpoint certificates on Apple iOS devices, you might see a “Profiled Failed to Install” error message. This error message appears if the expiring or expired network profiles were signed by a different Admin HTTPS certificate than the one that is used in processing the renewal, either on the same Policy Service Node (PSN) or on another PSN.

As a workaround, use a multi-domain SSL certificate, which is commonly referred to as Unified Communications Certificate (UCC), or a wildcard certificate for Admin HTTPS on all PSNs in the deployment.

Certificate Periodic Check Settings

Cisco ISE checks the Certificate Revocation Lists (CRL) periodically. Using this window, you can configure Cisco ISE to check ongoing sessions against CRLs that are downloaded automatically. You can specify the time of the day when the OCSP or CRL checks should begin each day and the time interval in hours that Cisco ISE waits before checking the OCSP server or CRLs again.

The following table describes the fields in the Certificate Periodic Check Settings window, which you can use to specify the time interval for checking the status of certificates (OCSP or CRL). To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Certificate Management** > **Certificate Periodic Check Settings**.

Table 33: Certificate Periodic Check Settings

Field Name	Usage Guidelines
Certificate Check Settings	
Check ongoing sessions against automatically retrieved CRL	Check this check box if you want Cisco ISE to check ongoing sessions against CRLs that are automatically downloaded.
CRL/OCSP Periodic Certificate Checks	
First check at	Specify the time of the day when the CRL or OCSP check should begin each day. Enter a value between 00:00 and 23:59 hours.
Check every	Specify the time interval in hours that Cisco ISE waits before checking the CRL or OCSP server again.

Cisco ISE doesn’t allow the specification of LDAP binding type in its CRL retrieval configuration, and connects to an LDAP URL using anonymous bind at the certificate distribution point. Cisco ISE only supports LDAP binding for authentication to LDAP servers.

Cisco ISE uses HTTP (port 80), HTTPS (port 443), and LDAP (port 389) protocols by default for CRL processes. In the case of Windows Vista SP1 and Windows Server 2008 endpoints, Microsoft only supports the following protocols for CRLs:

- HTTP: A PKI client only performs authentications for locally configured proxies. By default, authentication is performed only when a proxy server returns an error message that proxy authentication is required.
- LDAP: The PKI client signs and encrypts all LDAP traffic for PKI objects and only uses Kerberos authentication if authentication is required for network retrieval.

For more information, see What’s New in Certificate Revocation in Windows Vista and Windows Server 2008

Related Topics

OCSP Services, on page 360

Add OCSP Client Profiles, on page 363

Extract a Certificate and Private Key from a .pfx File

Cisco ISE does not allow import of certificates in .pfx format. Hence, if the certificate intended for import is in the .pfx format, you must convert it to .pem or .key file formats before import.

Before you begin

Ensure that OpenSSL is installed in the server that contains the SSL certificate.

Step 1 Start OpenSSL from the OpenSSL\bin folder.

Step 2 Open the command prompt and go to the folder that contains your .pfx file.

Step 3 Run the following command to extract the private key in .pem format: **openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes**

You will be prompted to type the import password. Type the password that you used to protect your keypair when you created the .pfx file. You will be prompted again to provide a new password to protect the .pem file that you are creating. Store the password to your key file in a secure place to avoid misuse.

Step 4 Run the following command to extract the certificate in .pem format: **openssl pkcs12 -in certname.pfx -nokeys -out cert.pem**

Step 5 Run the following command to decrypt the private key: **openssl rsa -in key.pem -out server.key**

Type the pasword that you created to protect the private key file in the previous step.

The .pem file and the decrypted and the encrypted .key files are available in the path, where you started OpenSSL.

Cisco ISE CA Service

Certificates can be self-signed or digitally signed by an external Certificate Authority (CA). The Cisco ISE Internal Certificate Authority (ISE CA) issues and manages digital certificates for endpoints from a centralized console to allow employees to use their personal devices on the company's network. A CA-signed digital certificate is considered industry standard and more secure. The Primary PAN is the Root CA. The Policy Service Nodes (PSNs) are subordinate CAs to the Primary PAN (SCEP RA). The ISE CA offers the following functionalities:

- Certificate Issuance: Validates and signs Certificate Signing Requests (CSRs) for endpoints that connect to your network.
- Key Management: Generates and securely stores keys and certificates on both PAN and PSN nodes.
- Certificate Storage: Stores certificates issued to users and devices.
- Online Certificate Status Protocol (OCSP) Support: Provides an OCSP responder to check for the validity of certificates.

When a CA Service is disabled on the primary administrative node, the CA service is still seen as running on the secondary administration node's CLI. Ideally, the CA service should be seen as disabled. This is a known Cisco ISE issue.

Cisco ISE Certificate Fingerprinting

Certificate fingerprinting process is used to evaluate certificate immediate Issuer Fingerprint SHA256 to match with the trusted certificates. This enforces a secured mechanism for multiple CAs to support different domains and also allows you to lock the trusted CAs for 802.1x protocol.

Ensure that the Issuer- Fingerprint SHA-256 certificate is added to your Cisco ISE deployment before updating the certificate in the policy condition.

Note After the trusted certificate is configured with a policy, you cannot delete the certificate. The following message is displayed in the **This Trusted Certificate Refered by Policy Sets** section in the **Trusted Certificates** window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Trusted Certificates**:

```
Certificate cannot be deleted because it is used in a policy. To delete
the certificate, please modify policy condition first.
```

To configure certificate fingerprint for Cisco ISE, follow the below steps in compliance with the order:

1. Create an internal user. For more information, see "Add Users" section in the chapter "Asset Visibility" in *Cisco Identity Services Engine Administrator Guide, Release 3.0*.
2. Add a network device. For more information, see "Add a Network Device in Cisco ISE" section in the chapter "Basic Setup"in *Cisco Identity Services Engine Administrator Guide, Release 3.0*.
3. Import external CA in **External Certificates**. For more information, see "Import a System Certificate" section in the chapter "Basic Setup" in *Cisco Identity Services Engine Administrator Guide, Release 3.0*.

   You can also import the Issuer- Fingerprint SHA-256 certificate using the SCEP protocol. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Certificate Authority** > **External CA Settings**. In the **Add SCEP RA Profile** window that is displayed, click **Add**. Enter the certificate name in the **Name** field. Enter the CA server URL in the **URL** field. Click **Test Connection**.
4. Create a Policy with SHA-256 Fingerprint.
5. Create and Map an Authentication Policy with SHA-256 Fingerprint.
6. Create an Authorization Policy.
7. Verify PRRT Logs.

Create a Policy with SHA-256 Fingerprint

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Set**.

Step 2 In the **Policy Set** window that is displayed, click **Settings** and from the drop down list, choose **insert a new row**.

Step 3 In the **New Policy Name** field, enter a name.

Step 4 Enter the **Description** for the policy.

Step 5 Click the **Add** (+) icon adjacent to the new **Policy Set Name** under the **Conditions** column.

Step 6 In the **Condition Studio** window that is displayed, click the **Click to Add Attribute** field.

Step 7 Select the **Network Access-Protocol** (**Dictionary-Attribute**) combination from the **All Dictionary** drop-down list.

Step 8 Select the **Equals** operator to build a logical condition.

Step 9 Choose **RADIUS** from the **Choose from List or Type** drop-down list.

Step 10 Click **Use**.

Step 11 In the **Policy Set** window that is displayed, from the **Allowed Protocols/ Server Sequence** drop down list, select **Default Network Access**.

Step 12 Click **Save**.

Create and Map an Authentication Policy with SHA-256 Fingerprint

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Set** > **Default**.

Step 2 Click **Authentication Policy**.

Step 3 Click the settings icon and choose **insert a new row**.

Step 4 In the **Authentication Rule Name** window, enter the name.

Step 5 Click on the **Add** (**+**) icon adjacent to the rule name.

Step 6 In the **Condition Studio** window that is displayed, click the **Click to add Attributes** field.

Step 7 Choose **CERTIFICATE-Issuer- Fingerprint SHA-256** (**Dictionary-Attribute**) combination from the **All Dictionary** drop-down list.

Step 8 Select the **Equals** operator to build a logical condition.

Step 9 Choose **Cisco Manufacturing CA SHA2 fingerprint sha256** from **Choose from List or Type** drop-down list.

Step 10 Click **Use**.

Step 11 In the **Policy Set** window that is displayed, from the **Allowed Protocols/Server Sequence** drop-down list, select **Preloaded_Certificate_Profile**.

Step 12 Click **Save**.

Create an Authorization Policy

Step 1 Choose In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Set** > **Default**.

Step 2 Click **Authorization Policy**.

Step 3 Click on the settings icon and choose **insert a new row**from the drop-down list.

Step 4 In the **Authorization Rule Name** window, enter the name.

Step 5 Click the **Add** (**+**) icon adjacent to the rule name.

Step 6 In the **Condition Studio** window that is displayed, click the **Click to Add Attributes** field.

Step 7 Select the **CERTIFICATE-Issuer- Fingerprint SHA-256** (**Dictionary-Attribute**) combination from the **All Dictionary** drop-down list.

Step 8 Select the **Equals** operator to build a logical condition.

Step 9 Select **Cisco Root CA 2099 fingerprint sha**from **Choose from List or Type** drop-down list.

Step 10 Click **Use**.

Step 11 In the **Policy Set** window that is displayed, from the **Allowed Protocols/Server Sequence** drop down list, select **PermitAccess**.

Step 12 Click **Save**.

Verify PRRT Logs

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operation** > **RADIUS** > **Live Logs**.

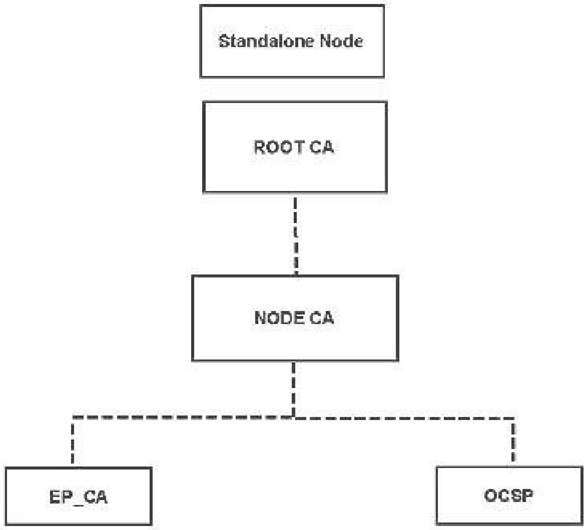
Step 2 In the **Live Logs** window that is displayed, click the latest log details.

Step 3 In the **Authentication Details** window that is displayed, view the SHA-256 value in the **Issuer- Fingerprint SHA-256** column to confirm that the **Issuer- Fingerprint SHA-256** certificate is successfully added and validated.

Cisco ISE CA Certificates Provisioned on Administration and Policy Service Nodes

After installation, a Cisco ISE node is provisioned with a Root CA certificate, and a Node CA certificate to manage certificates for endpoints.

Figure 8: Cisco ISE CA Certificates Provisioned on a Standalone Node

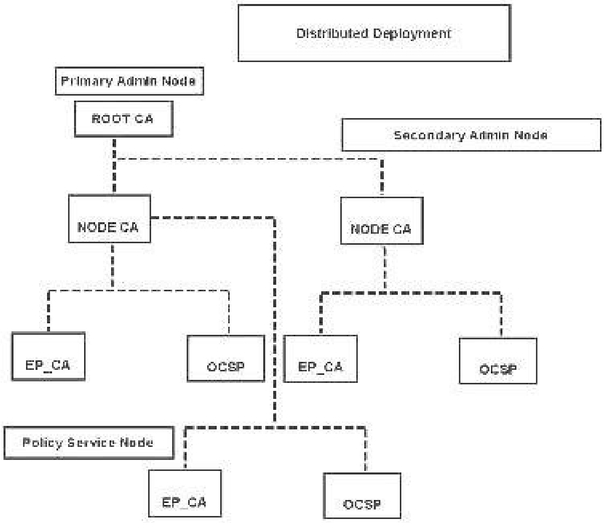


When you set up a deployment, the node that you designate as the Primary Administration Node (PAN) becomes the Root CA. The PAN has a Root CA certificate and a Node CA certificate that is signed by the Root CA.

When you register a Secondary Administration Node to the PAN, a Node CA certificate is generated and is signed by the Root CA on the Primary Administration Node.

Any Policy Service Node (PSN) that you register with the PAN is provisioned an Endpoint CA and an OCSP certificate signed by the Node CA of the PAN. The Policy Service Nodes (PSNs) are subordinate CAs to the PAN. When you use the ISE CA, the Endpoint CA on the PSN issues the certificates to the endpoints that access your network.

Figure 9: Cisco ISE CA Certificates Provisioned on Administration and Policy Service Nodes in a Deployment



Requirements for CA to Interoperate with Cisco ISE

While using a CA server with Cisco ISE, make sure that the following requirements are met:

- Key size should be 1024, 2048, or higher. In CA server, the key size is defined using certificate template. You can define the key size on Cisco ISE using the supplicant profile.
- Key usage should allow signing and encryption in extension.
- While using GetCACapabilities through the SCEP protocol, cryptography algorithm and request hash should be supported. It is recommended to use RSA and SHA1.
- Online Certificate Status Protocol (OCSP) is supported. This is not directly used in BYOD, but a CA which can act as an OCSP server can be used for certificate revocation.

Note Cisco ISE supports Enterprise Java Beans Certificate Authority (EJBCA) for standard EAP authentication like PEAP, EAP-TLS, and so on. You must disable the **Enable End Entity Profile Limitations** option (under **System > Basic Configurations**) in EJBCA to enable EJBCA support for proxy SCEP.

- If you use an enterprise PKI to issue certificates for Apple iOS devices, ensure that you configure key usage in the SCEP template and enable the **Key Encipherment** option.

  If you use Microsoft CA, edit the Key Usage Extension in the certificate template. In the **Encryption** area, click the **Allow Key Exchange only with Key Encryption (Key encipherment)** radio button and check the **Allow Encryption of User Data** check box.
- Cisco ISE supports the use of RSASSA-PSS algorithm for trusted certificates and endpoint certificates for EAP-TLS authentication. When you view the certificate, the signature algorithm is listed as 1.2.840.113549.1.1.10 instead of the algorithm name.

Note If you use the Cisco ISE internal CA for the BYOD flow, the Admin certificate should not be signed using the RSASSA-PSS algorithm (by an external CA). The Cisco ISE internal CA cannot verify an Admin certificate that is signed using this algorithm and the request would fail.

Client Certificate Requirements for Certificate-Based Authentication

For certificate-based authentication with Cisco ISE, the client certificate should meet the following requirements:

Table 34: Client-Certificate Requirements for RSA and ECC

RSA		
Supported Key Sizes	1024, 2048, and 4096 bits	
Supported Secure Hash Algorithms (SHA)	SHA-1 and SHA-2 (includes SHA-256)	
ECC [1] [2]		
Supported Curve Types	P-192, P-256, P-384, and P-521	
Supported Secure Hash Algorithm (SHA)	SHA-256	
Client Machine Operating Systems and Supported Curve Types		
Windows	8 and later	P-256, P-384, and P-521
Android	4.4 and later **Note** Android 6.0 requires May 2016 patch to support ECC certificates.	All curve types (except Androidv6.0, which does not support the P-192 curve type).

[1] Windows 7 and Apple iOS do not natively support ECC for EAP-TLS authentication.

[2] This release of Cisco ISE does not support the use of ECC certificates on MAC OS X devices.

Cisco ISE CA Chain Regeneration

When you regenerate the Cisco ISE CA chain, all the certificates including the Root CA, Node CA, and Endpoint CA certificates are regenerated. You must regenerate the ISE CA chain when you change the domain name or hostname of your PAN or PSN.

When you regenerate a system certificate, whether root CA or an intermediate CA certificate, ISE Messaging Service restarts to load the new certificate chain. Audit logs will be lost until the ISE Messaging Service is available again.

Note

Whenever the Cisco ISE internal CA is replaced in a deployment, then the ISE messaging service must also be refreshed at that time to retrieve the complete certificate chain.

When you regenerate the Cisco ISE internal CA chain, the **Valid From** field of all the certificates in the chain will display the date one day previous to the day of regeneration.

If there is a change in domain or host name and if the root CA chain is regenerated, all the certificates including the system certificates will get updated with the new domain or host name except the SAML certificate. The SAML certificate has to be regenerated separately.

Cisco ISE Messaging Certificate Support with External CA

Cisco ISE Messaging certificate signed by an external CA must be configured with EKU client and server authentication (like pxGrid). To configure the pxGrid template, see: https://community.cisco.com/t5/security-documents/deploying-certificates-with-cisco-pxgrid-using-an-external/ta-p/3639677. The Cisco ISE Messaging Certificate must be either signed internally by Cisco ISE or by an external (third-party) CA on all nodes. It cannot be a combination of both signatures.

Wildcard certificates are not supported.

Elliptical Curve Cryptography Certificates Support

Cisco ISE CA service supports certificates that are based on Elliptical Curve Cryptography (ECC) algorithms. ECC offers more security and better performance than other cryptographic algorithms even when using a much smaller key size.

The following table compares the key sizes of ECC and RSA and security strength.

ECC Key Size (in bits)	RSA Key Size (in bits)
160	1024
224	2048
256	3072
384	7680
521	15360

Because of the smaller key size, encryption is quicker.

Cisco ISE supports the following ECC curve types. The higher the curve type or key size, the greater is the security.

- P-192
- P-256
- P-384
- P-521

ISE does not support explicit parameters in the EC part of a certificate. If you try to import a certificate with explicit parameters, you get the error: Validation of certificate failed: Only named ECParameters supported.

Cisco ISE CA service supports ECC certificates for devices connecting through the BYOD flow. You can also generate ECC certificates from the Certificate Provisioning Portal.

Note The following table lists the operating systems and versions that support ECC along with the supported curve types. If your devices are not running a supported operating system or on a supported version, you can use RSA-based certificates instead.

Operating System	Supported Versions	Supported Curve Types
Windows	8 and later	P-256, P-384, and P-521
Android	4.4 and later **Note** Android 6.0 requires May 2016 patch to support ECC certificates.	All curve types (except Android 6.0, which does not support the P-192 curve type).

Windows 7 and Apple iOS do not natively support ECC for authentication over EAP-TLS. This release of Cisco ISE does not support the use of ECC certificates on MAC OS X devices.

If the BYOD flow with Enrollment over Secure Transport (EST) protocol is not working properly, check the following:

- Certificate Services Endpoint Sub CA certificate chain is complete. To check whether the certificate chain is complete:
  1. Choose **Administration** > **System** > **Certificates** > **Certificate Authority** > **Certificate Authority Certificates**.
  2. Check the check box next to the certificate that you want to check and click **View**.
- Ensure that the CA and EST services are up and running. If the services are not running, go to **Administration** > **System** > **Certificates** > **Certificate Authority** > **Internal CA Settings** to enable the CA service.

Note

- This release of Cisco ISE does not support EST clients to authenticate directly against the EST Server residing within Cisco ISE. While on-boarding an Android or a Windows endpoint, ISE triggers an EST flow if the request is for an ECC-based certificate.
- BYOD flow with Android clients might fail when using EST protocol along with a static IP address, an FQDN or a hostname in the authorization profile. The workaround is to use SCEP instead of EST. You can configure SCEP in the native supplicant profile. See Create Native Supplicant Profiles for more information.

Cisco ISE Certificate Authority Certificates

The Certificate Authority (CA) Certificates page lists all the certificates related to the internal Cisco ISE CA. In previous releases, these CA certificates were present in the Trusted Certificates store and are now moved to the CA Certificates page. These certificates are listed node wise in this page. You can expand a node to view all the ISE CA certificates of that particular node. The Primary and Secondary Administration nodes have the root CA, node CA, subordinate CA, and OCSP responder certificates. The other nodes in the deployment have the endpoint subordinate CA and OCSP certificates.

When you enable the Cisco ISE CA service, these certificates are generated and installed on all the nodes automatically. Also, when you replace the entire ISE Root CA Chain, these certificates are regenerated and installed on all the nodes automatically. There is no manual intervention required.

The Cisco ISE CA certificates follow the following naming convention: **Certificate Services** <***Endpoint Sub CA/Node CA/Root CA/OCSP Responder***>**-**<*node_hostname*>#*certificate_number*.

From the CA Certificates page, you can edit, import, export, delete, and view the Cisco ISE CA certificates.

Edit a Cisco ISE CA Certificate

After you add a certificate to the Cisco ISE CA Certificates Store, you can further edit it by using the edit settings.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration** > **System** > **Certificates** > **Certificate Authority** > **Certificate Authority Certificates.**.

Step 2 In the ISE-PIC GUI, click the **Menu** icon (☰) and choose .

Step 3 Check the check box next to the certificate that you want to edit, and click **Edit**.

Step 4 Modify the editable fields as required. See Trusted Certificate Settings, on page 306 for a description of the fields.

Step 5 Click **Save** to save the changes you have made to the certificate store.

Export a Cisco ISE CA Certificate

To export the Cisco ISE root CA and node CA certificates:

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration** > **System** > **Certificates** > **Certificate Authority** > **Certificate Authority Certificates**.

Step 2 In the ISE-PIC GUI, click the **Menu** icon (☰) and choose .

Step 3 Check the check box next to the certificate that you want to export, and click **Export**. You can export only one certificate at a time.

Step 4 Save the privacy-enhanced mail file to the file system that is running your client browser.

Import a Cisco ISE CA Certificate

If an endpoint tries to authenticate to your network using a certificate issued by Cisco ISE CA from another deployment, you must import the Cisco ISE root CA, node CA, and endpoint sub CA certificates from that deployment in to the Cisco ISE Trusted Certificates store.

Before you begin

- To perform the following task, you must be a Super Admin or System Admin.
- Export the ISE root CA, node CA, and endpoint sub CA certificates from the deployment where the endpoint certificate is signed and store it on the file system of the computer where your browser is running.

Step 1 Log in to the Admin Portal of the deployment where the endpoint is getting authenticated.

Step 2 Choose **Administration** > **System** > **Certificates** > **Trusted Certificates**.

Step 3 Click **Import**.

Step 4 Configure the field values as necessary. See Trusted Certificate Import Settings, on page 309 for more information.

If client certificate-based authentication is enabled, then Cisco ISE will restart the application server on each node in your deployment, starting with the application server on the PAN and followed, one-by-one, by each additional node.

Certificate Templates

Certificate templates contain properties that are common to all certificates issued by the Certificate Authority (CA) based on that template. The certificate template defines the Subject, Subject Alternative Name (SAN), key type, key size, SCEP RA profile that must be used, validity period of the certificate, and the extended key usage (EKU) that specifies whether the certificate has to be used for client or server authentication or both. The internal Cisco ISE CA (ISE CA) uses a certificate template to issue certificates based on that template.

Cisco ISE comes with the following default certificate templates for the ISE CA. You can create additional certificate templates, if needed. The default certificate templates are:

- CA_SERVICE_Certificate_Template—For other network services that use Cisco ISE as the Certificate Authority. For example, use this certificate template while configuring ISE to issue certificates for ASA VPN users. You can modify only the validity period in this certificate template.
- EAP_Authentication_Certificate_Template—For EAP authentication.
- pxGrid_Certificate_Template—For the pxGrid controller while generating the certificate from the Certificate Provisioning Portal.

Certificate Template Name Extension

The Cisco ISE Internal CA includes an extension to represent the certificate template that was used to create the endpoint certificate. All endpoint certificates issued by the internal CA contain a certificate template name extension. This extension represents the certificate template that was used to create that endpoint certificate. The extension ID is 1.3.6.1.4.1.9.21.2.5. You can use the CERTIFICATE: Template Name attribute in authorization policy conditions and assign appropriate access privileges based on the results of the evaluation.

Use Certificate Template Name in Authorization Policy Conditions

You can use the certificate template name extension in authorization policy rules.

Step 1 Choose **Policy** > **Policy Sets**, and expand the Default policy set to view the authorization policy rules.

Step 2 Add a new rule or edit an existing rule. This example describes editing the Compliant_Device_Access rule:

a) Edit the Compliant_Device_Access rule.
b) Choose **Add Attribute/Value**.
c) From Dictionaries, choose the **CERTIFICATE: Template Name** attribute and **Equals** operator.
d) Enter the value of the certificate template name. For example, EAP_Authentication_Certificate_Template.

Step 3 Click **Save**.

Deploy Cisco ISE CA Certificates for pxGrid Controller

Cisco ISE CA provides a certificate template for the pxGrid controller to generate a certificate from the Certificate Provisioning Portal.

Before you begin

Generate a certificate signing request (CSR) for the pxGrid client and copy the contents of the CSR in to the clipboard.

Step 1 Create a network access user account (Administration > Identity Management > Identities > Users > Add).

Make note of the user group to which the user is assigned.

Step 2 Edit the Certificate Provisioning Portal Settings (Administration > Device Portal Management > Certificate Provisioning).

a) Select the certificate provisioning portal and click **Edit**.
b) Click the **Portal Settings** drop-down list. From the Configure authorized groups Available list, select the user group to which the network access user belongs to and move it to Chosen list.
c) Click the **Certificate Provisioning Portal Settings** drop-down list. Choose the pxGrid_Certificate_Template. See Portal Settings for Certificate Provisioning Portal, on page 1308 for more information.
d) Save the portal settings.

Step 3 Launch the Certificate Provisioning Portal. Click the Portal Test URL link.

a) Log in to the Certificate Provisioning Portal using the user account created in step 1.
b) Accept the AUP and click **Continue**.
c) From the **I want to** drop-down list, choose **Generate a single certificate (with certificate signing request)**.
d) In the Certificate Signing Request Details field, paste the contents of the CSR from the clipboard.
e) From the **Certificate Download Format** drop-down list, choose **PKCS8 format**.

   Note If you choose the PKCS12 format, you must convert the single certificate file in to separate certificate and key files. The certificate and key files must be in binary DER encoded or PEM format before you can import them in to Cisco ISE.

f) From the **Choose Certificate Template** drop-down list, choose **pxGrid_Certificate_Template**.
g) Enter a certificate password.

h) Click **Generate**.

The certificate is generated.

i) Export the certificate.

The certificate along with the certificate chain is exported.

Step 4 Import the Cisco ISE CA chain in to the Trusted Certificates store in the pxGrid client.

MAC Randomization for BYOD

Android and iOS devices are increasingly using the *random MAC address* property by default. A device that has the random MAC address feature enabled uses a random MAC address for every SSID that it connects to. Cisco ISE and Mobile Device Management (MDM) systems receive different MAC addresses for the same device depending on which SSID they have connected with for a service. Therefore, a unique identifier called GUID is generated by the Cisco ISE provisioning service to identify an endpoint by the same value in both systems.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Certificate Authority** > **Certificate Templates**.

Step 2 Check the check box next to EAP Certificate Template.

Step 3 Click **Edit**.

Step 4 From the **Subject Alternative Name (SAN)** drop-down list, choose **MAC Address and GUID**.

To handle random and changing MAC addresses in BYOD flows, the Cisco ISE provisioning service generates a GUID value for Windows, iOS, and Android endpoints. If you have configured the Subject Alternative Name (SAN) of your certificate to include the GUID value to handle random MAC addresses in a BYOD flow, choose **Subject - Common Name** as the certificate attribute for identity validation when you configure a Create a Certificate Authentication Profile for TLS-Based Authentication to authenticate AD users.

Step 5 Click **Save**.

Simple Certificate Enrollment Protocol Profiles

To help enable certificate provisioning functions for the variety of mobile devices that users can register on the network, Cisco ISE enables you to configure one or more Simple Certificate Enrollment Protocol (SCEP) Certificate Authority (CA) profiles (called as Cisco ISE External CA Settings) to point Cisco ISE to multiple CA locations. The benefit of allowing for multiple profiles is to help ensure high availability and perform load balancing across the CA locations that you specify. If a request to a particular SCEP CA goes unanswered three consecutive times, Cisco ISE declares that particular server unavailable and automatically moves to the CA with the next lowest known load and response times, then it begins periodic polling until the server comes back online.

For details on how to set up your Microsoft SCEP server to interoperate with Cisco ISE, see

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf.

Issued Certificates

The Admin portal lists all the certificates issued by the internal ISE CA to endpoints (Administration > System > Certificates > Endpoint Certificates). The Issued Certificates page provides you an at-a-glance view of the certificate status. You can mouse over the Status column to find out the reason for revocation if a certificate has been revoked. You can mouse over the Certificate Template column to view additional details such as Key Type, Key Size or Curve Type, Subject, Subject Alternative Name (SAN), and Validity of the certificate. You can click on the endpoint certificate to view the certificate.

All certificates issued by the ISE CA (certificates automatically provisioned through the BYOD flow and certificates obtained from the Certificate Provisioning portal) are listed in the Endpoint Certificates page. You can manage these certificates from this page.

For example, if you want to view the certificates issued to user7, enter user7 in the text box that appears below the Friendly Name field. All the certificates issued by Cisco ISE to this user appear. Remove the search term from the text box to cancel the filter. You can also use the Advanced Filter option to view records based on various search criteria.

This Endpoint Certificates page also provides you the option to revoke an endpoint certificate, if necessary.

The Certificate Management Overview page displays the total number of endpoint certificates issued by each PSN node in your deployment. You can also view the total number of revoked certificates per node and the total number of certificates that have failed. You can filter the data on this page based on any of the attributes.

Issued and Revoked Certificates

The following table describes the fields on the Overview of Issued and Revoked Certificates window. The PSN nodes in your deployment issue certificates to endpoints. This window provides you information about the endpoint certificates issued by each of the PSN nodes in your deployment. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Overview**.

Note Expired or revoked issued certificates will be automatically deleted after 30 days.

Table 35: Issued and Revoked Certificates

Fields	Usage Guidelines
Node Name	Name of the Policy Service node (PSN) that issued the certificate.
Certificates Issued	Number of endpoint certificates issued by the PSN node.
Certificates Revoked	Number of revoked endpoint certificates (certificates that were issued by the PSN node).
Certificates Requests	Number of certificate-based authentication requests processed by the PSN node.
Certificates Failed	Number of failed authentication requests processed by the PSN node.

Related Topics

Issued Certificates, on page 340

User and Endpoint Certificate Renewal, on page 324
Configure Cisco ISE to Use Certificates for Authenticating Personal Devices, on page 344
Configure Cisco ISE to Allow Users to a Renew Certificate, on page 325
Revoke an Endpoint Certificate, on page 360

Backup and Restoration of Cisco ISE CA Certificates and Keys

You must back up the Cisco ISE CA certificates and keys securely to be able to restore them back on a Secondary Administration Node in case of a PAN failure and you want to promote the Secondary Administration Node to function as the root CA or intermediate CA of an external PKI. The Cisco ISE configuration backup does not include the CA certificates and keys. Instead, you should use the Command Line Interface (CLI) to export the CA certificates and keys to a repository and to import them. The **application configure ise** command now includes export and import options to backup and restore CA certificates and keys.

The following certificates from the Trusted Certificates Store are restored on the Secondary Administration Node:

- Cisco ISE Root CA certificate
- Cisco ISE Sub CA certificate
- Cisco ISE Endpoint RA certificate
- Cisco ISE OCSP Responder certificate

You must back up and restore Cisco ISE CA certificates and keys when you:

- Have a Secondary Administration Node in the deployment
- Replace the entire Cisco ISE CA root chain
- Configure Cisco ISE root CA to act as a subordinate CA of an external PKI
- Restore data from a configuration backup. In this case, you must first regenerate the Cisco ISE CA root chain and then back up and restore the ISE CA certificates and keys.

Note Whenever the Cisco ISE internal CA is replaced in a deployment, then the ISE messaging service must also be refreshed that time to retrieve the complete certificate chain.

Export Cisco ISE CA Certificates and Keys

You must export the CA certificates and keys from the PAN to import them on the Secondary Administration Node. This option enables the Secondary Administration Node to issue and manage certificates for endpoints when the PAN is down and you promote the Secondary Administration Node to be the PAN.

Before you begin

Ensure that you have created a repository to store the CA certificates and keys.

Step 1 Enter **application configure ise** command from the Cisco ISE CLI.

Step 2 Enter 7 to export the certificates and keys.

Step 3 Enter the repository name.

Step 4 Enter an encryption key.

A success message appears with the list of certificates that were exported, along with the subject, issuer, and serial number.

Example:

```
 The following 4 CA key pairs were exported to repository 'sftp' at 'ise_ca_key_pairs_of_ise-vm1':
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x621867df-568341cd-944cc77f-c9820765

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x7027269d-d80a406d-831d5c26-f5e105fa

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x1a65ec14-4f284da7-9532f0a0-8ae0e5c2

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x6f6d4097-21f74c4d-8832ba95-4c320fb1
ISE CA keys export completed successfully
```

Import Cisco ISE CA Certificates and Keys

After you register the Secondary Administration Node, you must export the CA certificates and keys from the PAN and import them in to the Secondary Administration Node.

Step 1 Enter **application configure ise** command from the Cisco ISE CLI.

Step 2 Enter 8 to import the CA certificates and keys.

Step 3 Enter the repository name.

Step 4 Enter the name of the file that you want to import. The file name should be in the format **`ise_ca_key_pairs_of_<vm hostname>`**.

Step 5 Enter the encryption key to decrypt the file.

A success message appears.

Example:

```
The following 4 CA key pairs were imported:
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x21ce1000-8008472c-a6bc4fd9-272c8da4

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x05fa86d0-092542b4-8ff68ed4-f1964a56

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x77932e02-e8c84b3d-b27e2f1c-e9f246ca

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x5082017f-330e412f-8d63305d-e13fd2a5

Stopping ISE Certificate Authority Service...
Starting ISE Certificate Authority Service...
ISE CA keys import completed successfully
```

Note Encryption of exported keys file was introduced in Cisco ISE Release 2.6. The export of keys from Cisco ISE Release 2.4 and earlier versions and import of keys in Cisco ISE Release 2.6 and later versions will not be successful.

Generate Root CA and Subordinate CAs on the Primary PAN and PSN

When you set up the deployment, Cisco ISE generates a root CA on the primary PAN and subordinate CA certificates on the PSNs for the Cisco ISE CA service. However, when you change the domain name or the hostname of the primary PAN or PSN, you must regenerate root CA on the primary PAN and sub CAs on the PSNs respectively.

If you want to change the hostname on a PSN, instead of regenerating the root CA and subordinate CAs on the primary PAN and PSNs respectively, you can deregister the PSN before changing the hostname, and register it back. A new subordinate certificate gets provisioned automatically on the PSN.

Note PXgrid and IMS certificates will not be replaced by Internal CA while regenerating root CA if the respective certificate is externally signed.

If you want to change the signing by Internal CA for PXgrid certificate, generate a self-signed Pxgrid certificate and regenerate the root CA.

If you want to change the signing by Internal CA for Cisco ISE Messaging Services certificate, regenerate the Cisco ISE Messaging Services certificate from the CSR page.

Step 1 Choose **Administration** > **System** > **Certificates** > **Certificate Signing Requests**

Step 2 Click **Generate Certificate Signing Requests (CSR)**.

Step 3 Choose ISE Root CA from the **Certificate(s) will be used for** drop-down list.

Step 4 Click **Replace ISE Root CA Certificate chain**.

The root CA and subordinate CA certificates get generated for all the nodes in your deployment.

Configure Cisco ISE Root CA as Subordinate CA of an External PKI

If you want the root CA on the primary PAN to act as a subordinate CA of an external PKI, generate an ISE intermediate CA certificate signing request, send it to the external CA, obtain the root and CA-signed certificates, import the root CA certificate in to the Trusted Certificates Store, and bind the CA-signed certificate to the CSR. In this case, the external CA is the root CA, the Primary PAN is a subordinate CA of the external CA, and the PSNs are subordinate CAs of the primary PAN.

Step 1 Choose **Administration** > **System** > **Certificates** > **Certificate Signing Requests**.

Step 2 Click **Generate Certificate Signing Requests (CSR)**.

Step 3 Choose ISE Intermediate CA from the **Certificate(s) will be used for** drop-down list.

Step 4 Click **Generate**.

Step 5 Export the CSR, send it to the external CA, and obtain the CA-signed certificate.

Step 6 Import the root CA certificate from the external CA in to the Trusted Certificates store.

Step 7 Bind the CA-signed certificate with the CSR.

What to do next

If you have a secondary PAN in the deployment, obtain a backup of the Cisco ISE CA certificates and keys from the primary PAN and restore it on the secondary PAN. Server and root certificates are then automatically replicated in the secondary PAN. This ensures that the secondary PAN can function as subordinate CA of the external PKI in case of administration node failover.

Configure Cisco ISE to Use Certificates for Authenticating Personal Devices

You can configure Cisco ISE to issue and manage certificates for endpoints (personal devices) that connect to your network. You can use the internal Cisco ISE CA service to sign the certificate signing request from endpoints or forward the CSR to an external CA.

Before you begin

- Obtain a backup of the Cisco ISE CA certificates and keys from the primary PAN and store them in a secure location for disaster recovery purposes.

Step 1 Add Users to Employee User Group, on page 345.

You can add users to the internal identity store or to an external identity store such as Microsoft Active Directory.

Step 2 Create a Certificate Authentication Profile for TLS-Based Authentication, on page 345 .

Step 3 Create an Identity Source Sequence for TLS-Based Authentication, on page 346.

Step 4 Create a client provisioning policy:

a) Configure Certificate Authority Settings, on page 346
b) Create a CA Template, on page 347
c) Create a Native Supplicant Profile to be Used in Client-Provisioning Policy, on page 349
d) Download Agent Resources from Cisco for Windows and MAC OS X Operating Systems, on page 350
e) Create Client-Provisioning Policy Rules for Apple iOS, Android, and MAC OS X Devices, on page 350

Step 5 Configure the Dot1X Authentication Policy Rule for TLS-Based Authentication, on page 351

Step 6 Configure authorization policy rules for TLS-based authentications.

a) Create Authorization Profiles for Central Web Authentication and Supplicant-Provisioning Flows, on page 352
b) Create Authorization Policy Rules, on page 352

When you use ECDHE-RSA based certificates, while connecting to the wireless SSID from your personal device, you will be prompted to enter the password a second time.

Add Users to Employee User Group

The following procedure describes how to add users to the Employee user group in the Cisco ISE identity store. If you are using an external identity store, make sure that you have an Employee user group to which you can add users.

Step 1 Choose **Administration** > **Identity Management** > **Identities** > **Users**.

Step 2 Click **Add**.

Step 3 Enter the user details.

Step 4 In the **Passwords** section, choose the **Login Password** and TACACS+ **Enable Password** to set the access level to a network device.

Step 5 Select Employee from the User Group drop-down list.

All users who belong to the Employee user group share the same set of privileges.

Step 6 Click **Submit**.

What to do next

Create a Certificate Authentication Profile for TLS-Based Authentication, on page 345

Create a Certificate Authentication Profile for TLS-Based Authentication

To use certificates for authenticating endpoints that connect to your network, you must define a certificate authentication profile in Cisco ISE or edit the default Preloaded_Certificate_Profile. The certificate authentication profile includes the certificate field that should be used as the principal username. For example, if the username is in the Common Name field, then you can define a certificate authentication profile with the Principal Username being the Subject - Common Name, which can be verified against the identity store.

Step 1 Choose **Administration** > **Identity Management** > **External Identity Sources** > **Certificate Authentication Profile**.

Step 2 Enter a name for your certificate authentication profile. For example, CAP.

Step 3 Choose Subject - Common Name as the **Principal Username X509 Attribute**.

Step 4 Click **Save**.

What to do next

Create an Identity Source Sequence for TLS-Based Authentication, on page 346

Create an Identity Source Sequence for TLS-Based Authentication

After you create a certificate authentication profile, you must add it to the identity source sequence so that Cisco ISE can obtain the attribute from the certificate and match it against the identity sources that you have defined in the identity source sequence.

Before you begin

Ensure that you have completed the following tasks:

- Add users to the Employee user group.
- Create a certificate authentication profile for certificate-based authentication.

Step 1 Choose **Administration** > **Identity Management** > **Identity Source Sequences**.

Step 2 Click **Add**.

Step 3 Enter a name for the identity source sequence. For example, Dot1X.

Step 4 Check the **Select Certificate Authentication Profile** check box and select the certificate authentication profile that you created earlier, namely CAP.

Step 5 Move the identity source that contains your user information to the **Selected** list box in the Authentication Search List area.

You can add additional identity sources and Cisco ISE searches these data stores sequentially until a match is found.

Step 6 Click the **Treat as if the user was not found and proceed to the next store in the sequence** radio button.

Step 7 Click **Submit**.

What to do next

Configure Certificate Authority Settings, on page 346

Configure Certificate Authority Settings

You must configure the external CA settings if you are going to use an external CA for signing the CSRs. The external CA settings was known as the SCEP RA profile in previous releases of Cisco ISE. If you are using the Cisco ISE CA, then you do not have to explicitly configure the CA settings. You can review the Internal CA settings at Administration > System > Certificates > Internal CA Settings.

Once users' devices receive their validated certificate, they reside on the device as described in the following table.

Table 36: Device Certificate Location

Device	Certificate Storage Location	Access Method
iPhone/iPad	Standard certificate store	Settings > General > Profile
Android	Encrypted certificate store	Invisible to end users. **Note** Certificates can be removed using Settings > Location & Security > Clear Storage.

Device	Certificate Storage Location	Access Method
Windows	Standard certificate store	Launch mmc.exe from the **/cmd** prompt or view in the certificate snap-in.
Mac	Standard certificate store	Application > Utilities > Keychain Access

Before you begin

If you are going to use an external Certificate Authority (CA) for signing the certificate signing request (CSR), then you must have the URL of the external CA.

Step 1 Choose **Administration** > **System** > **Certificates** > **External CA Settings**.

Step 2 Click **Add**.

Step 3 Enter a name for the external CA setting. For example, EXTERNAL_SCEP.

Step 4 Enter the external CA server URL in the URL text box.

Click **Test Connection** to check if the external CA is reachable. Click the + button to enter additional CA server URLs.

Step 5 Click **Submit**.

What to do next

Create a CA Template, on page 347

Create a CA Template

The certificate template defines the SCEP RA profile that must be used (for the internal or external CA), Key Type, Key Size or Curve Type, Subject, Subject Alternative Name (SAN), validity period of the certificate, and the Extended Key Usage. This example assumes that you are going to use the internal Cisco ISE CA. For an external CA template, the validity period is determined by the external CA and you cannot specify it.

You can create a new CA template or edit the default certificate template, EAP_Authentication_Certificate_Template.

By default, the following CA templates are available in Cisco ISE:

- CA_SERVICE_Certificate_Template—For other network services that use the ISE CA. For example, use this certificate template while configuring ISE to issue certificates for ASA VPN users.
- EAP_Authentication_Certificate_Template—For EAP authentication.
- pxGrid_Certificate_Template—For pxGrid controller while generating the certificate from the Certificate Provisioning Portal.

Note Certificate templates that use the ECC key type can be used only with the internal Cisco ISE CA.

Before you begin

Ensure that you have configured the CA settings.

Step 1 Choose **Administration** > **System** > **CA Service** > **Internal CA Certificate Template**.

Step 2 Enter a name for the internal CA template. For example, Internal_CA_Template.

Step 3 (Optional) Enter values for the Organizational Unit, Organization, City, State, and Country fields.

We do not support UTF-8 characters in the certificate template fields (Organizational Unit, Organization, City, State, and Country). Certificate provisioning fails if UTF-8 characters are used in the certificate template.

The username of the internal user generating the certificate is used as the Common Name of the certificate. Cisco ISE Internal CA does not support "+" or "*" characters in the Common Name field. Ensure that your username does not include "+" or "*" special characters.

Step 4 Specify the Subject Alternative Name (SAN) and the validity period of the certificate.

Step 5 Specify a Key Type. Choose RSA or ECC.

The following table lists the operating systems and versions that support ECC along with the curve types that are supported. If your devices are not running a supported operating system or on a supported version, you can use RSA-based certificates instead.

Operating System	Supported Versions	Supported Curve Types
Windows	8 and later	P-256, P-384, and P-521
Android	4.4 and later **Note** Android 6.0 requires May 2016 patch to support ECC certificates.	All curve types (except Android 6.0, which does not support the P-192 curve type).

Windows 7 and Apple iOS do not natively support ECC for EAP-TLS authentication. This release of Cisco ISE does not support the use of ECC certificates on MAC OS X devices.

If the devices in your network run an operating system that is not supported (Windows 7, MAC OS X, or Apple iOS, we recommend that you choose RSA as the Key Type.

Step 6 (Applicable if you choose the RSA Key Type) Specify a key size. You must choose 1024 or a higher key size.

Step 7 (Applicable only if you choose the ECC Key Type) Specify the Curve Type. The default is P-384.

Step 8 Choose ISE Internal CA as the SCEP RA Profile.

Step 9 Enter the validity period in days. The default is 730 days. Valid range is between 1 and 730.

Step 10 Specify the Extended Key Usage. Check the **Client Authentication** check box if you want the certificate to be used for client authentication. Check the **Server Authentication** check box if you want the certificate to be used for server authentication.

Step 11 Click **Submit**.

The internal CA certificate template is created and will be used by the client provisioning policy.

What to do next

Create a Native Supplicant Profile to be Used in Client-Provisioning Policy, on page 349

Internal CA Settings

The following table describes the fields in the internal CA Settings window. You can view the internal CA settings and disable the internal CA service from this window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Certificate Authority** > **Internal CA Settings**.

Table 37: Internal CA Settings

Field Name	Usage Guidelines
Disable Certificate Authority	Click this button to disable the internal CA service.
Host Name	Host name of the Cisco ISE node that is running the CA service.
Personas	Cisco ISE node personas that are enabled on the node running the CA service. For example, Administration, Policy Service, etc.
Role(s)	The role(s) assumed by the Cisco ISE node running the CA service. For example, Standalone or Primary or Secondary.
CA, EST & OCSP Responder Status	Enabled or disabled
OCSP Responder URL	URL for Cisco ISE node to access the OCSP server.
SCEP URL	URL for the Cisco ISE node to access the SCEP server.

Related Topics

Cisco ISE CA Service, on page 328
Configure Cisco ISE to Use Certificates for Authenticating Personal Devices, on page 344

Create a Native Supplicant Profile to be Used in Client-Provisioning Policy

You can create native supplicant profiles to enable users to bring personal devices to your Corporate network. Cisco ISE uses different policy rules for different operating systems. Each client provisioning policy rule contains a native supplicant profile, which specifies which provisioning wizard is to be used for which operating system.

Before you begin

- Configure the CA certificate template in Cisco ISE.
- Open up TCP port 8905 and UDP port 8905 to enable client agents and supplicant provisioning wizard installation. For more information about port usage, see the "Cisco ISE Appliance Ports Reference" appendix in the *Cisco Identity Services Engine Hardware Installation Guide*.

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Step 2 Choose **Add** > **Native Supplicant Profile**.

Step 3 Enter a name for the native supplicant profile. For example, EAP_TLS_INTERNAL.

Step 4 Choose ALL from the **Operating System** drop-down list.

Note The MAC OS version 10.10 user should manually connect to the provisioned SSID for dual-SSID PEAP flow.

Step 5 Check the **Wired** or **Wireless** check box.

Step 6 Choose TLS from the **Allowed Protocol** drop-down list.

Step 7 Choose the CA certificate template that you created earlier.

Step 8 Click **Submit**.

What to do next

Download Agent Resources from Cisco for Windows and MAC OS X Operating Systems, on page 350

Download Agent Resources from Cisco for Windows and MAC OS X Operating Systems

For Windows and MAC OS X operating systems, you must download the remote resources from the Cisco site.

Before you begin

Ensure that you are able to access the appropriate remote location to download client provisioning resources to Cisco ISE, by verifying that the proxy settings for your network are correctly configured.

Step 1 Choose **Policy** > **Policy Elements** > **Resources** > **Client Provisioning** > **Resources**.

Step 2 Choose **Add** > **Agent resources from Cisco site**.

Step 3 Check the check boxes next to the **Windows** and **MAC OS X** packages. Be sure to include the latest versions.

Step 4 Click **Save**.

What to do next

Create Client-Provisioning Policy Rules for Apple iOS, Android, and MAC OS X Devices, on page 350

Create Client-Provisioning Policy Rules for Apple iOS, Android, and MAC OS X Devices

Client provisioning resource policies determine which users receive which version (or versions) of resources (agents, agent compliance modules, and agent customization packages/profiles) from Cisco ISE upon login and user session initiation.

When you download the agent compliance module, it always overwrites the existing one, if any, available in the system.

To enable employees to bring iOS, Android, MAC OS X devices, you must create policy rules for each of these devices on the Client Provisioning Policy page.

Before you begin

You must have configured the required native supplicant profiles and downloaded the required agents from the Client Provisioning Policy pages.

Step 1 Choose **Policy** > **Client Provisioning**.

Step 2 Create client provisioning policy rules for Apple iOS, Android, and MAC OS X devices.

Step 3 Click **Save**.

What to do next

Configure the Dot1X Authentication Policy Rule for TLS-Based Authentication, on page 351

Configure the Dot1X Authentication Policy Rule for TLS-Based Authentication

This task shows how to update the Dot1X authentication policy rule for TLS-based authentications.

Before you begin

Ensure that you have the certificate authentication profile created for TLS-based authentication.

Step 1 Choose **Policy** > **Policy Sets**.

Step 2 Click the arrow icon › from the **View** column to open the Set view screen and view, manage, and update the authentication policy.

The default rule-based authentication policy includes a rule for Dot1X authentication.

Step 3 To edit the conditions for the Dot1X authentication policy rule, hover over the cell in the **Conditions** column and click ✎. The Conditions Studio opens.

Step 4 From the **Actions** column in the Dot1X policy rule, click the cog icon and then from the drop-down menu, insert a new policy set by selecting any of the insert or duplicate options, as necessary.
A new row appears in the Policy Sets table.

Step 5 Enter a name for the rule. For example, eap-tls.

Step 6 From the **Conditions** column, click the (+) symbol.

Step 7 Create the required conditions in the **Conditions Studio Page**. In the **Editor** section, click the **Click To Add an Attribute** text box, and select the required Dictionary and Attribute (for example, Network Access:UserName Equals User1).

You can drag and drop a Library condition to the **Click To Add An Attribute** text box.

Step 8 Click **Use**.

Step 9 Leave the default rule as is.

Step 10 Click **Save**.

What to do next

Create Authorization Profiles for Central Web Authentication and Supplicant-Provisioning Flows, on page 352

Create Authorization Profiles for Central Web Authentication and Supplicant-Provisioning Flows

You must define authorization profiles to determine the access that must be granted to the user after the certificate-based authentication is successful.

Before you begin

Ensure that you have configured the required access control lists (ACLs) on the wireless LAN controller (WLC). Refer to the *TrustSec How-To Guide: Using Certificates for Differentiated Access* for information on how to create the ACLs on the WLC.

This example assumes that you have created the following ACLs on the WLC.

- NSP-ACL - For native supplicant provisioning
- BLACKHOLE - For restricting access to block listed devices
- NSP-ACL-Google - For provisioning Android devices

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.

Step 2 Click **Add** to create a new authorization profile.

Step 3 Enter a name for the authorization profile.

Step 4 From the **Access Type** drop-down list, choose ACCESS_ACCEPT.

Step 5 Click **Add** to add the authorization profiles for central web authentication, central web authentication for Google Play, native supplicant provisioning, and native supplicant provisioning for Google.

Step 6 Click **Save**.

What to do next

Create Authorization Policy Rules, on page 352

Create Authorization Policy Rules

Cisco ISE evaluates the authorization policy rules and grants the user access to the network resources based on the authorization profile specified in the policy rule.

Before you begin

Ensure that you have created the required authorization profiles.

Step 1 Choose **Policy** > **Policy Sets**, and expand the policy set to view the authorization policy rules.

Step 2 Insert additional policy rules above the default rule.

Step 3 Click **Save**.

CA Service Policy Reference

This section provides reference information for the authorization and client provisioning policy rules that you must create before you can enable the Cisco ISE CA service.

Client-Provisioning Policy Rules for Certificate Services

This section lists the client provisioning policy rules that you must create while using the Cisco ISE certificate services. The following table provides the details.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
iOS	Any	Apple iOS All	Condition(s)	EAP_TLS_INTERNAL (the native supplicant profile that you created earlier). If you are using an external CA, select the native supplicant profile that you have created for the external CA.
Android	Any	Android	Condition(s)	EAP_TLS_INTERNAL (the native supplicant profile that you created earlier). If you are using an external CA, select the native supplicant profile that you have created for the external CA.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
MAC OS X	Any	MACOSX	Condition(s)	Under the Native Supplicant Configuration, specify the following: **1.** Config Wizard: Select the MAC OS X supplicant wizard that you downloaded from the Cisco site. **2.** Wizard Profile: Choose the EAP_TLS_INTERNAL native supplicant profile that you created earlier. If you are using an external CA, select the native supplicant profile that you have created for the external CA.

Authorization Profiles for Certificate Services

This section lists the authorization profiles that you must create for enabling certificate-based authentication in Cisco ISE. You must have already created the ACLs (NSP-ACL and NSP-ACL-Google) on the wireless LAN controller (WLC).

- CWA - This profile is for devices that go through the central web authentication flow. Check the **Web Authentication** check box, choose Centralized from the drop-down list, and enter NSP-ACL in the ACL text box.
- CWA_GooglePlay - This profile is for Android devices that go through the central web authentication flow. This profile enables Android devices to access Google Play Store and download the Cisco Network Setup Assistant. Check the **Web Authentication** check box, choose Centralized from the drop-down list, and enter NSP-ACL-Google in the ACL text box.
- NSP - This profile is for non-Android devices that go through the supplicant provisioning flow. Check the **Web Authentication** check box, choose Supplicant Provisioning from the drop-down list, and enter NSP-ACL in the ACL text box.
- NSP-Google - This profile is for Android devices that go through the supplicant provisioning flow. Check the **Web Authentication** check box, choose Supplicant Provisioning from the drop-down list, and enter NSP-ACL-Google in the ACL text box.

Review the default Blackhole_Wireless_Access authorization profile. The Advanced Attributes Settings should be:

- Cisco:cisco-av-pair = url-redirect=https://*ip:port*/blockedportal/gateway?portal=*PortalID*
- Cisco:cisco-av-pair = url-redirect-acl=BLACKHOLE

Authorization Policy Rules for Certificate Services

This section lists the authorization policy rules that you must create while enabling the Cisco ISE CA service.

- Corporate Assets-This rule is for corporate devices that connect to the corporate wireless SSID using 802.1X and MSCHAPV2 protocol.
- Android_SingleSSID-This rule is for Android devices that access the Google Play Store to download the Cisco Network Setup Assistant for provisioning. This rule is specific to single SSID setup.
- Android_DualSSID-This rule is for Android devices that access the Google Play Store to download the Cisco Network Setup Assistant for provisioning. This rule is specific to dual SSID setup.
- CWA-This rule is for devices that go through the central web authentication flow.
- NSP-This rule is for devices that go through the native supplicant provisioning flow using a certificate for EAP-TLS authentication.
- EAP-TLS-This rule is for devices that have completed the supplicant provisioning flow and are provisioned with a certificate. They will be given access to the network.

The following table lists the attributes and values that you must choose while configuring authorization policy rules for the Cisco ISE CA service. This example assumes that you have the corresponding authorization profiles configured in Cisco ISE as well.

Rule Name	**Conditions**	**Permissions (Authorization Profiles to be Applied)**
Corporate Assets	Corp_Assets AND (Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	PermitAccess
Android_SingleSSID	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND Session:Device-OS EQUALS Android)	NSP_Google
Android_DualSSID	(Wireless_MAB AND Session:Device-OS EQUALS Android)	CWA_GooglePlay
CWA	Wireless_MAB	CWA
NSP	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	NSP
EAP-TLS	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS x509_PKI	PermitAccess

Cisco ISE CA Issues Certificates to ASA VPN Users

ISE CA issues certificates to client machines connecting over ASA VPN. Using this feature, you can automatically provision certificates to end devices that connect over ASA VPN.

Cisco ISE uses the Simple Certificate Enrollment Protocol (SCEP) for enrollment and to provision certificates to the client machines. The AnyConnect client sends the SCEP request to the ASA over an HTTPS connection. The ASA evaluates the request and enforces policies before it relays the request to Cisco ISE over an HTTP connection established between Cisco ISE and ASA. The response from the Cisco ISE CA is relayed back to the client. The ASA cannot read the contents of the SCEP message and functions as a proxy for the Cisco ISE CA. The Cisco ISE CA decrypts the SCEP message from the client and sends the response in an encrypted form.

The ISE CA SCEP URL is http://<*IP Address or FQDN of ISE CA server*>:9090/auth/caservice/pkiclient.exe. If you are using FQDN of the ISE node, the DNS server connected to ASA must be able to resolve the FQDN.

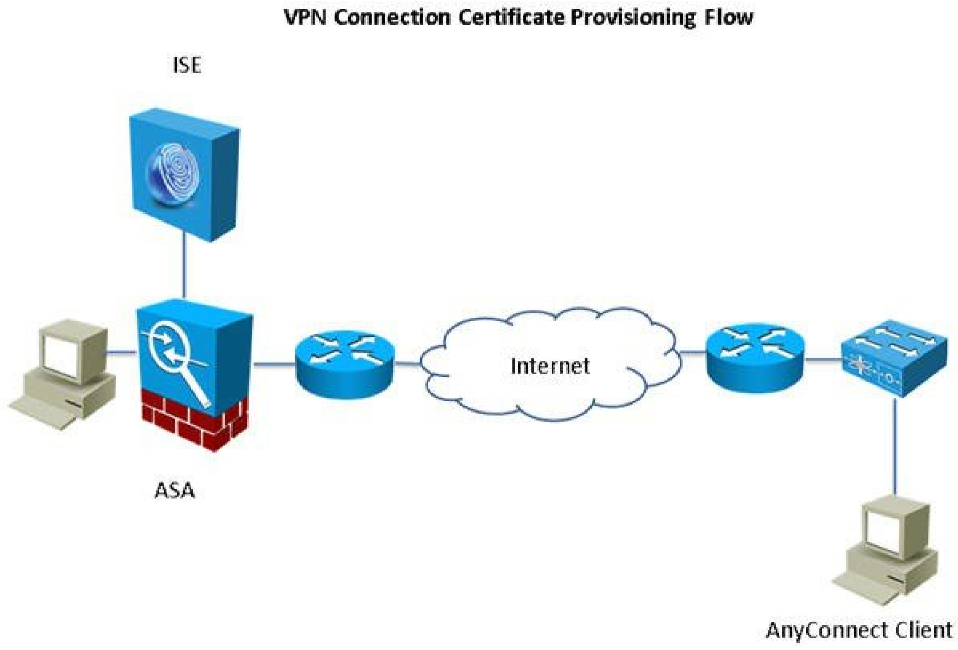
You can configure certificate renewal before expiration in the AnyConnect client profile. If the certificate has already expired, the renewal flow is similar to a new enrollment.

Supported versions include:

- Cisco ASA 5500 Series Adaptive Security Appliances that run software version 8.x
- Cisco AnyConnect VPN version 2.4 or later

VPN Connection Certificate-Provisioning Flow

Figure 10: Certificate Provisioning for ASA VPN Users



1. The user initiates a VPN connection.

2. The AnyConnect client scans the client machine and sends the attributes such as the unique device identifier (for example, IMEI) to the ASA.
3. The ASA requests certificate-based authentication from the client. The authentication fails because there is no certificate.
4. The ASA proceeds to primary user authentication (AAA) using the username/password and passes the information to the authentication server (ISE).
   a. If authentication fails, the connection is terminated immediately.
   b. If authentication passes, limited access is granted. You can configure dynamic access policies (DAP) for client machines that request a certificate using the aaa.cisco.sceprequired attribute. You can set the value for this attribute to "true" and apply ACLs and web ACLs.
5. The VPN connection is established after the relevant policies and ACLs are applied. The client starts key generation for SCEP only after AAA authentication succeeds and the VPN connection is established.
6. The client starts the SCEP enrollment and sends SCEP requests to ASA over HTTP.
7. ASA looks up the session information of the request and relays the request to ISE CA, if the session is allowed for enrollment.
8. ASA relays the response from ISE CA back to the client.
9. If enrollment succeeds, the client presents a configurable message to the user and disconnects the VPN session.
10. The user can again authenticate using the certificate and a normal VPN connection is established.

Configure Cisco ISE CA to Issue Certificates to ASA VPN Users

You must perform the following configurations on Cisco ISE and ASA to provision certificates to ASA VPN users.

Before you begin

- Ensure that the VPN user account is present in Cisco ISE internal or external identity source.
- Ensure that the ASA and the Cisco ISE Policy Service Nodes are synchronized using the same NTP server.

Step 1 Define the ASA as a network access device in Cisco ISE. See Add a Network Device in Cisco ISE, on page 358 for information on how to add ASA as a network device.

Step 2 Configure Group Policy in ASA, on page 358.

Step 3 Configure AnyConnect Connection Profile for SCEP Enrollment, on page 358.

Step 4 Configure a VPN Client Profile in ASDM, on page 359.

Step 5 Import Cisco ISE CA Certificates into ASA.

Add a Network Device in Cisco ISE

You can add a network device in Cisco ISE or use the default network device.

You can also add a network device in the **Network Devices** (**Work Centers** > **Device Administration** > **Network Resources** > **Network Devices**) window.

Before you begin

The AAA function must be enabled on the network device to be added. See Command to Enable AAA Functions, on page 1332.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Devices**.

Step 2 Click **Add**.

Step 3 Enter the corresponding values in the **Name**, **Description**, and **IP Address** fields.

Step 4 Choose the required values from the **Device Profile**, **Model Name**, **Software Version**, and **Network Device Group** drop-down lists.

Step 5 (Optional) Check the **RADIUS Authentication Settings** check box to configure the RADIUS protocol for authentication.

Step 6 (Optional) Check the **TACACS Authentication Settings** check box to configure the TACACS protocol for authentication.

Step 7 (Optional) Check the **SNMP Settings** check box to configure SNMP for the Cisco ISE profiling service to collect information from the network device.

Step 8 (Optional) Check the **Advanced Trustsec Settings** check box to configure a Cisco TrustSec-enabled device.

Step 9 Click **Submit**.

Configure Group Policy in ASA

Configure a group policy in ASA to define the ISE CA URL for AnyConnect to forward the SCEP enrollment request.

Step 1 Log in to Cisco ASA ASDM.

Step 2 From the Remote Access VPN navigation pane on the left, click **Group Policies**.

Step 3 Click **Add** to create a group policy.

Step 4 Enter a name for the group policy. For example, ISE_CA_SCEP.

Step 5 In the SCEP forwarding URL field, uncheck the **Inherit** check box and enter the ISE SCEP URL with port number.

If you are using the FQDN of the ISE node, the DNS server connected to ASA must be able to resolve the FQDN of the ISE node.

Example:

http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe.

Step 6 Click **OK** to save the group policy.

Configure AnyConnect Connection Profile for SCEP Enrollment

Configure an AnyConnect connection profile in ASA to specify the ISE CA server, authentication method, and ISE CA SCEP URL.

Step 1 Log in to Cisco ASA ASDM.

Step 2 From the Remote Access VPN navigation pane on the left, click **AnyConnect Connection Profiles**.

Step 3 Click **Add** to create a connection profile.

Step 4 Enter a name for the connection profile. For example, Cert-Group.

Step 5 (Optional) Enter a description for the connection profile in the Aliases field. For example, SCEP-Call-ASA.

Step 6 In the Authentication area, specify the following:

- Method—Click the **Both** radio button
- AAA Server Group—Click **Manage** and choose your ISE server

Step 7 In the Client Address Assignment area, select the DHCP server and client address pools to use.

Step 8 In the Default Group Policy area, click **Manage** and select the Group Policy that you have created with the ISE SCEP URL and port number.

Example:

For example, ISE_CA_SCEP.

Step 9 Choose **Advanced** > **General** and check the **Enable Simple Certificate Enrollment Protocol** check box for this connection profile.

Step 10 Click **OK**.
Your AnyConnect connection profile is created.

Configure a VPN Client Profile in ASDM

Configure a VPN client profile in AnyConnect for SCEP enrollment.

Step 1 Log in to Cisco ASA ASDM.

Step 2 From the Remote Access VPN navigation pane on the left, click **AnyConnect Client Profile**.

Step 3 Select the client profile that you want to use and click **Edit**.

Step 4 Click **Certificate Enrollment** from the Profile navigation pane on the left.

Step 5 Check the **Certificate Enrollment** check box.

Step 6 Enter the values in the following fields:

- Certificate Expiration Threshold—The number of days before the certificate expiration date that AnyConnect warns users their certificate is going to expire (not supported when SCEP is enabled). The default is zero (no warning displayed). The range of values is zero to 180 days.
- Automatic SCEP Host—Enter the host name and connection profile (tunnel group) of the ASA that has SCEP certificate retrieval configured. Enter a Fully Qualified Domain Name (FQDN) or a connection profile name of the ASA. For example, the hostname asa.cisco.com and the connection profile name Cert_Group.
- CA URL—Identifies the SCEP CA server. Enter the FQDN or IP Address of the ISE server. For example, http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe.

Step 7 Enter values for the Certificate Contents that define how the client requests the contents of the certificate.

Step 8 Click **OK**.

The AnyConnect client profile is created. Refer to the Cisco AnyConnect Secure Mobility Client for your version of AnyConnect for additional information.

Import Cisco ISE CA Certificates into ASA

Import the Cisco ISE internal CA certificates into the ASA.

Before you begin

Export the Cisco ISE internal CA certificates. Go to **Administration** > **System** > **Certificates** > **Certificate Authority** > **Certificate Authority Certificates**. Check the check boxes next to **Certificate Services Node CA** and **Certificate Services Root CA** certificates and export them, one certificate at a time.

Step 1 Log in to Cisco ASA ASDM.

Step 2 From the Remote Access VPN navigation pane on the left, choose **Certificate Management** > **CA Certificates**.

Step 3 Click **Add** and select the Cisco ISE internal CA certificates to import them in to ASA.

Revoke an Endpoint Certificate

If you need to revoke a certificate issued to an employee's personal device, you can revoke it from the Endpoint Certificates page. For example, if an employee's device has been stolen or lost, you can log in to the Cisco ISE Admin portal and revoke the certificate issued to that device from the Endpoint Certificates page. You can filter the data on this page based on the Friendly Name, Device Unique Id, or Serial Number.

If a PSN (sub CA) is compromised, you can revoke all certificates issued by that PSN by filtering on the Issued By field from the Endpoint Certificates page.

When you revoke a certificate issued to an employee, if there is an active session (authenticated using that certificate), the session is terminated immediately. Revoking a certificate ensures that unauthorized users do not have any access to resources as soon as the certificate is revoked.

Step 1 Choose **Administration** > **System** > **Certificates** > **Certificate Authority** > **Issued Certificates**.

Step 2 Check the check box next to the endpoint certificate that you want to revoke and click **Revoke**.

You can search for the certificate based on the Friendly Name and Device Type.

Step 3 Enter the reason for revoking the certificate.

Step 4 Click **Yes**.

OCSP Services

The Online Certificate Status Protocol (OCSP) is a protocol that is used for checking the status of x.509 digital certificates. This protocol is an alternative to the Certificate Revocation List (CRL) and addresses issues that result in handling CRLs.

Cisco ISE has the capability to communicate with OCSP servers over HTTP to validate the status of certificates in authentications. The OCSP configuration is configured in a reusable configuration object that can be referenced from any certificate authority (CA) certificate that is configured in Cisco ISE.

You can configure CRL and/or OCSP verification per CA. If both are selected, then Cisco ISE first performs verification over OCSP. If a communication problem is detected with both the primary and secondary OCSP servers, or if an unknown status is returned for a given certificate, Cisco ISE switches to checking the CRL.

Cisco ISE CA Service Online Certificate Status Protocol Responder

The Cisco ISE CA OCSP responder is a server that communicates with OCSP clients. The OCSP clients for the Cisco ISE CA include the internal Cisco ISE OCSP client and OCSP clients on the Adaptive Security Appliance (ASA). The OCSP clients should communicate with the OCSP responder using the OCSP request/response structure defined in RFC 2560, 5019.

The Cisco ISE CA issues a certificate to the OCSP responder. The OCSP responder listens on port 2560 for any incoming requests. This port is configured to allow only OCSP traffic.

The OCSP responder accepts a request that follows the structure defined in RFC 2560, 5019. Nonce extension is supported in the OCSP request. The OCSP responder obtains the status of the certificate and creates an OCSP response and signs it. The OCSP response is not cached on the OCSP responder, although you can cache the OCSP response on the client for a maximum period of 24 hours. The OCSP client should validate the signature in the OCSP response.

The self-signed CA certificate (or the intermediate CA certificate if ISE acts as an intermediate CA of an external CA) on the PAN issues the OCSP responder certificate. This CA certificate on the PAN issues the OCSP certificates on the PAN and PSNs. This self-signed CA certificate is also the root certificate for the entire deployment. All the OCSP certificates across the deployment are placed in the Trusted Certificates Store for ISE to validate any response signed using these certificates.

Note Cisco ISE receives from OCSP responder servers a thisUpdate value, which indicates the time since the last certificate revocation. If the thisUpdate value is greater than 7 days, the OCSP certificate verification fails in Cisco ISE.

OCSP Certificate Status Values

OCSP services return the following values for a given certificate request:

- Good—Indicates a positive response to the status inquiry. It means that the certificate is not revoked, and the state is good only until the next time interval (time to live) value.
- Revoked—The certificate was revoked.
- Unknown—The certificate status is unknown. OCSP service returns this value if the certificate was not issued by the CA of this OCSP responder.
- Error—No response was received for the OCSP request.

Update of OCSP Responder Certificates

Cisco ISE Release 3.1 Cumulative Patch 3 and above has a change in hierarchy of the internal CA in Cisco ISE. This requires a one-time update of the OCSP responder certificates in Cisco ISE.

From Cisco ISE Release 3.1 Cumulative Patch 3 onwards, the following rules are applicable for the update of OCSP responder certificates:

- When updating to Cisco ISE Release 3.1 Cumulative Patch 3 and later patches from Cisco ISE Release 3.1 Cumulative Patch 2 or earlier patches:
  - For a multi-node Cisco ISE deployment, OCSP certificates are renewed automatically if you install the patch through the Cisco ISE GUI. If you install the patch through the Cisco ISE CLI, we recommend you to renew the OCSP certificate manually.
  - For a standalone Cisco ISE deployment, OCSP certificates are renewed automatically irrespective of whether you install the patch through the Cisco ISE GUI or the Cisco ISE CLI.
  - If you uninstall Patch 3 or later patches, you have to renew the OCSP certificate manually.
- A full upgrade from an earlier Cisco ISE Release to Cisco ISE 3.2 and later releases will renew the OCSP responder certificates.
- A split upgrade (both legacy upgrade and new upgrade) will regenerate the Cisco ISE internal root CA.
- Restoring a backup will regenerate the Cisco ISE internal root CA.

OCSP High Availability

Cisco ISE has the capability to configure up to two OCSP servers per CA, and they are called primary and secondary OCSP servers. Each OCSP server configuration contains the following parameters:

- URL—The OCSP server URL.
- Nonce—A random number that is sent in the request. This option ensures that old communications cannot be reused in replay attacks.
- Validate response—Cisco ISE validates the response signature that is received from the OCSP server.

In case of timeout (which is 5 seconds), when Cisco ISE communicates with the primary OCSP server, it switches to the secondary OCSP server.

Cisco ISE uses the secondary OCSP server for a configurable amount of time before attempting to use the primary server again.

OCSP Failures

The three general OCSP failure scenarios are as follows:

- Failed OCSP cache or OCSP client side (Cisco ISE) failures.
- Failed OCSP responder scenarios, for example:

  The first primary OCSP responder not responding, and the secondary OCSP responder responding to the Cisco ISE OCSP request.

Errors or responses not received from Cisco ISE OCSP requests.

An OCSP responder may not provide a response to the Cisco ISE OCSP request or it may return an OCSP Response Status as not successful. OCSP Response Status values can be as follows:

- tryLater
- signRequired
- unauthorized
- internalError
- malformedRequest

  There are many date-time checks, signature validity checks and so on, in the OCSP request. For more details, refer to *RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP* which describes all the possible states, including the error states.

- Failed OCSP reports

Add OCSP Client Profiles

You can use the OCSP Client Profile page to add new OCSP client profiles to Cisco ISE.

Before you begin

If the Certificate Authority (CA) is running the OCSP service on a nonstandard port (other than 80 or 443), you must configure ACLs on the switch to allow for communication between Cisco ISE and the CA on that port. For example:

permit tcp *<source ip> <destination ip>* **eq** *<OCSP port number>*

Step 1 Choose **Administration** > **System** > **Certificates** > **Certificate Management** > **OCSP Client Profile**.

Step 2 Enter the values to add an OCSP Client Profile.

Step 3 Click **Submit**.

OCSP Client Profile Settings

The following table describes the fields on the OCSP Client Profile window, which you can use to configure OCSP client profiles. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Certificates** > **Certificate Management** > **OCSP Client Profile**.

Table 38: OCSP Client Profile Settings

Field Name	Usage Guidelines
Name	Name of the OCSP Client Profile.
Description	Enter an optional description.

Field Name	Usage Guidelines
Configure OCSP Responder	
Enable Secondary Server	Check this check box to enable a secondary OCSP server for high availability.
Always Access Primary Server First	Use this option to check the primary server before trying to move to the secondary server. Even if the primary was checked earlier and found to be unresponsive, Cisco ISE will try to send a request to the primary server before moving to the secondary server.
Fallback to Primary Server After Interval *n* Minutes	Use this option when you want Cisco ISE to move to the secondary server and then fall back to the primary server again. In this case, all other requests are skipped, and the secondary server is used for the amount of time that is configured in the text box. The allowed time range is 1 to 999 minutes.
Primary and Secondary Servers	
URL	Enter the URL of the primary and/or secondary OCSP server.
Enable Nonce Extension Support	You can configure a nonce to be sent as part of the OCSP request. The Nonce includes a pseudo-random number in the OCSP request. It is verified that the number that is received in the response is the same as the number that is included in the request. This option ensures that old communications cannot be reused in replay attacks.
Validate Response Signature	The OCSP responder signs the response with one of the following certificates: • The CA certificate • A certificate different from the CA certificate In order for Cisco ISE to validate the response signature, the OCSP responder needs to send the response along with the certificate, otherwise the response verification fails, and the status of the certificate cannot be relied on. According to the RFC, OCSP can sign the response using different certificates. This is true as long as OCSP sends the certificate that signed the response for Cisco ISE to validate it. If OCSP signs the response with a different certificate that is not configured in Cisco ISE, the response verification will fail.

Field Name	Usage Guidelines
Use OCSP URLs specified in Authority Information Access (AIA)	Click the radio button to use the OCSP URLs specified in the Authority Information Access extension.
Response Cache	
Cache Entry Time To Live *n* Minutes	Enter the time in minutes after which the cache entry expires. Each response from the OCSP server holds a nextUpdate value. This value shows when the status of the certificate will be updated next on the server. When the OCSP response is cached, the two values (one from the configuration and another from response) are compared, and the response is cached for the period of time that is the lowest value of these two. If the nextUpdate value is 0, the response is not cached at all. Cisco ISE will cache OCSP responses for the configured time. The cache is not replicated or persistent, so when Cisco ISE restarts, the cache is cleared. The OCSP cache is used in order to maintain the OCSP responses and for the following reasons: • To reduce network traffic and load from the OCSP servers on an already-known certificate • To increase the performance of Cisco ISE by caching already-known certificate statuses By default, the cache is set to 2 minutes for the internal CA OCSP client profile. If an endpoint authenticates a second time within 2 minutes of the first authentication, the OCSP cache is used and the OCSP responder is not queried. If the endpoint certificate has been revoked within the cache period, the previous OCSP status of Good will be used and the authentication succeeds. Setting the cache to 0 minutes prevents any responses from being cached. This option improves security, but decreases authentication performance.
Clear Cache	Click **Clear Cache** to clear entries of all the certificate authorities that are connected to the OCSP service. In a deployment, **Clear Cache** interacts with all the nodes and performs the operation. This mechanism updates every node in the deployment.

Related Topics

OCSP Services, on page 360
Cisco ISE CA Service Online Certificate Status Protocol Responder, on page 361
OCSP Certificate Status Values, on page 361
OCSP High Availability, on page 362

OCSP Failures, on page 362
OCSP Statistics Counters, on page 366
Add OCSP Client Profiles, on page 363

OCSP Statistics Counters

Cisco ISE uses OCSP counters to log and monitor the data and health of the OCSP servers. Logging occurs every five minutes. Cisco ISE sends a syslog message to the Monitoring node and it is preserved in the local store. The local store contains data from the previous five minutes. After Cisco ISE sends the syslog message, the counters are recalculated for the next interval. This means, after five minutes, a new five-minute window interval starts again.

The following table lists the OCSP syslog messages and their descriptions.

Table 39: OCSP Syslog Messages

Message	Description
OCSPPrimaryNotResponsiveCount	The number of nonresponsive primary requests
OCSPSecondaryNotResponsiveCount	The number of nonresponsive secondary requests
OCSPPrimaryCertsGoodCount	The number of 'good' certificates that are returned for a given CA using the primary OCSP server
OCSPSecondaryCertsGoodCount	The number of 'good' statuses that are returned for a given CA using the primary OCSP server
OCSPPrimaryCertsRevokedCount	The number of 'revoked' statuses that are returned for a given CA using the primary OCSP server
OCSPSecondaryCertsRevokedCount	The number of 'revoked' statuses that are returned for a given CA using the secondary OCSP server
OCSPPrimaryCertsUnknownCount	The number of 'Unknown' statuses that are returned for a given CA using the primary OCSP server
OCSPSecondaryCertsUnknownCount	The number of 'Unknown' statuses that are returned for a given CA using the secondary OCSP server
OCSPPrimaryCertsFoundCount	The number of certificates that were found in cache from a primary origin
OCSPSecondaryCertsFoundCount	The number of certificates that were found in cache from a secondary origin
ClearCacheInvokedCount	How many times clear cache was triggered since the interval
OCSPCertsCleanedUpCount	How many cached entries were cleaned since the t interval
NumOfCertsFoundInCache	Number of the fulfilled requests from the cache
OCSPCacheCertsCount	Number of certificates that were found in the OCSP cache

Configure Admin Access Policies

An RBAC policy is represented in an if-then format, where "if" is the RBAC Admin Group value and "then" is the RBAC Permissions value.

The RBAC policies window (click the **Menu** icon (≡) and choose **Administration** > **System** > **Admin Access** > **Authorization** > **RBAC Policy**) contains a list of default policies. You cannot edit or delete these default policies. However, you can edit the data access permissions for the Read-Only Admin policy. The RBAC policies page also allows you to create custom RBAC policies for an admin group specifically for your work place, and apply to personalized admin groups.

When you assign limited menu access, make sure that the data access permissions allow the administrator to access the data that is required to use the specified menus. For example, if you give menu access to the MyDevices portal, but don't allow data access to Endpoint Identity Groups, then that administrator cannot modify the portal.

Note Admin users can move endpoint MAC addresses from the Endpoint Identity Groups they have read-only access to, to the Endpoint Identity Groups they have full access to. The other way around is not possible.

Before you begin

- Create all the admin groups for which you want to define the role-based access control (RBAC) policies.
- Ensure that these admin groups are mapped to individual admin users.
- Ensure that you have configured the RBAC permissions such as menu access and data access permissions.

Step 1 Choose **Administration** > **System** > **Admin Access** > **Authorization** > **RBAC Policy**.

The RBAC Policies page contains a set of ready-to-use predefined policies for default admin groups. You cannot edit or delete these default policies. However, you can edit the data access permissions for the default Read-Only Admin policy.

Step 2 Click **Actions** next to any of the default RBAC policy rule.

Here, you can insert new RBAC policies, duplicate an existing RBAC policy, and delete an existing RBAC policy.

Step 3 Click **Insert new policy**.

Step 4 Enter values for the Rule Name, RBAC Group(s), and Permissions fields.

You cannot select multiple menu access and data access permissions when creating an RBAC policy.

Step 5 Click **Save**.

Administrator Access Settings

Cisco ISE allows you to define some rules for administrator accounts to enhance security. You can restrict access to the management interfaces, force administrators to use strong passwords, regularly change their passwords, and so on. The password policy that you define in the Administrator Account Settings in Cisco ISE applies to all administrator accounts.

Cisco ISE supports administrator passwords with UTF-8 characters.

Configure Maximum Number of Concurrent Administrative Sessions and Login Banners

You can configure the maximum number of concurrent administrative GUI or CLI (SSH) sessions and login banners that help and guide administrators who access your administrative web or CLI interface. You can configure login banners that appear before and after an administrator logs in. By default, these login banners are disabled. However, you cannot configure the maximum number of concurrent sessions for individual administrator accounts.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration** > **System** > **Admin Access** > **Settings** > **Access** > **Session**.

Step 2 Enter the maximum number of concurrent administrative sessions that you want to allow through the GUI and CLI interfaces. The valid range for concurrent administrative GUI sessions is from 1 to 20. The valid range for concurrent administrative CLI sessions is 1 to 10.

Step 3 If you want Cisco ISE to display a message before an administrator logs in, check the **Pre-login banner** check box and enter your message in the text box.

Step 4 If you want Cisco ISE to display a message after an administrator logs in, check the **Post-login banner** check box and enter your message in the text box.

Step 5 Click **Save**.

Note The character limit is set at 1500 for the Pre-login banner and 3000 for the Post-login banner. All characters except **%** and < are supported. For login banner installation through CLI, the maximum length of the file name used is 256 characters.

Related Topics

Allow Administrative Access to Cisco ISE from Select IP Addresses, on page 368

Allow Administrative Access to Cisco ISE from Select IP Addresses

Cisco ISE allows you to configure a list of IP addresses from which administrators can access the Cisco ISE management interfaces.

The administrator access control settings are only applicable to Cisco ISE nodes that assume the Administration, Policy Service, or Monitoring personas. These restrictions are replicated from the primary to the secondary nodes.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Settings** > **Access** > **IP Access**.

Step 2 Click the **Allow only Listed IP addresses to Connect** radio button.

Note Connection on Port 161 (SNMP) is used for administrative access. However, when IP access restrictions are configured, the **snmpwalk** fails if the node from which it was performed is not configured for administrative access.

Step 3 In the **Configure IP List for Access Restriction** area, click **Add**.

Step 4 In the **Add IP CIDR** dialog box, enter the IP addresses in the classless interdomain routing (CIDR) format in the **IP Address** field.

Note This IP address can be an IPv4 or an IPv6 address. You can configure multiple IPv6 addresses for a Cisco ISE node.

Step 5 Enter the subnet mask in the **Netmask in CIDR format** field.

Step 6 Click **OK**.

Repeat steps 4 to 7 to add more IP address ranges to this list.

Step 7 Click **Save** to save the changes.

Step 8 Click **Reset** to refresh the **IP Access** window.

Allow Access to MnT Nodes in Cisco ISE

Cisco ISE allows you the option either to allow only the nodes within the deployment to send logs and alarms to MnT nodes, or to make no restrictions.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 From the Cisco ISE home page, choose **Administration** > **System** > **Admin Access** > **Settings** > **Access**.

Step 2 Click the **MnT Access** tab.

Step 3 To allow nodes or entities either within the deployment or outside the deployment to send syslogs to MnT, click the **Allow any IP address to connect to MnT** radio button. To allow only nodes or entities within the deployment to send syslogs to MnT, click the **Allow only the nodes in the deployment to connect to MnT** radio button.

Note For ISE 2.6 P2 and later, Syslog over Cisco ISE Messaging Service is turned on by default. This allows syslog events including alarms, configuration changes, and session information, to come in from other entities outside of deployment.

Configure a Password Policy for Administrator Accounts

Cisco ISE also allows you to create a password policy for administrator accounts to enhance security. You can define whether you want a password-based or client certificate-based administrator authentication. The password policy that you define here is applied to all the administrator accounts in Cisco ISE.

Note

- Email notifications for internal admin users are sent to root@host. You cannot configure the email address, and many SMTP servers reject this email.

  Follow open defect CSCui5583, which is an enhancement to allow you to change the email address.

- Cisco ISE supports administrator passwords with UTF-8 characters.

Before you begin

- To perform the following task, you must be a Super Admin or System Admin.
- Turn off the automatic failover configuration, if this is enabled in your deployment. See Support for Automatic Failover for the Administration Node, on page 200

  When you change the authentication method, you restart the application server processes. There might be a delay while these services restart. Due to this delay in restart of services, automatic failover of secondary administration node might get initiated.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Authentication**.

Step 2 Click the radio button for one of the following authentication methods:

- **Password Based**: Choose this option to use the standard user ID and password credentials for administrator logins. Choose **Internal** or **External** from the **Identity Source** drop-down list.

  Note If you have configured an external identity source such as LDAP and want to use that as your authentication source to grant access to the admin user, you must select that particular identity source from the Identity Source list box.

- **Client Certificate Based**: Choose this option to specify a certificate-based policy. From the **Certificate Authentication Profile** drop-down list, choose an existing authentication profile. Choose the required value from the **Identity Source** drop-down list.

Step 3 Click the **Password Policy** tab and enter the required values to configure the Cisco ISE GUI and CLI password requirements.

Step 4 Click **Save** to save the administrator password policy.

Note If you use an external identity store to authenticate administrators at login, note that even if this setting is configured for the password policy applied to the administrator profile, the external identity store will still validate the administrator's username and password.

Related Topics

Administrator Password Policy Settings, on page 190

Configure Account Disable Policy for Administrator Accounts, on page 371
Configure Lock or Suspend Settings for Administrator Accounts, on page 371

Configure Account Disable Policy for Administrator Accounts

Cisco ISE allows you to disable an administrator account if the administrator account is not authenticated for the configured consecutive number of days.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Authentication** > **Account Disable Policy**.

Step 2 Check the **Disable account after *n* days of inactivity** check box, and enter the number of days in the corresponding field.

This option allows you to disable the administrator account if the administrator account was inactive for the specified number of days. However, you can exclude individual administrator accounts from this account disable policy using the **Inactive Account Never Disabled** option in the **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Users** window.

When an administrator account is disabled and enabled later, it does not remain active for more than 24 hours. If you want an administrator account to remain active even when disabled, keep the **Disable account after *n* days of inactivity** checkbox unchecked.

Attention Cisco ISE does not support the **Disable account after *n* days of inactivity** option even if it is enabled, for administrator accounts that have **Collection Filters** (**Work Centers** > **Network Access** > **Settings** > **Collection Filters** > **Filter All**) configured.

Step 3 Click **Save** to configure the global account disable policy for administrators.

Configure Lock or Suspend Settings for Administrator Accounts

Cisco ISE allows you to lock or suspend administrator accounts (including password-based internal administrator accounts and certificate-based administrator accounts) that have more than a specified number of failed login attempts.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Authentication** > **Lock/Suspend Settings**.

Step 2 Check the **Suspend Or Lock Account With Incorrect Login Attempts** check box and enter the number of failed attempts after which action should be taken. The valid range is from 3 through 20. Click the radio button for one of the following options:

- **Suspend Account For *n* Minutes**: Choose this option to suspend any account that exceeds a specified number of incorrect login attempts. The valid range is from 15 through 1440.
- **Lock Account**: Choose this option to lock an account that exceeds a specified number of incorrect login attempts.

You can enter a custom email remediation message, such as asking the end user to contact the helpdesk to unlock the account. You can also unlock all locked accounts by disabling and then enabling the **Suspend Or Lock Account With Incorrect Login Attempts** option.

Configure Session Timeout for Administrators

Cisco ISE allows you to determine the length of time an administration GUI session can be inactive and still remain connected. You can specify a time in minutes after which Cisco ISE logs out the administrator. After a session timeout, the administrator must log in again to access the Cisco ISE Admin portal.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration** > **System** > **Admin Access** > **Settings** > **Session** > **Session Timeout**.

Step 2 Enter the time in minutes that you want Cisco ISE to wait before it logs out the administrator if there is no activity. The default value is 60 minutes. The valid range is from 6 to 100 minutes.

Step 3 Click **Save**.

Terminate an Active Administrative Session

Cisco ISE displays all active administrative sessions from which you can select any session and terminate at any point of time, if a need to do so arises. The maximum number of concurrent administrative GUI sessions is 20. If the maximum number of GUI sessions is reached, an administrator who belongs to the super admin group can log in and terminate some of the sessions.

Before you begin

To perform the following task, you must be a Super Admin.

Step 1 Choose **Administration** > **System** > **Admin Access** > **Settings** > **Session** > **Session Info**.

Step 2 Check the check box next to the session ID that you want to terminate and click **Invalidate**.

Change Administrator Name

Cisco ISE allows you to change your username from the Cisco ISE GUI.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Log in to the Cisco ISE administration portal.

Step 2 Click the **Gear** icon (⚙) at the upper right corner of the Cisco ISE GUI, and choose **Account Settings** from the drop-down list.

Step 3 Enter the new username in the **Admin User** dialog box that is displayed.

Step 4 Edit any other details about your account that you want to change.

Step 5 Click **Save**.

Admin Access Settings

These sections enable you to configure access settings for administrators.

Administrator Password Policy Settings

The following table describes the fields in the **Password Policy** tab that you can use to define a criteria that administrator passwords should meet. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Authentication** > **Password Policy**.

Table 40: Administrator Password Policy Settings

Field Name	Usage Guidelines
Minimum Length	Specify the minimum length of the password (in characters). The default is six characters.

Field Name	Usage Guidelines
Password must not contain	**Admin name or its characters in reverse order**: Check this check box to restrict the use of the administrator username or its characters in reverse order as the password.
	Cisco or its characters in reverse order: Check this check box to restrict the use of the word "Cisco" or its characters in the reverse order as the password.
	This word or its characters in reverse order: Check this check box to restrict the use of any word that you define or its characters in the reverse order as the password.
	Repeated characters four or more times consecutively: Check this check box to restrict the use of repeated characters four or more times consecutively as the password.
	Dictionary words, their characters in reverse order, or their letters replaced with other characters: Check this check box to restrict the use of dictionary words, their characters in reverse order, or their letters replaced with other characters, as the password. Substitution of $ for s, @ for a, 0 for o, 1 for l, ! for i, 3 for e, and so on, is not permitted. For example, Pa$$w0rd is not permitted. • **Default Dictionary**: Choose this option to use the default Linux dictionary in Cisco ISE. The default dictionary contains approximately 480,000 English words. This option is selected by default. • **Custom Dictionary**: Choose this option to use your customized dictionary. Click **Choose File** to select a custom dictionary file. The text file must comprise newline-delimited (JSON format) words, .dic extension, and a size less than 20 MB.
Password must contain at least one character of each of the selected types	Check the check box for the type of characters an administrator's password must contain. Choose one or more of the following options: • **Lowercase alphabetic characters** • **Uppercase alphabetic characters** • **Numeric characters** • **Non-alphanumeric characters**
Password History	Specify the number of previous passwords from which the new password must be different, to prevent the repeated use of the same password. Check the **Password must be different from the previous *n*versions** check box, and enter the number in the corresponding field. Enter the number of days before which you cannot reuse a password. Check the **Cannot reuse password within *n* days** check box, and enter the number in the corresponding field.

Field Name	Usage Guidelines
Password Lifetime	Check the check boxes for the following options to force users to change passwords after a specified time period: • **Administrator passwords expire *n* days after creation or last change**: Time (in days) before the administrator account is disabled if the password is not changed. The valid range is 1 to 3650 days. • **Send an email reminder to administrators *n* days prior to password expiration**: Time (in days) before which administrators are reminded that their password will expire. The valid range is 1 to 3650 days.
Display Network Device-Sensitive Data	
Require Admin Password	Check this check box if you want the admin user to enter the login password to view network device-sensitive data such as shared secrets and passwords.
Password cached for *n* Minutes	The password that is entered by the admin user is cached for this time period. The admin user will not be prompted to enter the password again during this period to view the network device-sensitive data. The valid range is from 1 to 60 minutes.

Related Topics

Cisco ISE Administrators, on page 15

Create a New Administrator, on page 16

Session Timeout and Session Information Settings

The following table describes the fields in the **Session** window that you can use to define session timeout and terminate an active administrative session. To access this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Settings** > **Session**.

Table 41: Session Timeout and Session Information Settings

Field Name	Usage Guidelines
Session Timeout	
Session Idle Timeout	Enter the time, in minutes, that you want Cisco ISE to wait for, before it logs out the administrator if there is no activity. The default value is 60 minutes. The valid range is from 6 to 100 minutes.
Session Info	
Invalidate	Check the check box adjacent to the session ID that you want to terminate and click **Invalidate.**

Related Topics

Administrator Access Settings, on page 367

Configure Session Timeout for Administrators, on page 372

Terminate an Active Administrative Session, on page 372

CHAPTER 6

Maintain and Monitor

- Adaptive Network Control, on page 378
- Enable Adaptive Network Control in Cisco ISE, on page 379
- Configure Network Access Settings, on page 379
- ANC NAS Port Shutdown Flow, on page 380
- Endpoints Purge Settings, on page 381
- Quarantined Endpoints Do Not Renew Authentication Following Policy Change, on page 382
- ANC Operations Fail when IP Address or MAC Address is not Found, on page 382
- Externally Authenticated Administrators Cannot Perform ANC Operations, on page 383
- Backup Data Type, on page 383
- Backup and Restore Repositories, on page 384
- On-Demand and Scheduled Backups, on page 389
- Cisco ISE Restore Operation, on page 395
- Export Authentication and Authorization Policy Configuration, on page 400
- Schedule Policy Export Settings, on page 401
- Synchronize Primary and Secondary Nodes in a Distributed Environment, on page 402
- Recovery of Lost Nodes in Standalone and Distributed Deployments, on page 402
- Cisco ISE Logging Mechanism, on page 406
- Cisco ISE System Logs, on page 407
- Configure Remote Syslog Collection Locations, on page 407
- Cisco ISE Message Codes, on page 409
- Cisco ISE Message Catalogs, on page 409
- Endpoint Debug Log Collector, on page 410
- Collection Filters, on page 410
- Cisco ISE Reports, on page 412
- Report Filters, on page 412
- Create the Quick Filter Criteria, on page 413
- Create the Advanced Filter Criteria, on page 413
- Run and View Reports, on page 414
- Reports Navigation, on page 414
- Export Reports, on page 414
- My Reports, on page 415
- Scheduling Cisco ISE Reports, on page 415
- Cisco ISE Active RADIUS Sessions, on page 418

- Available Reports, on page 419
- RADIUS Live Logs, on page 443
- RADIUS Live Sessions, on page 446
- TACACS Live Logs, on page 449
- Export Summary, on page 450
- RADIUS Live Logs, on page 452
- RADIUS Live Sessions, on page 454
- TACACS Live Logs, on page 458
- Export Summary, on page 459

Adaptive Network Control

Adaptive Network Control (ANC) is a service that runs on the Administration node. This service monitors and controls network access of endpoints. ANC is invoked by the ISE administrator on the admin GUI, and also can be invoked through pxGrid from third-party systems. ANC supports wired and wireless deployments and requires an Advantage License.

You can use ANC to change the authorization state without having to modify the overall authorization policy of the system. ANC allows you to set the authorization state when you quarantine an endpoint. As a result, the established authorization policies where authorization policies are defined to check for ANCPolicy to limit or deny network access. You can unquarantine an endpoint for full network access. You can also shut down the port on the network attached system (NAS) that disconnects the endpoint from the network.

There are no limits to the number of users that can be quarantined at one time. Also, there are no time constraints on the quarantine period length.

You can perform the following operations to monitor and control network access through ANC:

- Quarantine: Allows you to use Exception policies (authorization policies) to limit or deny an endpoint access to the network. You must create Exception policies to assign different authorization profiles (permissions) depending on the ANCPolicy. Setting to the Quarantine state essentially moves an endpoint from its default VLAN to a specified Quarantine VLAN. You must define the Quarantine VLAN previously that is supported on the same NAS as the endpoint.

- Unquarantine: Allows you to reverse the quarantine status that permits full access to the network for an endpoint. This happens by returning the endpoint to its original VLAN.

- Shutdown: Allows you to deactivate a port on the NAS and disconnect the endpoint from the network. Once the port is shut down on the NAS to which an endpoint is connected, manually reset the port on the NAS again. This allows an endpoint to connect to the network, which is not available for wireless deployments.

Quarantine and unquarantine operations can be triggered from the session directory reports for active endpoints.

Note If a quarantined session is unquarantined, the initiation method for a newly unquarantined session depends on the authentication method that is specified by the switch configuration.

Enable Adaptive Network Control in Cisco ISE

ANC is disabled by default. ANC gets enabled only when pxGrid is enabled, and it remains enabled until you manually disable the service in the Admin portal.

Configure Network Access Settings

ANC allows you to reset the network access status of an endpoint to quarantine, unquarantine, or shut down a port. These define the degree of authorization for the endpoints in the network.

You can quarantine or unquarantine endpoints, or shut down the network access server (NAS) ports to which endpoints are connected, by using their endpoint IP addresses or MAC addresses. You can perform quarantine and unquarantine operations on the same endpoint multiple times, provided they are not performed simultaneously. If you discover a hostile endpoint on your network, you can shut down the endpoint's access, using ANC to close the NAS port.

To assign an ANC policy to an endpoint:

Before you begin

- Enable ANC.
- Create authorization profiles and exception type authorization policies for ANC.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Adaptive Network Control** > **Policy List**.

Step 2 Click **Add**.

Step 3 Enter a name for the ANC policy and specify the ANC action. The following options are available:

- Quarantine
- Shut_Down
- Port_Bounce

You can select one or multiple actions, but you cannot combine Shut_Down and Port_Bounce with the other ANC actions .

Quarantine and Re_Authenticate are the only two actions that can be combined.

When an ANC policy with Quarantine, Port_Bounce, or Re_Authenticate is assigned or unassigned to an active endpoint, a CoA is triggered for that endpoint.

When an ANC policy with Shut_Down action is assigned to an active endpoint, a CoA is triggered to shutdown the switch interface. However, CoA is not triggered when an ANC policy with Shut_Down action is unassigned.

Step 4 Choose **Policy** > **Policy Sets**, and expand the policy set.

Step 5 Associate the ANC policy with the corresponding authorization policy by using the ANCPolicy attribute.

Step 6 Choose **Operations** > **Adaptive Network Control** > **Endpoint Assignment**.

Step 7 Click **Add**.

Step 8 Enter the IP address or MAC address of the endpoint and select the policy from the **Policy Assignment** drop-down list.

Step 9 Click **Submit**.

Create Authorization Profiles for Network Access through ANC

You need to create an authorization profile that should be use with ANC. you can view the authorization profile in the list of Standard Authorization Profiles. An endpoint can be authenticated and authorized in the network, but restricted to access network.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Authorization** > **Authorization Profiles**.

Step 2 Click **Add**.

Step 3 Enter a unique name and description for the authorization profile, and update the **Access Type** as **ACCESS_ACCEPT**.

Step 4 Check the **DACL Name** check box, and choose **DENY_ALL_TRAFFIC** from the drop-down list.

Step 5 Click **Submit**.

Exception authorization polices are intended for authorizing limited access to meet special conditions or permissions or an immediate requirement. For ANC authorization, you need to create a quarantine exception policy that is processed before all standard authorization policies. You need to create an exception rule with the following condition:

Session:ANCPolicy EQUALS Quarantine.

ANC NAS Port Shutdown Flow

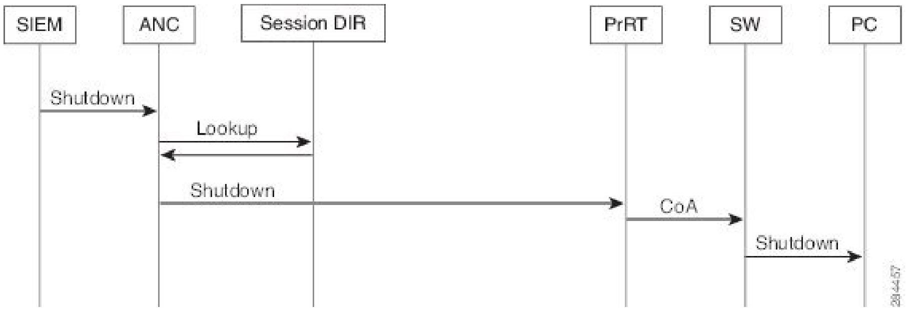
You can shut down the NAS port to which an endpoint is connected by using the endpoint IP address or MAC address.

Shutdown allows you to close a NAS port based on a specified IP address for a MAC address. You have to manually reinstate the port to bring the endpoint back into the network, which is effective only for endpoints that are connected through wired media.

Shutdown may not be supported on all devices. Most switches should support the shutdown command, however. You can use the getResult() command to verify that the shutdown is executed successfully.

This figure illustrates the ANC shutdown flow. For the client device, the shutdown operation is performed on the NAS that the client device uses to access the network.

Figure 11: ANC Shutdown Flow



Endpoints Purge Settings

You can define the endpoint purge policy by configuring rules, based on identity groups and other conditions. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **Settings** > **Endpoint Purge**. You can choose not to purge specified endpoints and to purge endpoints based on selected profiling conditions.

You can schedule an endpoint purge job. This endpoint purge schedule is enabled by default. Cisco ISE, by default, deletes endpoints and registered devices that are older than 30 days. The purge job runs at 1:00 a.m. (midnight) every day based on the time zone configured in the primary PAN.

Endpoint purge deletes over five thousand endpoints every 3 minutes.

The following are some of the conditions with examples you can use for purging the endpoints:

- InactivityDays— Number of days since last profiling activity or update on endpoint
    - This condition purges stale devices that have accumulated over time, commonly transient guest or personal devices, or retired devices. These endpoints tend to represent noise in your deployment as they are no longer active on network or not likely to be seen in near future. If they do happen to connect again, then they will be rediscovered, profiled, registered, etc as needed.
    - When there are updates from endpoint, InactivityDays will be reset to 0 only if profiling is enabled.
- ElapsedDays—Numbers days since object is created.
    - This condition can be used for endpoints that have been granted unauthenticated or conditional access for a set time period, such as a guest or contractor endpoint, or employees leveraging webauth for network access. After the allowed connect grace period, they must be fully reauthenticated and registered.
- PurgeDate—Date to purge the endpoint.
    - This option can be used for special events or groups where access is granted for a specific time, regardless of creation or start time. This allows all endpoints to be purged at same time. For example, a trade show, a conference, or a weekly training class with new members each week, where access is granted for specific week or month rather than absolute day, week, or month.

Note If the endpoint count to be purged is more than 10000, only the first 10000 endpoints are purged during the initial purge. After 1 hour, another purge is initiated to delete the next set of 10000 endpoints. This purge cycle will continue until all the endpoints are purged based on purge condition that is matched. This behavior optimizes system performance.

Quarantined Endpoints Do Not Renew Authentication Following Policy Change

Problem

Authentication has failed following a change in policy or additional identity and no reauthentication is taking place. Authentication fails or the endpoint in question remains unable to connect to the network. This issue often occurs on client machines that fails posture assessment per the posture policy that is assigned to the user role.

Possible Causes

The authentication timer setting is not correctly set on the client machine, or the authentication interval is not correctly set on the switch.

Solution

There are several possible resolutions for this issue:

1. Check the **Session Status Summary** report in Cisco ISE for the specified NAD or switch, and ensure that the interface has the appropriate authentication interval configured.
2. Enter “show running configuration” on the NAD/switch and ensure that the interface is configured with an appropriate “authentication timer restart” setting. (For example, “authentication timer restart 15,” and “authentication timer reauthenticate 15.”)
3. Enter “interface shutdown” and “no shutdown” to bounce the port on the NAD/switch and force reauthentication following a potential configuration change in Cisco ISE.

Note Because CoA requires a MAC address or session ID, we recommend that you do not bounce the port that is shown in the Network Device SNMP report.

ANC Operations Fail when IP Address or MAC Address is not Found

An ANC operation that you perform on an endpoint fails when an active session for that endpoint does not contain information about the IP address. This also applies to the MAC address and session ID for that endpoint.

Note When you want to change the authorization state of an endpoint through ANC, you must provide the IP address or the MAC address for the endpoint. If the IP address or the MAC address is not found in the active session for the endpoint, then you will see the following error message:

```
 No active session found for this MAC address, IP Address or Session ID
```

.

Externally Authenticated Administrators Cannot Perform ANC Operations

If an externally authenticated administrator tries to issue CoA-Quarantine from a live session, Cisco ISE returns the following error message:

```
CoA Action of Quarantine for xx:xx:xx:xx:xx:xx can not be initiated. (Cause:User
 not found internally. Possible use of unsupported externally authenticated user
```

If an externally authenticated administrator performs an ANC operation from **Operations** in the Cisco ISE using the IP address or MAC address of the endpoint, Cisco ISE returns the following error message:

```
Server failure: User not found internally. Possible use of unsupported externally
 authenticated user
```

Backup Data Type

Cisco ISE allows you to back up data from the primary PAN and from the Monitoring node. Backup can be done from the CLI or user interface.

Cisco ISE allows you to back up the following type of data:

- Configuration data—Contains both application-specific and Cisco ADE operating system configuration data. Backup can be done via the primary PAN using the GUI or CLI.
- Operational Data—Contains monitoring and troubleshooting data. Backup can be done via the primary PAN GUI or using the CLI for the Monitoring node.

When Cisco ISE is run on VMware, VMware snapshots are not supported for backing up ISE data.

Note Cisco ISE does not support VMware snapshots for backing up ISE data because a VMware snapshot saves the status of a VM at a given point in time. In a multinode Cisco ISE deployment, data in all the nodes are continuously synchronized with current database information. Restoring a snapshot might cause database replication and synchronization issues. We recommend that you use the backup functionality included in Cisco ISE for archival and restoration of data.

Using VMware snapshots or any third-party backup service to back up Cisco ISE data might result in interrupting Cisco ISE services. When a backup is initiated by VMware or any other third-party backup service like CommVault SAN level backup, it quiesces the file system to maintain crash consistency, which can cause your Cisco ISE functionalities to freeze. A reboot is required to resume the services on your Cisco ISE deployment.

The restore operation can be performed with the backup files of previous versions of Cisco ISE and restored on a later version, as long as the previous versions are in the supported direct upgrade path for the later version.

Cisco ISE, Release 3.1 supports restore from backups obtained from Release 2.6 and later.

Note While recreating a deployment after backing up and restoring data, a **Context Visibility Reset** of both the Primary PAN and Secondary PAN are required to ensure that data on both the nodes are synced.

Backup and Restore Repositories

Cisco ISE allows you to create and delete repositories through the administrator portal. You can create the following types of repositories:

- DISK
- FTP
- SFTP
- NFS
- CD-ROM
- HTTP
- HTTPS

Note Repositories are local to each device.

We recommend that you have a repository size of minimum 100 GB for all types of deployment (small, medium, and large).

The following table shows the supportability information between the Cisco ISE operations and the type of external repositories:

Table 42: Supportability Matrix for External Repositories

Repository Type	Config Backup	Config Restore	Upgrade	Operational Backup	Operational Restore	Support Bundle	Validation from the User Interface	Exporting Reports from the User Interface	Exporting Policies from the User Interface
FTP	√	√	√	√	√	√	√	√	√
SFTP	√	√	√	√	√	√	√	√	√
TFTP	X	X	X	X	X	X	X	X	X
HTTP	X	X	√	X	X	X	X	X	X
HTTPS	X	*X*	√	X	X	X	X	X	X
NFS	√	√	√	√	√	√	√	√	√

Create Repositories

You can use the CLI and GUI to create repositories. We recommend that you use the GUI due to the following reasons:

- Repositories that are created through the CLI are saved locally and do not get replicated to the other deployment nodes. These repositories do not get listed in the GUI's repository page.
- Repositories that are created on the primary PAN get replicated to the other deployment nodes.

The keys are generated only at the primary PAN on GUI, and so during upgrade you need to generate the keys again at GUI of new primary admin and export it to the SFTP server. If you remove the nodes from your deployment, you need to generate the keys on GUI of non-admin nodes and export it to the SFTP server.

You can configure an SFTP repository in Cisco ISE with RSA public key authentication. Instead of using an administrator-created password to encrypt the database and logs, you can choose the RSA public key authentication that uses secure keys. In case of SFTP repository created with RSA public key, the repositories created through the GUI do not get replicated in the CLI and the repositories created through the CLI do not get replicated in the GUI. To configure same repository on the CLI and GUI, generate RSA public keys on both CLI and GUI and export both the keys to the SFTP server.

Note Cisco ISE initiates outbound SSH or SFTP connections in FIPS mode even if FIPS mode is not enabled on ISE. Ensure that the remote SSH or SFTP servers that communicate with ISE allow FIPS 140 approved cryptographic algorithms.

Cisco ISE uses embedded FIPS 140 validated cryptographic modules. For details of the FIPS compliance claims, see the FIPS Compliance Letter.

Before you begin

- To perform the following task, you must have the privileges of either a Super Admin or System Admin.

- If you want to create an SFTP repository with RSA public key authentication, perform the following steps:
    - Enable RSA public key authentication in the SFTP repository.
    - You must log in as the Admin CLI user. Enter the host key of the SFTP server from the Cisco ISE CLI using the **crypto host_key add** command. The host key string should match the hostname that you enter in the **Path** field of the repository configuration page.
    - Generate the key pairs and export the public key to your local system from the GUI. From the Cisco ISE CLI, generate the key pairs using the **crypto key generate rsa passphrase** *test123* command, where, passphrase must be greater than 13 letters, and export the keys to any repository (local disk or any other configured repository).
    - Copy the exported RSA public key to the PKI-enabled SFTP server and add it to the "authorized_keys" file.

Note When primary PAN and primary MnT are separate nodes, you can use the **Generate Key Pairs** option in the **Repository List** window to generate RSA keys for both primary PAN and primary MnT nodes. You can use the **Export Public Key** option in the **Repository List** window to export the generated RSA keys from both primary PAN and primary MnT nodes.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Maintenance** > **Repository**.

Step 2 Click **Add** to add a new repository.

Step 3 Enter the values as required to set up new repository. See Repository Settings, on page 387 for a description of the fields.

Step 4 Click **Submit** to create the repository.

Step 5 Verify that the repository is created successfully by clicking **Repository** from the **Operations** navigation pane on the left or click the **Repository List** link at the top of **Repository** window to go to the repository listing page.

What to do next

- Ensure that the repository that you have created is valid. You can do so from the **Repository Listing** window. Select the corresponding repository and click **Validate**. Alternatively, you can execute the following command from the Cisco ISE command-line interface:

  show repository *repository_name*

  where *repository_name* is the name of the repository that you have created.

  Note If the path that you provided while creating the repository does not exist, then you will get the following error:

  ```
  %Invalid Directory
  ```

- Run an on-demand backup or schedule a backup.

Repository Settings

The following table describes the fields on the **Repository List** window, which you can use to create repositories to store your backup files. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Maintenance** > **Repository**.

Table 43: Repository Settings

Fields	Usage Guidelines
Repository	Enter the name of the repository. Alphanumeric characters are allowed and the maximum length is 80 characters.
Protocol	Choose one of the available protocols that you want to use.
Server Name	(Required for TFTP, HTTP, HTTPS, FTP, SFTP, and NFS) Enter the hostname or IP address (IPv4 or IPv6) of the server where you want to create the repository. **Note** Ensure that the ISE eth0 interface is configured with an IPv6 address if you are adding a repository with an IPv6 address.
Path	Enter the path to your repository. The path must be valid and must exist at the time you create the repository. This value can start with two forward slashes (//) or a single forward slash (/) denoting the root directory of the server. However, for the FTP protocol, a single forward slash (/) denotes the FTP of the local device home directory and not the root directory.
Enable PKI authentication	(Optional; applicable only for SFTP repository) Check this check box if you want to enable RSA Public Key Authentication in SFTP repository.
User Name	(Required for FTP, SFTP) Enter the username that has write permission to the specified server. A username can contain alphanumeric and _-. /@\$ characters.
Password	(Required for FTP, SFTP) Enter the password that will be used to access the specified server. Passwords can consist of the following characters: 0 to 9, a to z, A to Z, -, ., |, @, #,$, ^, &, *, (,), +, and =. Note that some of the special characters like !, ?, ~ (that are not included in the list above) are allowed for the FTP and SFTP password configuration via GUI. However, these special characters are not allowed for configuration via CLI or Open API.

Related Topics

Backup and Restore Repositories, on page 384

Create Repositories, on page 385

Enable RSA Public Key Authentication in SFTP Repository

In the SFTP server, each node must have two RSA public keys, one each for CLI and for GUI. To enable RSA public key authentication in SFTP repository, perform the following steps:

Note After you enable RSA public key authentication in SFTP repository, you will not be able to log in using SFTP credentials. You can either use PKI-based authentication or credential-based authentication. If you want to use credential-based authentication again, you must remove the public key pair from the SFTP server.

Step 1 Log in to SFTP server with an account that has permission to edit the */etc/ssh/sshd_config.file*.

Note The location of the *sshd_config* file might vary based on the operating system installation.

Step 2 Enter the **vi /etc/ssh/sshd_config** command.

The contents of the sshd_config file is listed.

Step 3 Remove the "#" symbol from the following lines to enable RSA public key authentication:

- RSAAuthentication yes
- PubkeyAuthentication yes

  Note If Public Auth Key is no, change it to yes.
- AuthorizedKeysFile ~/.ssh/authorized_keys

Download Files from Local Disk

You can easily add, download, or delete the files that are used for local disk management.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **System** > **Maintenance** > **Localdisk Management**.

Step 2 Check the check box next to the file to be downloaded.

Step 3 Click **Download**.

Step 4 (Optional) Run the following command from the Cisco ISE CLI to download a file from local disk: **#copy disk:/** *filename* **repository** *repository_name*

Upload a File to Local Disk

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **System** > **Maintenance** > **Localdisk Management**.

Step 2 To upload a file, click **Upload**.

Step 3 Click **Select File** to browse and select the file to be uploaded. You can also drag and drop the file.

Step 4 Click **Start Upload**.

On-Demand and Scheduled Backups

You can configure on-demand backups of the primary PAN and the primary monitoring node. Perform an on-demand backup when you want to back up data immediately.

You can schedule system-level backups to run once, daily, weekly, or monthly. Because backup operations can be lengthy, you can schedule them so they are not a disruption. You can schedule a backup from the Admin portal.

Note If you are using the internal CA, you should use the CLI to export certificates and keys. Backup using in the administration portal does not back up the CA chain.

For more information, see the "Export Cisco ISE CA Certificates and Keys" section in the "Basic Setup" chapter *Cisco Identity Services Engine Administrator Guide* .

Configurational and operational backups on Cisco ISE can overload your system for a short time. This expected behaviour of temporary system overload will depend on the configuration and monitoring database size of your system.

Related Topics

Maintenance Settings, on page 1276

Perform an On-Demand Backup

You can perform an On-demand backup to instantly back up the configuration or monitoring (operational) data. The restore operation restores Cisco ISE to the configuration state that existed at the time of obtaining the backup.

Important When performing a back up and restore, the restore overwrites the list of trusted certificates on the target system with the list of certificates from the source system. It is critically important to note that backup and restore functions do not include private keys associated with the Internal Certificate Authority (CA) certificates.

If you are performing a back up and restore from one system to another, you have to choose from one of these options to avoid errors:

- **Option 1:**

  Export the CA certificates from the source ISE node through the CLI and import them in to the target system through the CLI.

  Pros: Any certificates issued to endpoints from the source system will continue to be trusted. Any new certificates issued by the target system will be signed by the same keys.

  Cons: Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

- **Option 2:**

  After the restore process, generate all new certificates for the internal CA.

  Pros: This option is the recommended and clean method, where neither the original source certificates or the original target certificates will be used. Certificates issued by the original source system continues to be trusted.

  Cons: Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

Before you begin

- Before you perform an on-demand backup, you should have a basic understanding of the backup data types in Cisco ISE.
- Ensure that you have created repositories for storing the backup files.
- Do not back up using a local repository. You cannot back up the monitoring data in the local repository of a remote Monitoring node.
- Ensure that you perform all certificate-related changes before you obtain the backup.
- To perform the following task, you must be a Super Admin or System Admin.

Note For backup and restore operations, the following repository types are not supported: CD-ROM, HTTP, HTTPS, or TFTP. This is because, either these repository types are read-only or the protocol does not support file listing. To restore a backup, choose the repository and click **Restore**.

Step 1 Choose **Administration** > **System** > **Backup and Restore**.

Step 2 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Backup and Restore**.

Step 3 Choose the type of backup: Configuration or Operational.

Step 4 Click **Backup Now**.

Step 5 Enter the values as required to perform a backup.

Step 6 Click **Backup**.

Step 7 Verify that the backup completed successfully.

Cisco ISE appends the backup filename with a timestamp and stores the file in the specified repository. In addition to the timestamp, Cisco ISE adds a CFG tag for configuration backups and OPS tag for operational backups. Ensure that the backup file exists in the specified repository.

In a distributed deployment, do not change the role of a node or promote a node when the backup is running. Changing node roles does not shut down all the processes and might cause some inconsistency in data if a backup is running concurrently. Wait for the backup to complete before you make any node role changes.

Do not promote a node when the backup is running. This will shut down all the processes and might cause some inconsistency in data if a backup is running concurrently. Wait for the backup to complete before you make any node changes.

Note High CPU usage might be observed and High Load Average alarm might be seen when the backup is running. CPU usage will be back to normal when the backup is complete.

Related Topics

Cisco ISE Restore Operation, on page 395
Export Authentication and Authorization Policy Configuration, on page 400

On-Demand Backup Settings

The following table describes the fields on the **On-Demand Backup** window, which you can use to obtain a backup at any point of time. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Backup & Restore**.

Table 44: On-Demand Backup Settings

Field Name	Usage Guidelines
Type	Choose one of the following: • **Configuration Data Backup**: Includes both application-specific and Cisco ADE operating system configuration data • **Operational Data Backup**: Includes monitoring and troubleshooting data
Backup Name	Enter the name of your backup file.
Repository Name	Repository where your backup file should be saved. You cannot enter a repository name here. You can only choose an available repository from the drop-down list. Ensure that you create the repository before you run a backup.
Encryption Key	This key is used to encrypt and decrypt the backup file.

Related Topics

- Backup Data Type, on page 383
- On-Demand and Scheduled Backups, on page 389
- Backup History, on page 394
- Backup Failures, on page 394
- Cisco ISE Restore Operation, on page 395
- Export Authentication and Authorization Policy Configuration, on page 400
- Synchronize Primary and Secondary Nodes in a Distributed Environment, on page 402
- Perform an On-Demand Backup, on page 389

Schedule a Backup

You can perform an On-demand backup to instantly back up the configuration or monitoring (operational) data. The restore operation restores Cisco ISE to the configuration state that existed at the time of obtaining the backup.

Important When performing a back up and restore, the restore overwrites the list of trusted certificates on the target system with the list of certificates from the source system. It is critically important to note that backup and restore functions do not include private keys associated with the Internal Certificate Authority (CA) certificates.

If you are performing a back up and restore from one system to another, you will have to choose from one of these options to avoid errors:

- **Option 1:**

  Export the CA certificates from the source ISE node through the CLI and import them in to the target system through the CLI.

  Pros: Any certificates issued to endpoints from the source system will continue to be trusted. Any new certificates issued by the target system will be signed by the same keys.

  Cons: Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

- **Option 2:**

  After the restore process, generate all new certificates for the internal CA.

  Pros: This option is the recommended and clean method, where the original source certificates or the original target certificates will be used. Certificates issued by the original source system will continue to be trusted.

  Cons: Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

Before you begin

- Before you schedule a backup, you should have a basic understanding of the backup data types in Cisco ISE.
- Ensure that you have configured repositories.

- Do not back up using a local repository. You cannot back up the monitoring data in the local repository of a remote Monitoring node.
- To perform the following task, you must be a Super Admin or System Admin.

Note For backup and restore operations, the following repository types are not supported: CD-ROM, HTTP, HTTPS, or TFTP. This is because, either these repository types are read-only or the protocol does not support file listing.

Scheduled Backup Settings

The following table describes the fields on the Scheduled Backup window, which you can use to restore a full or incremental backup. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Backup and Restore**.

Table 45: Scheduled Backup Settings

Field Name	Usage Guidelines
Type	Choose one of the following: • **Configuration Data Backup**: Includes both application-specific and Cisco ADE operating system configuration data • **Operational Data Backup**: Includes monitoring and troubleshooting data
Name	Enter a name for your backup file. You can enter a descriptive name of your choice. Cisco ISE appends the timestamp to the backup filename and stores it in the repository. You will have unique backup filenames even if you configure a series of backups. On the Scheduled Backup list window, the backup filename will be prepended with “backup_occur” to indicate that the file is an occurrence **kron** job.
Description	Enter a description for the backup.
Repository Name	Select the repository where your backup file should be saved. You cannot enter a repository name here. You can only choose an available repository from the drop-down list. Ensure that you create the repository before you run a backup.
Encryption Key	Enter a key to encrypt and decrypt the backup file.
Schedule Options	Choose the frequency of your scheduled backup and fill in the other options accordingly.

Related Topics

Backup Data Type, on page 383
On-Demand and Scheduled Backups, on page 389
Backup History, on page 394
Backup Failures, on page 394
Cisco ISE Restore Operation, on page 395
Export Authentication and Authorization Policy Configuration, on page 400

Synchronize Primary and Secondary Nodes in a Distributed Environment, on page 402
Backup Using the CLI, on page 394
Schedule a Backup, on page 392

Backup Using the CLI

Although you can schedule backups both from the CLI as well as the GUI, it is recommended to use GUI. However, you can perform operational backup on the secondary monitoring node only from the CLI.

Backup History

Backup history provides basic information about scheduled and on-demand backups. It lists the name of the backup, backup file size, repository where the backup is stored, and time stamp that indicates when the backup was obtained. This information is available in the Operations Audit report and on the Backup and Restore page in the History table.

For failed backups, Cisco ISE triggers an alarm. The backup history page provides the failure reason. The failure reason is also cited in the Operations Audit report. If the failure reason is missing or is not clear, you can run the **backup-logs** command from the Cisco ISE CLI and look at the ADE.log for more information.

While the backup operation is in progress, you can use the **show backup status** CLI command to check the progress of the backup operation.

Backup history is stored along with the Cisco ADE operating system configuration data. It remains there even after an application upgrade and are only removed when you reimage the PAN.

Backup Failures

If backup fails, check the following:

- Check if there is any NTP sync or service failure issue. When the NTP service on Cisco ISE is not working, Cisco ISE raises the NTP Service Failure alarm. When Cisco ISE cannot sync with all the configured NTP servers, Cisco ISE raises the NTP Sync Failure alarm. Cisco ISE backup might fail if the NTP services are down or if there is any sync issue. Check the Alarms dashlet and fix the NTP sync or service issue before you retry the backup operation.
- Make sure that no other backup is running at the same time.
- Check the available disk space for the configured repository.
    - Monitoring (operational) backup fails if the monitoring data takes up more than 75% of the allocated monitoring database size. For example, if your Monitoring node is allocated 600 GB, and the monitoring data takes up more than 450 GB of storage, then monitoring backup fails.
    - If the database disk usage is greater than 90%, a purge occurs to bring the database size to less than or equal to 75% of its allocated size.
- Verify if a purge is in progress. Backup and restore operations will not work while a purge is in progress.
- Verify if the repository is configured correctly.

Cisco ISE Restore Operation

You can restore configuration data on a primary or standalone administration node. After you restore data on the Primary PAN, you must manually synchronize the secondary nodes with the Primary PAN.

The process for restoring the operational data is different depending on the type of deployment.

Note The new backup/restore user interface in Cisco ISE makes use of meta-data in the backup filename. Therefore, after a backup completes, you should not modify the backup filename manually. If you manually modify the backup filename, the Cisco ISE backup/restore user interface will not be able to recognize the backup file. If you have to modify the backup filename, you should use the Cisco ISE CLI to restore the backup.

Guidelines for Data Restoration

Following are guidelines to follow when you restore Cisco ISE backup data.

- Cisco ISE allows you to obtain a backup from an ISE node (A) and restore it on another ISE node (B), both having the same host names (but different IP addresses). However, after you restore the backup on node B, do not change the hostname of node B because it might cause issues with certificates and portal group tags.
- If you obtain a backup from the Primary PAN in one timezone and try to restore it on another Cisco ISE node in another timezone, the restore process might fail. This failure happens if the timestamp in the backup file is later than the system time on the Cisco ISE node on which the backup is restored. If you restore the same backup a day after it was obtained, then the timestamp in the backup file is in the past and the restore process succeeds.
- When you restore a backup on the Primary PAN with a different hostname than the one from which the backup was obtained, the Primary PAN becomes a standalone node. The deployment is broken and the secondary nodes become nonfunctional. You must make the standalone node the primary node, reset the configuration on the secondary nodes, and reregister them with the primary node. To reset the configuration on Cisco ISE nodes, enter the following command from the Cisco ISE CLI:
  - **application reset-config ise**
- We recommend that you do not change the system timezone after the initial Cisco ISE installation and setup.
- If you changed the certificate configuration on one or more nodes in your deployment, you must obtain another backup to restore the data from the standalone Cisco ISE node or Primary PAN. Otherwise, if you try to restore data using an older backup, the communication between the nodes might fail.
- After you restore the configuration backup on the Primary PAN, you can import the Cisco ISE CA certificates and keys that you exported earlier.

Note If you did not export the Cisco ISE CA certificates and keys, then after you restore the configuration backup on the Primary PAN, generate the root CA and subordinate CAs on the Primary PAN and Policy Service Nodes (PSNs).

- If you are trying to restore a platinum database without using the correct FQDN (FQDN of a platinum database), you need to regenerate the CA certificates. (To view this window, click the **Menu** icon (☰) and choose **Administration** > **Certificates** > **Certificate Signing Requests** > **Replace ISE Root CA certificate chain**).However, If you restore the platinum database with the correct FQDN, note that the CA certificates regenerated automatically.
- You need a data repository, which is the location where Cisco ISE saves your backup file. You must create a repository before you can run an on-demand or scheduled backup.
- If you have a standalone administration node that fails, you must run the configuration backup to restore it. If the Primary PAN fails, you can use the distributed setup to promote your Secondary Administration Node to become the primary. You can then restore data on the Primary PAN after it comes up.

Note Cisco ISE also provides the **backup-logs** CLI command that you can use to collect log and configuration files for troubleshooting purposes.

Restoration of Configuration or Monitoring (Operational) Backup from the CLI

To restore configuration data through the Cisco ISE CLI, use the **restore** command in the EXEC mode. Use the following command to restore data from a configuration or operational backup:

restore *filename* **repository** *repository-name* **encryption-key hash|plain** *encryption-key name* **include-adeos**

Syntax Description

restore	Type this command to restore data from a configuration or operational backup.
filename	Name of the backed-up file that resides in the repository. Supports up to 120 alphanumeric characters. **Note** You must add the .tar.gpg extension after the filename (for example, myfile.tar.gpg).
repository	Specifies the repository that contains the backup.
repository-name	Name of the repository you want to restore the backup from.
encryption-key	(Optional) Specifies user-defined encryption key to restore backup.
hash	Hashed encryption key for restoring backup. Specifies an encrypted (hashed) encryption key that follows. Supports up to 40 characters.
plain	Plaintext encryption key for restoring backup. Specifies an unencrypted plaintext encryption key that follows. Supports up to 15 characters.
encryption-key name	Enter the encryption key.
include-adeos	(Optional, applicable only for configuration backup) Enter this command operator parameter if you want to restore ADE-OS configuration from a configuration backup. When you restore a configuration backup, if you do not include this parameter, Cisco ISE restores only the Cisco ISE application configuration data.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

When you use restore commands in Cisco ISE, the Cisco ISE server restarts automatically.

The encryption key is optional while restoring data. To support restoring earlier backups where you have not provided encryption keys, you can use the **restore** command without the encryption key.

Examples

```
ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository encryption-key plain
 Lab12345
Restore may require a restart of application services. Continue? (yes/no) [yes] ? yes
Initiating restore.  Please wait...
ISE application restore is in progress.
This process could take several minutes. Please wait...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Alert Process...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Alert Process...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin#
```

Related Commands

	Description
backup	Performs a backup (Cisco ISE and Cisco ADE OS) and places the backup in a repository.
backup-logs	Backs up system logs.
repository	Enters the repository submode for configuration of backups.
show repository	Displays the available backup files located on a specific repository.
show backup history	Displays the backup history of the system.
show backup status	Displays the status of the backup operation.
show restore status	Displays the status of the restore operation.

If the sync status and replication status after application restore for any secondary node is *Out of Sync*, you have to reimport the certificate of that secondary node to the Primary PAN and perform a manual synchronization.

Restore Configuration Backups from the GUI

You can restore a configuration backup from the Admin portal.

Before you begin

Ensure that the primary PAN Auto Failover configuration, if enabled in your deployment, is turned off. When you restore a configuration backup, the application server processes are restarted. There might be a delay while these services restart. Due to this delay in restart of services, auto failover of secondary PAN might get initiated.

When your deployment is a dual node deployment at the time configuration backup, ensure the following:

- Source and target nodes for the restore are same as the ones used for the configuration backup, the target node can be either stand-alone or primary.
- Source and target nodes for the restore are different from the ones used in the configuration backup, the target node must be stand-alone.

Note You can restore configuration database backup and regenerate the Root CA on a primary PAN only. However, you cannot restore the configuration database backup on a registered PAN.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Backup and Restore**.

Step 2 Select the name of the backup from the list of Configurational backup and click **Restore**.

Step 3 Enter the Encryption Key used during the backup.

Step 4 Click **Restore**.

What to do next

If you are using the Cisco ISE CA service, you must:

1. Regenerate the entire Cisco ISE CA root chain.
2. Obtain a backup of the Cisco ISE CA certificates and keys from the primary PAN and restore it on the secondary PAN. This ensures that the secondary PAN can function as the root CA or subordinate CA of an external PKI in case of a Primary PAN failure and you promote the secondary PAN to be the primary PAN.

Restoration of Monitoring Database

The process for restoring the Monitoring database is different depending on the type of deployment. The following sections explain how to restore the Monitoring database in standalone and distributed deployments.

You must use the CLI to restore an on-demand Monitoring database backup from previous releases of Cisco ISE. Restoring a scheduled backup across Cisco ISE releases is not supported.

Note If you attempt to restore data to a node other than the one from which the data was taken, you must configure the logging target settings to point to the new node. This ensures that the monitoring syslogs are sent to the correct node.

Restore a Monitoring (Operational) Backup in a Standalone Environment

The GUI lists only the backups that are taken from the current release. To restore backups that obtained from earlier releases, use the restore command from the CLI.

Before you begin

- Purge the old monitoring data.
- Schedule a backup or perform an on-demand backup.

Step 1 Choose **Administration** > **System** > **Backup and Restore**.

Step 2 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Backup and Restore**.

Step 3 Select the name of the backup from the list of Operational backup and click **Restore**.

Step 4 Enter the Encryption Key used during the backup.

Step 5 Click **Restore**.

Restore a Monitoring Backup with Administration and Monitor Personas

You can restore a Monitoring backup in a distributed environment with administration and monitor personas.

Before you begin

- Purge the old monitoring data.
- Schedule a backup or perform an on-demand backup.

Step 1 If you are using a primary and secondary PAN, synchronize the PANs.

When you synchronize the PANs, you must chose a PAN and promote that to be the active primary.

Step 2 Before you deregister the Monitoring node, assign the Monitoring persona to another node in the deployment.

Every deployment must have at least one functioning Monitoring node.

Step 3 Deregister the Monitoring node for backup.

Step 4 Restore the Monitoring backup to the newly deregistered node.

Step 5 Register the newly restored node with the current Administration node.

Step 6 Promote the newly restored and registered node as the active Monitoring node.

Restore a Monitoring Backup with a Monitoring Persona

You can restore a Monitoring backup in a distributed environment with only Monitoring persona.

Before you begin

- Purge the old monitoring data.
- Schedule a backup or perform an on-demand backup.

Step 1 Prepare to deregister the node to be restored. This is done by assigning the monitoring persona to another node in the deployment.

A deployment must have at least one functioning Monitoring node.

Step 2 Deregister the node to be restored.

Note Wait until the deregistration is complete before proceeding with the restore. The node must be in a standalone state before you can continue with the restore.

Step 3 Restore the Monitoring backup to the newly deregistered node.

Step 4 Register the newly restored node with the current Administration node.

Step 5 Promote the newly restored and registered node as the active Monitoring node.

Restore History

You can obtain information about all restore operations, log events, and statuses from the **Operations Audit Report** window.

Note However, the **Operations Audit Report** window does not provide information about the start times corresponding to the previous restore operations.

For troubleshooting information, you have to run the **backup-logs** command from the Cisco ISE CLI and look at the ADE.log file.

While the restore operation is in progress, all Cisco ISE services are stopped. You can use the **show restore status** CLI command to check the progress of the restore operation.

Export Authentication and Authorization Policy Configuration

You can export authentication and authorization policy configuration in the form of an XML file that you can read offline to identify any configuration errors and use for troubleshooting purposes. This XML file includes authentication and authorization policy rules, simple and compound policy conditions, Discretionary Access control Lists (DACLs), and authorization profiles. You can choose to email the XML file or save it to your local system.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Backup & Restore**.

Step 2 Click **Policy Export**.

Step 3 Enter the values as needed.

Step 4 Click **Export**.

Use a text editor such as WordPad to view the contents of the XML file.

Schedule Policy Export Settings

The following table describes the fields on the **Schedule Policy Export** window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Backup and Restore** > **Policy Export**.

Table 46: Schedule Policy Export Settings

Field Name	Usage Guidelines
Encryption	
Encryption Key	Enter a key to encrypt and decrypt the export data. This field is enabled only if you select the **Export with Encryption Key** option.
Destination	
Download file to local computer	Allows you to download the policy export file to your local system.
Email file to	You can enter multiple email addresses separated by a comma.
Repository	Select the repository to export policy data to. You can’t enter a repository name here. You can only choose an available repository from the drop-down list. Ensure that you create the repository before scheduling a policy export.
Export Now	Click this option to export the data to the local computer or send as an email attachment. You can’t export to a repository; you can only schedule a repository export.
Schedule	
Schedule Options	Choose the frequency of the export schedule and enter the other details accordingly.

Synchronize Primary and Secondary Nodes in a Distributed Environment

In a distributed environment, sometimes the Cisco ISE database in the primary and secondary nodes are not synchronized automatically after restoring a backup file on the PAN. If this happens, you can manually force a full replication from the PAN to the secondary ISE nodes. You can force a synchronization only from the PAN to the secondary nodes. During the sync-up operation, you cannot make any configuration changes. Cisco ISE allows you to navigate to other Cisco ISE Admin portal pages and make any configuration changes only after the synchronization is complete.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 2 Check the check boxes next to the secondary ISE nodes with an Out of Sync replication status.

Step 3 Click **Syncup** and wait until the nodes are synchronized with the PAN. You will have to wait until this process is complete before you can access the Cisco ISE Admin portal again.

Recovery of Lost Nodes in Standalone and Distributed Deployments

This section provides troubleshooting information that you can use to recover lost nodes in standalone and distributed deployments. Some of the following use cases use the backup and restore functionality and others use the replication feature to recover lost data.

Recovery of Lost Nodes Using Existing IP Addresses and Hostnames in a Distributed Deployment

Scenario

In a distributed deployment, a natural disaster leads to a loss of all the nodes. After recovery, you want to use the existing IP addresses and hostnames.

For example, you have two nodes: N1 (Primary Policy Administration Node or Primary PAN) and N2 (Secondary Policy Administration Node or Secondary PAN.) A backup of the N1 node, which was taken at time T1, is available. Later, both N1 and N2 nodes fail because of a natural disaster.

Assumption

All Cisco ISE nodes in the deployment were destroyed. The new hardware was imaged using the same hostnames and IP addresses.

Resolution Steps

1. You have to replace both the N1 and N2 nodes. N1 and N2 nodes will now have a standalone configuration.
2. Obtain a license with the UDI of the N1 and N2 nodes and install it on the N1 node.
3. You must then restore the backup on the replaced N1 node. The restore script will try to sync the data on N2, but N2 is now a standalone node and the synchronization fails. Data on N1 will be reset to time T1.
4. You must log in to the N1 Admin portal to delete and reregister the N2 node. Both the N1 and N2 nodes will have data reset to time T1.

Recovery of Lost Nodes Using New IP Addresses and Hostnames in a Distributed Deployment

Scenario

In a distributed deployment, a natural disaster leads to loss of all the nodes. The new hardware is reimaged at a new location and requires new IP addresses and hostnames.

For example, you have two ISE nodes: N1 (primary Policy Administration Node or primary PAN) and N2 (secondary Policy Service Node.) A backup of the N1 node which was taken at time T1, is available. Later, both N1 and N2 nodes fail because of a natural disaster. The Cisco ISE nodes are replaced at a new location and the new hostnames are N1A (primary PAN) and N2A (secondary Policy Service Node). N1A and N2A are standalone nodes at this point in time.

Assumptions

All Cisco ISE nodes in the deployment were destroyed. The new hardware was imaged at a different location using different hostnames and IP addresses.

Resolution Steps

1. Obtain the N1 backup and restore it on N1A. The restore script will identify the hostname change and domain name change, and will update the hostname and domain name in the deployment configuration based on the current hostname.
2. You must generate a new self-signed certificate.
3. You must log in to the Cisco ISE administrator portal on N1A.In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**, and do the following:

   Delete the old N2 node.

   Register the new N2A node as a secondary node. Data from the N1A node will be replicated to the N2A node.

Recovery of a Node Using Existing IP Address and Hostname in a Standalone Deployment

Scenario

A standalone administration node is down.

For example, you have a standalone administration node, N1. A backup of the N1 database was taken at time T1. The N1 node goes down because of a physical failure and must be reimaged or a new hardware is required. The N1 node must be brought back up with the same IP address and hostname.

Assumptions

This deployment is a standalone deployment and the new or reimaged hardware has the same IP address and hostname.

Resolution Steps

Once the N1 node is up after a reimage or you have introduced a new Cisco ISE node with the same IP address and hostname, you must restore the backup taken from the old N1 node. You do not have to make any role changes.

Recovery of a Node Using New IP Address and Hostname in a Standalone Deployment

Scenario

A standalone administration node is down.

For example, you have a standalone administration node, N1. A backup of the N1 database taken at time T1 is available. The N1 node is down because of a physical failure and will be replaced by a new hardware at a different location with a different IP address and hostname.

Assumptions

This is a standalone deployment and the replaced hardware has a different IP address and hostname.

Resolution Steps

1. Replace the N1 node with a new hardware. This node will be in a standalone state and the hostname is N1B.
2. You can restore the backup on the N1B node. No role changes are required.

Configuration Rollback

Problem

There may be instances where you inadvertently make configuration changes that you later determine were incorrect. For example, you may delete several NADs or modify some RADIUS attributes incorrectly and realize this issue several hours later. In this case, you can revert to the original configuration by restoring a backup that was taken before you made the changes.

Possible Causes

There are two nodes: N1 (primary Policy Administration Node or primary PAN) and N2 (secondary Policy Administration Node or secondary PAN) and a backup of the N1 node is available. You made some incorrect configuration changes on N1 and want to remove the changes.

Solution

Obtain a backup of the N1 node that was taken before the incorrect configuration changes were made. Restore this backup on the N1 node. The restore script will synchronize the data from N1 to N2.

Recovery of Primary Node in Case of Failure in a Distributed Deployment

Scenario

In a multinode deployment, the PAN fails.

For example, you have two Cisco ISE nodes, N1 (PAN) and N2 (Secondary Administration Node). N1 fails because of hardware issues.

Assumptions

Only the primary node in a distributed deployment has failed.

Resolution Steps

1. Log in to the N2 administrator portal. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment** and configure N2 as your primary node.

   The N1 node is replaced with a new hardware, reimaged, and is in the standalone state.

2. From the N2 administrator portal, register the new N1 node as a secondary node.

   Now, the N2 node becomes your primary node and the N1 node becomes your secondary node.

If you wish to make the N1 node the primary node again, log in to the N1 administrator portal and make it the primary node. N2 automatically becomes a secondary server. There is no data loss.

Recovery of Secondary Node in Case of Failure in a Distributed Deployment

Scenario

In a multinode deployment, a single secondary node has failed. No restore is required.

For example, you have multiple nodes: N1 (primary PAN), N2 (secondary PAN), N3 (secondary Policy Service Node), N4 (secondary Policy Service Node). One of the secondary nodes, N3, fails.

Resolution Steps

1. Reimage the new N3A node to the default standalone state.

2. Log in to the N1 Admin portal and delete the N3 node.
3. Reregister the N3A node.

   Data is replicated from N1 to N3A. No restore is required.

Cisco ISE Logging Mechanism

Cisco ISE provides a logging mechanism that is used for auditing, fault management, and troubleshooting. The logging mechanism helps you to identify fault conditions in deployed services and troubleshoot issues efficiently. It also produces logging output from the monitoring and troubleshooting primary node in a consistent fashion.

You can configure a Cisco ISE node to collect the logs in the local systems using a virtual loopback address. To collect logs externally, you configure external syslog servers, which are called targets. Logs are classified into various predefined categories. You can customize logging output by editing the categories with respect to their targets, severity level, and so on.

As a best practice, do not configure network devices to send syslogs to a Cisco ISE Monitoring and Troubleshooting (MnT) node as this could result in the loss of some Network Access Device (NAD) syslogs, and overloads the MnT servers resulting in loading issues. If NAD Syslogs are configured to be sent directly to MnT, session management functionality would break. NAD syslogs can be directed to external syslog servers for troubleshooting but should not be directed to MnT.

The Process Down alarm is no longer triggered when ISE Messaging Service fails on a node. When ISE Messaging Service fails on a node, all the syslogs and the Process Down alarm will be lost until the messaging service is brought back up on that node.

In this case, an administrator must look for the **Queue Link Error** alarm that will be listed in the **Alarms** dashlet on the Cisco ISE **Home** window. Click on the alarm, and a new window will open with a **Suggested Actions** section. Follow these instructions to resolve the issue.

Note If the Monitoring node is configured as the syslog server for a network device, ensure that the logging source sends the correct network access server (NAS) IP address in the following format:

<message_number>sequence_number: NAS_IP_address: timestamp: syslog_type: <message_text>

Otherwise, this might impact functionalities that depend on the NAS IP address.

Configure Syslog Purge Settings

Use this process to set local log-storage periods and to delete local logs after a certain period of time.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Local Log Settings**.

Step 2 In the **Local Log Storage Period** field, enter the maximum number of days to keep the log entries in the configuration source.

Logs may be deleted earlier than the configured **Local Log Storage Period** depending on the size of the localStore folder:

If the disk size is…	The local store size limit is…
< 100 GB	10 GB
< 250 GB	30 GB
< 400 GB	50 GB
> 400 GB	95 GB

Step 3 Click **Delete Logs Now** to delete the existing log files at any time before the expiration of the storage period.

Step 4 Click **Save**.

Cisco ISE System Logs

In Cisco ISE, system logs are collected at locations called logging targets. Targets refer to the IP addresses of the servers that collect and store logs. You can generate and store logs locally, or you can use the FTP facility to transfer them to an external server. Cisco ISE has the following default targets, which are dynamically configured in the loopback addresses of the local system:

- LogCollector—Default syslog target for the Log Collector.
- ProfilerRadiusProbe—Default syslog target for the Profiler Radius Probe.

By default, AAA Diagnostics subcategories and System Diagnostics subcategories logging targets are disabled during a fresh Cisco ISE installation or an upgrade to reduce the disk space. You can configure logging targets manually for these subcategories but local logging for these subcategories are always enabled.

You can use the default logging targets that are configured locally at the end of the Cisco ISE installation or you can create external targets to store the logs.

Note If a syslog server is configured in a distributed deployment, syslog messages are sent directly from the authenticating PSNs to the syslog server and not from the MnT node.

Related Topics

Cisco ISE Message Codes, on page 409

Configure Remote Syslog Collection Locations

You can use the web interface to create remote syslog server targets to which system log messages are sent. Log messages are sent to the remote syslog server targets in accordance with the syslog protocol standard (see RFC-3164). The syslog protocol is an unsecure UDP.

A message is generated when an event occurs. An event may be one that displays a status, such as a message displayed when exiting a program, or an alarm. There are different types of event messages generated from multiple facilities such as the kernel, mail, user level, and so on. An event message is associated with a severity level, which allows an administrator to filter the messages and prioritize it. Numerical codes are assigned to the facility and the severity level. A syslog server is an event message collector and collects event messages from these facilities. The administrator can select the event message collector to which messages will be forwarded based on their severity level.

The UDP syslog (log collector) is the default remote logging target. When you disable this logging target, it no longer functions as a log collector and is removed from the **Logging Categories** window. When you enable this logging target, it becomes a log collector in the **Logging Categories** window.

Note Any changes to the default remote logging target **SecureSyslogCollector** results in the restart of the Cisco ISE Monitoring & Troubleshooting Log Processor service.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Remote Logging Targets**.

Step 2 Click **Add**.

Step 3 Enter the required details.

Step 4 Click **Save**.

Step 5 Go to the Remote Logging Targets page and verify the creation of the new target.

The logging targets can then be mapped to each of the logging categories below. The PSN nodes send the relevant logs to the remote logging targets depending on the services that are enabled on those nodes.

- AAA Audit
- AAA Diagnostics
- Accounting
- External MDM
- Passive ID
- Posture and Client Provisioning Audit
- Posture and Client Provisioning Diagnostics
- Profiler

Logs of the following categories are sent by all nodes in the deployment to the logging targets:

- Administrative and Operational Audit
- System Diagnostics
- System Statistics

Cisco ISE Message Codes

A logging category is a bundle of message codes that describe a function, a flow, or a use case. In Cisco ISE, each log is associated with a message code that is bundled with the logging categories according to the log message content. Logging categories help describe the content of the messages that they contain.

Logging categories promote logging configuration. Each category has a name, target, and severity level that you can set, as per your application requirement.

Cisco ISE provides predefined logging categories for services, such as Posture, Profiler, Guest, AAA (authentication, authorization, and accounting), and so on, to which you can assign log targets.

For the logging category **Passed Authentications**, the option to allow local logging is disabled by default. Enabling local logging for this category will result in high utilization of operational space, and fill prrt-server.log along with the iseLocalStore.log.

If you choose to enable local logging for **Passed Authentications**, go to **Administration** > **System** > **Logging** > **Logging Categories**, click **Passed Authentications** from the category section, and check the check box against **Local Logging**.

Related Topics

Set Severity Levels for Message Codes, on page 409

Set Severity Levels for Message Codes

You can set the log severity level and choose logging targets where the logs of selected categories will be stored.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**.

Step 2 Click the radio button next to the category that you want to edit, and click **Edit**.

Step 3 Modify the required field values.

Step 4 Click **Save**.

Step 5 Go to the Logging Categories page and verify the configuration changes that were made to the specific category.

Cisco ISE Message Catalogs

You can use the Message Catalog page to view all possible log messages and the descriptions. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Message Catalog**.

The Log Message Catalog page appears, from which you can view all possible log messages that can appear in your log files. Choose **Export** to export all the syslog messages in the form of a CSV file.

See Cisco ISE Syslogs for a comprehensive list of the syslog messages sent by Cisco ISE, what they mean, and how they are recorded in local and remote targets.

Endpoint Debug Log Collector

To troubleshoot issues with a specific endpoint, you can download debug logs for that particular endpoint based on its IP address or MAC address. The logs from the various nodes in your deployment specific to that particular endpoint get collected in a single file thus helping you troubleshoot your issue quickly and efficiently. You can run this troubleshooting tool only for one endpoint at a time. The log files are listed in the GUI. You can download the logs for an endpoint from a single node or from all the nodes in your deployment.

Download Debug Logs for a Specific Endpoint

To troubleshoot issues related to a specific endpoint in your network, you can use the Debug Endpoint tool from the Admin portal. Alternatively, you can run this tool from the Authentications page. Right-click the Endpoint ID from the Authentications page and click **Endpoint Debug**. This tool provides all debug information for all services related to the specific endpoint in a single file.

Before you begin

You need the IP address or MAC address of the endpoint whose debug logs you want to collect.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **Endpoint Debug**.

Step 2 Click the **MAC Address** or **IP** radio button and enter the MAC or IP address of the endpoint.

Step 3 Check the **Automatic disable after *n* Minutes** check box if you want to stop log collection after a specified amount of time. If you check this check box, you must enter a time between 1 and 60 minutes.

The following message appears: "Endpoint Debug degrades the deployment performance. Would you like to continue?"

Step 4 Click **Continue** to collect the logs.

Step 5 Click **Stop** when you want to manually stop the log collection.

Related Topics

- Endpoint Debug Log Collector, on page 410

Collection Filters

You can configure the Collection Filters to suppress the syslog messages being sent to the monitoring and external servers. The suppression can be performed at the Policy Services Node levels based on different attribute types. You can define multiple filters with specific attribute type and a corresponding value.

Before sending the syslog messages to monitoring node or external server, Cisco ISE compares these values with fields in syslog messages to be sent. If any match is found, then the corresponding message is not sent.

Note If you configure a collection filter (**Administration** > **System** > **Logging** > **Collection Filter**) for any **Attribute** and **Filter Type**; and you have also selected the **Disable account after n days of inactivity** check box (**Administration** > **Identity Management** > **User Authentication Settings** > **Disable Account Policy**), your account might be disabled as a result of the syslog messages of successful authentication not being relayed to the monitoring node.

Configure Collection Filters

You can configure multiple collection filters based on various attribute types. It is recommended to limit the number of filters to 20. You can add, edit, or delete a collection filter.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Collection Filters**.

Step 2 Click **Add.**

Step 3 Choose the **Filter Type** from the following list:

- User Name
- MAC Address
- Policy Set Name
- NAS IP Address
- Device IP Address

Step 4 Enter the corresponding **Value** for the filter type you have selected.

Step 5 Choose the **Result** from the drop-down list. The result can be All, Passed, or Failed.

Step 6 Click **Submit.**

Related Topics

Collection Filters, on page 410
Event Suppression Bypass Filter, on page 411

Event Suppression Bypass Filter

Cisco ISE allows you to set filters to suppress some syslog messages from being sent to the Monitoring node and other external servers using the Collection Filters. At times, you need access to these suppressed log messages. Cisco ISE now provides you an option to bypass the event suppression based on a particular attribute such as username for a configurable amount of time. The default is 50 minutes, but you can configure the duration from 5 minutes to 480 minutes (8 hours). After you configure the event suppression bypass, it takes effect immediately. If the duration that you have set elapses, then the bypass suppression filter expires.

You can configure a suppression bypass filter from the Collection Filters page in the Cisco ISE user interface. Using this feature, you can now view all the logs for a particular identity (user) and troubleshoot issues for that identity in real time.

You can enable or disable a filter. If the duration that you have configured in a bypass event filter elapses, the filter is disabled automatically until you enable it again. Cisco ISE captures these configuration changes in the Change Configuration Audit Report. This report provides information on who configured an event suppression or a bypass suppression and the duration of time for which the event was suppressed or the suppression bypassed.

Cisco ISE Reports

Cisco Identity Services Engine (ISE) reports are used with monitoring and troubleshooting features to analyze trends, and, monitor system performance and network activities from a central location.

Cisco ISE collects logs and configuration data from your network. It then aggregates the data into reports for you to view and analyze. Cisco ISE provides a standard set of predefined reports that you can use and customize to fit your needs.

Cisco ISE reports are pre-configured and grouped into categories with information related to authentication, session traffic, device administration, configuration, administration, and troubleshooting.

Related Topics

Run and View Reports, on page 414
Export Reports, on page 414
Available Reports, on page 419

Report Filters

There are two types of reports, single-section and multi-section. Single-section reports contain a single grid (Radius Authentications report) and multi-section reports contain many grids (Authentications Summary report) and represent data in the form of charts and tables. The Filter drop-down menu in the single-section reports contains the **Quick Filter** and **Advanced Filter**. In the multi-section reports, you can specify only advanced filters.

Multi-section reports may contain one or more mandatory advanced filters that require your input. For example, when you click the Health Summary report (**Operations** > **Reports** > **Diagnostics** page), it displays two mandatory advanced filters—Server and Time Range. You must specify the operator command, server name, required values for both these filters, and click **Go** to generate the report. You can add new advanced filters by clicking the Plus (+) symbol. You can export multi-section reports only in the PDF format. You cannot schedule Cisco ISE multi-section reports to run and re-run at specific time or time intervals.

Note When you click a report, data for the current date is generated by default. However, some multi-section reports require mandatory input from the user apart from the time range.

By default, the Quick Filter is displayed as the first row in single-section reports. The fields may contain a drop-down list from which you can select the search criteria or may be a text box.

An Advanced Filter contains an outer criteria that contains one or more inner criteria. The outer criteria is used to specify if the search should meet All or Any specified inner criteria. The inner criteria contains one or more conditions that is used to specify the Category (Endpoint ID, Identity Group) Method (operator commands, such as Contains, Does Not Contain), and Time Range for the condition.

When using the **Quick Filter**, you can choose a date or time from the **Logged At** drop-down list to generate reports for a data set logged in the last 30 days or less. If you want to generate a report for a date or time prior to 30 days, use the **Advanced Filter** to set the required time frame in the **From** and **To** fields of the **Custom** option from the drop-down list.

Create the Quick Filter Criteria

The section describes how to create a quick filter criteria. You can create quick filter criteria for only single-section reports.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** and click the required report.

Step 2 From the **Settings** drop-down list, choose the required fields.

Step 3 In the required field, you can choose from the drop-down list or type the specific characters to filter data. The search uses the Contains operator command. For example, to filter by text that begins with "K", enter K or to filter text that has "geo" anywhere in the text, enter geo. You can also use asterisks (*), for example, the regex starting with *abc and ending with *def.

The quick filter uses the following conditions: contains, starts with, ends with, starts with or ends with, and multiple values with OR operator.

Step 4 Press **Enter**.

Create the Advanced Filter Criteria

The section describes how to create an advanced filter criteria. You can create advanced filters for single- and multi-section reports. The Filter drop-down menu in the single-section reports contains the **Quick Filter** and **Advanced Filter**. In the multi-section reports, you can specify only advanced filters.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** and click the required report.

Step 2 In the **Filters** section, from the **Match** drop-down list, choose one of the options.

a) Choose **All** to match all specified conditions.
b) Choose **Any** to match any one specified condition.

Step 3 From the **Time Range** drop-down list, choose the required category.

Step 4 From the **Operator Commands** drop-down list, choose the required command. For example, you can filter text that begins with a specific character (use Begin With), or specific characters anywhere in the text (use Contains). Or, you can choose the Logged Time and corresponding Custom option and specify the From and To date and time from the calendar to filter data.

Step 5 From the **Time Range** drop-down list, choose the required option.

Step 6 Click **Go**.

You can save a filtered report and retrieve it from the **Filter** drop-down list for future reference.

Run and View Reports

This section describes how to run, view, and navigate reports using Reports View. When you click a report, by default, data for the last seven days is generated. Each report displays 500 rows of data per page. You can specify time increments over which to display data in a report.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **ISE Reports**.

You can also navigate to the **Reports** link under each work center to view the set of reports specific to that work center.

Step 2 Click a report from the **report** categories available.

Step 3 Select one or more filters to run a report. Each report has different filters available, of which some are mandatory and some are optional.

Step 4 Enter an appropriate value for the filters.

Step 5 Click **Go**.

Related Topics

Export Reports, on page 414

Available Reports, on page 419

Reports Navigation

You can get detailed information from the reports output. For example, if you have generated a report for a period of five months, the graph and table will list the aggregate data for the report in a scale of months.

You can click a particular value from the table to see another report related to this particular field. For example, an authentication summary report will display the failed count for the user or user group. When you click the failed count, an authentication summary report is opened for that particular failed count.

Export Reports

You can only export the PDF file format of the following reports:

- Authentication Summary
- Health Summary
- RBACL Drop Summary

Note Flows for RBACL dropped packets are available only with the Cisco Catalyst 6500 series switches.

- Guest Sponsor summary
- End point Profile Changes

- Network Device Session Status

Step 1 Run a report, as described in the Running and Viewing Reports section.

Step 2 Click **Export To** in the top-right corner of the report summary page.

Step 3 Choose one of the following options:

- Repository (CSV): To export the report in CSV file format to a repository
- Local (CSV): To export the report in CSV file format to a local disk
- Local (PDF): To export the report in pdf file format to a local disk

Note
- When you select the local CSV or pdf option, only the first 500 records are exported. You can use the Repository CSV option to export all the records.
- When you export the multi-section reports using the local pdf option, only the first 100 rows are exported for each section.

My Reports

You can add preconfigured system reports and personally filtered reports to the **My Reports** section. Reports saved to the **My Reports** section retain the filters applied to them.

Step 1 On the **Reports** window (**Operations** > **Reports**), click the report that you require from the **Reports** drop-down menu displayed on the left.

Step 2 (Optional) When the selected report opens, add required filters to customize the report.

Step 3 Click the **Add to My Reports** button at the top right-hand corner of the window.

Step 4 The **Save to My Reports** dialog box opens. The name and description of the report is auto populated. You can edit these fields if needed.

Step 5 (Optional) The selected reports are saved with the applicable filters, thus, retaining their customization.

Step 6 Click **Save** to save the report. A dialog box saying that the report has been successfully saved will be displayed.

Step 7 The selected report will now appear in the **My Reports** drop-down list for easy access.

You can remove a report added to the **My Reports** section by clicking the **Remove From My Reports** button at the top right-hand corner of the window. Click **OK** in the Alert dialog box that appears and the report will be removed from your My Reports section.

Scheduling Cisco ISE Reports

You can schedule Cisco ISE reports to run and re-run at specific time or time intervals. You can also apply appropriate filters to your report of choice. You can schedule for reports to run on Cisco ISE with hourly, daily, weekly, monthly, and yearly frequency. It can also be a one-time report scheduling job. You can choose the start dates and end dates of the reports and choose the days of the week when you want to schedule the reports. You get to decide the time when the scheduled report would run.

You can also send and receive email notifications for the reports generated. These email notifications will tell you if the scheduled report has run successfully and will also contain details of the repository, time of scheduled report, and so on.

When scheduling reports with **Hourly** frequency, you can have the report run over multiple days, but the timeframe cannot spread across two days.

For example, when scheduling an hourly report from May 4, 2019, to May 8, 2019, you can set the time interval as between 6:00 a.m. and 11:00 p.m. each day, but not between 6:00 p.m. of one day and 11:00 a.m. of the next. Cisco ISE displays an error message that the time range is invalid in the latter case.

You cannot schedule the following reports:

- Authentication Summary
- Health Summary
- RBACL Drop Summary

Note Flows for RBACL dropped packets are available only with the Cisco Catalyst 6500 Series Switches.

- Guest Sponsor summary
- Endpoint Profile Changes
- Network Device Session Status

Step 1 On the **Reports** window (**Operations** > **Reports**), select the report that you want to schedule from the **Reports** drop-down menu displayed on the left.

Step 2 (Optional) When the selected report opens, apply the filters that you want to be applicable to the report.

Step 3 Click the **Schedule** button at the top right-hand corner of the window..

Step 4 The **Save as Schedule** dialog box opens.

Step 5 Fill in the details such as name, description, email, date, and time of the schedule job.

Step 6 From the **Repository** drop-down list, choose the external repository that would save the scheduled report. For more information, see “Table 1. Supportability Matrix for External Repositories” under the Backup and Restore Repositories section of the Cisco ISE Administrator Guide.

Step 7 From the **Frequency** drop-down list, choose the frequency of the schedule as required. For example, if you only need data of the last 12 hours, select the **Last 12 hours** data field while scheduling the report.

Step 8 Select a **Start Date** and **End Date** as required and click **Save**.

Step 9 All the selected filters will automatically apply to the report while scheduling it.

Step 10 You can see the created schedule and applied filters in the **Scheduled Reports** section at the bottom of the window.

You can also edit and delete scheduled reports as needed. Choose the scheduled report of your choice from the **Scheduled Reports** drop-down list (**Operations** > **Reports** > **Scheduled Reports**). Click **Edit Schedule** to make changes to your scheduled reports and click **Save**. Click **Delete Schedule** to delete your scheduled report.

Use Case: Scheduled Reports

To get the previous day's data at 12 AM on the current day, schedule the report following this procedure:

Step 1 On the **Reports** window (**Operations** > **Reports**), select the report that you want to schedule from the **Reports** drop-down menu displayed on the left.

Step 2 (Optional) When the selected report opens, apply the filters that you want to be applicable to the report.

Step 3 In this scenario, to get the data from the previous day, select the **Logged at** field and apply the **Yesterday** filter. This will return the previous day's data whenever the scheduled report runs. If you only need data of the last 12 hours, select the **Last 12 hours data**field in the **Save as Schedule** dialog box while scheduling the report.

Step 4 Click the **Schedule** button at the top right-hand corner of the window.

Step 5 The **Save as Schedule** dialog box opens.

Step 6 Fill in the details such as name, description, email, date, and time of the schedule job.

Step 7 From the **Repository** drop-down list, choose the external repository that would save the scheduled report. For more information, see "Table 1. Supportability Matrix for External Repositories" under the Backup and Restore Repositories section of the Cisco ISE Administrator Guide.

Step 8 From the **Frequency** drop-down list, choose the frequency of the schedule as required. For example, if you only need data of the last 12 hours, select the **Last 12 hours** data field while scheduling the report.

Step 9 Select a **Start Date** and **End Date** as required and click **Save**.

Step 10 All the selected filters will automatically apply to the report while scheduling it.

Step 11 You can see the created schedule and applied filters in the **Scheduled Reports** section at the bottom of the window.

Note

- Most scheduled reports are exported in .csv format. However, the scheduled reports for Radius Authentication, Radius Accounting, TACACS Authentication, TACACS Accounting, and Operations Audit are exported in a .zip folder containing .csv files.
- If an external administrator (for example: Active Directory Administrator) creates a scheduled report without filling the email-id field, no email notifications will be sent.
- An internal or external Cisco ISE user should be deleted only after deleting the scheduled reports created by that particular user to ensure that there are no active schedules running after the user is removed.
- You can save or schedule (with filters) Cisco ISE reports only from the PAN.
- A scheduled report job runs on both Primary MnT and Secondary MnT nodes. If the Primary MnT is down, the Secondary MnT executes the scheduled report job. In such a scenario, the Secondary MnT first pings the Primary MnT. Only if the ping fails, the Secondary MnT runs the scheduled export job.
- Cisco ISE 3.1 Patch 1 onwards, the date format in exported reports has changed from YYYY-MM-DD to DD-MM-YY. The time format has changed from hh:mm:ss.sss to hh:mm:ss.sss AM/PM (24 hour format to 12 hour format).

Cisco ISE Active RADIUS Sessions

Cisco ISE provides a dynamic Change of Authorization (CoA) feature for the Live Sessions that allows you to dynamically control active RADIUS sessions. You can send reauthenticate or disconnect requests to a Network Access Device (NAD) to perform the following tasks:

- Troubleshoot issues related to authentication—You can use the Session reauthentication option to follow up with an attempt to reauthenticate again. However, you must not use this option to restrict access. To restrict access, use the shutdown option.
- Block a problematic host—You can use the Session termination with port shutdown option to block an infected host that sends a lot of traffic over the network. However, the RADIUS protocol does not currently support a method for re-enabling a port that has been shut down.
- Force endpoints to reacquire IP addresses—You can use the Session termination with port bounce option for endpoints that do not have a supplicant or client to generate a DHCP request after a VLAN change.
- Push an updated authorization policy to an endpoint—You can use the Session reauthentication option to enforce an updated policy configuration, such as a change in the authorization policy on existing sessions based on the discretion of the administrator. For example, if posture validation is enabled, when an endpoint gains access initially, it is usually quarantined. After the identity and posture of the endpoint are known, it is possible to send the Session reauthentication command to the endpoint for the endpoint to acquire the actual authorization policy based on its posture.

For CoA commands to be understood by the device, it is important that you configure the options appropriately.

For CoA to work properly, you must configure the shared secret of each device that requires a dynamic change of authorization. Cisco ISE uses the shared secret configuration to request access from the device and issue CoA commands to it.

Note In this release of Cisco ISE, the maximum number of active authenticated endpoint sessions that can be displayed is limited to 100,000.

Related Topics

Change Authorization for RADIUS Sessions, on page 418

Change Authorization for RADIUS Sessions

Some Network Access Devices on your network may not send an Accounting Stop or Accounting Off packet after a reload. As a result, you might find two sessions in the Session Directory reports, one which has expired.

To dynamically change the authorization of an active RADIUS session or disconnect an active RADIUS session, be sure to choose the most recent session.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **RADIUS Livelog**.

Step 2 Switch the view to **Show Live Session**.

Step 3 Click the CoA link for the RADIUS session that you want to issue CoA and choose one of the following options:

- **SAnet Session Query**—Use this to query information about sessions from SAnet supported devices.

- **Session reauthentication**—Reauthenticate session. If you select this option for a session established on an ASA device supporting COA, this will invoke a Session Policy Push CoA.
- **Session reauthentication with last**—Use the last successful authentication method for this session.
- **Session reauthentication with rerun**—Run through the configured authentication method from the beginning.

  Note **Session reauthentication with last** and **Session reauthentication with rerun** options are not currently supported in Cisco IOS software.

- **Session termination**—Just end the session. The switch reauthenticates the client in a different session.
- **Session termination with port bounce**—Terminate the session and restart the port.
- **Session termination with port shutdown**—Terminate the session and shutdown the port.

Step 4 Click **Run** to issue CoA with the selected reauthenticate or terminate option.

If your CoA fails, it could be one of the following reasons:

- Device does not support CoA.
- Changes have occurred to the identity or authorization policy.
- There is a shared secret mismatch.

Available Reports

The following table lists the preconfigured reports, grouped according to their category. Descriptions of the report functionality and logging category are also provided.

To generate syslogs for a logging category, set its **Log Severity Level** to **Info**:

- In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**.
- Click the logging category for which syslogs must be generated.
- From the **Log Severity Level** drop-down list, choose **Info**.
- Click **Save**.

Note In Cisco ISE Release 2.6 and later, users with IPv6 addresses will have the following events logged in the audit reports—login/logout, password change, and operational changes made. In Administrator Logins, User Change Password Audit, and Operations Audit reports, you can filter logs by IPv4 and IPv6 records.

Report Name	Description	Logging Category
Audit		

Report Name	Description	Logging Category
Adaptive Network Control Audit	The Adaptive Network Control Audit report is based on RADIUS accounting. It displays historical reporting of all the network sessions for each endpoint.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and click **Passed Authentications** and **RADIUS Accounting**.
Administrator Logins	The Administrator Logins report provides information about all the GUI-based administrator login events as well as successful CLI login events.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and click **Administrative and Operational Audit**.
Change Configuration Audit	The Change Configuration Audit report provides details about configuration changes within a specified time period. If you need to troubleshoot a feature, this report can help you determine if a recent configuration change contributed to the problem.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and click **Administrative and Operational Audit**.

Report Name	Description	Logging Category
Data Purging Audit	The Data Purging Audit report records when the logging data is purged. This report reflects two sources of data purging. At 4 a.m. daily, Cisco ISE checks whether there are any logging files that meet the criteria you have set on the **Administration > Maintenance > Data Purging** window. If yes, the files are deleted and recorded in this report. Additionally, Cisco ISE continually maintains a maximum of 80 percent used storage space (threshold) for the log files. Every hour, Cisco ISE verifies this percentage and deletes the oldest data until this threshold is reached again. This information is also recorded in this report. If there is high disk space utilization, an alert message stating `ISE Monitor node(s) is about to exceed the maximum amount allocated` is displayed at 80 percent of the threshold, that is 60 percent of total disk space. Subsequently, an alert message stating `ISE Monitor node(s) has exceeded the maximum amount allocated` is displayed at 90 percent of the threshold, that is 70 percent of the total disk space.	—
Endpoints Purge Activities	The Endpoints Purge Activities report enables a user to review the history of endpoints purge activities. This report requires that the Profiler logging category is enabled. (Note that this category is enabled by default.)	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and click **Profiler**.

Report Name	Description	Logging Category
Internal Administrator Summary	The Internal Administrator Summary report enables you to verify the entitlement of administrator users. From this report, you can also access the Administrator Logins and Change Configuration Audit reports, which enables you to view these details for each administrator.	—
Operations Audit	The Operations Audit report provides details about any operational changes, such as, running backups, registering a Cisco ISE node, or restarting an application.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and click **Administrative and Operational Audit**.
pxGrid Administrator Audit	The pxGrid Administrator Audit report provides details of the pxGrid administration actions, such as client registration, client deregistration, client approval, topic creation, topic deletion, publisher-subscriber addition, and publisher-subscriber deletion on the Primary PAN. Every record has the name of the administrator who has performed the action on the node. You can filter the pxGrid Administrator Audit report based on the administrator and message criteria.	—
Secure Communications Audit	The Secure Communications Audit report provides auditing details about security-related events in Cisco ISE Admin CLI, which includes authentication failures, possible break-in attempts, SSH logins, failed passwords, SSH logouts, invalid user accounts, and so on.	—

Report Name	Description	Logging Category
User Change Password Audit	The User Change Password Audit report displays verification about employees' password changes.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and click **Administrative and Operational Audit**.
Trustsec Audit	TrustSec Audit logs contains: • Management (Create, Rename, Update, and Delete) of TrustSec components. • Deployments of SGACLs and SGTs to TrustSec-enabled NADs • TrustSec Sessions. If Cisco ISE is integrated with Catalyst Center, and SD Access is managed by Catalyst Center, then this log is empty.	—
Device Administration		
TACACS Authentication Summary	The TACACS Authentication Summary report provides details about the most common authentications, and the reason for authentication failures.	—
TACACS Accounting	The TACACS Accounting report provides accounting details for a device session. It displays information related to the generated and logged time of the users and devices.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and select TACACS Accounting.
Top N Authentication by Failure Reason	The Top N Authentication by Failure Reason report displays the total number of authentications by failure reason for a specific period, based on the selected parameters.	—

Report Name	Description	Logging Category
Top N Authentication by Network Device	The Top N Authentication by Network Device report displays the number of passed and failed authentications by network device name for a specific period, based on the selected parameters.	—
Top N Authentication by User	The Top N Authentication by User report displays the number of passed and failed authentications by the user name for the specific period based on the selected parameters.	—
Diagnostics		
AAA Diagnostics	The AAA Diagnostics report provides details of all the network sessions between Cisco ISE and users. If users cannot access the network, you can review this report to identify trends and identify whether the issue is isolated to a particular user or indicative of a more widespread problem. **Note** Sometimes ISE will silently drop the Accounting Stop request of an endpoint if user authentication is in progress. However, ISE starts acknowledging all the accounting requests after user authentication is completed.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and select the following logging categories: **Policy Diagnostics**, **Identity Stores Diagnostics**, **Authentication Flow Diagnostics**, and **RADIUS Diagnostics**.

Report Name	Description	Logging Category
AD Connector Operations	The AD Connector Operations report provides log of operations performed by the AD Connector, such as Cisco ISE Server password refresh, Kerberos tickets management, DNS queries, DC discovery, LDAP, RPC Connections management, and so on. If some AD failures are encountered, you can review the details in this report to identify the possible causes.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and select **AD Connector**.
Endpoint Profile Changes	The Top Authorization by Endpoint (MAC address) report displays how many times each endpoint MAC address was authorized by Cisco ISE to access the network.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and select **Passed Authentications** and **Failed Attempts**.
Health Summary	The Health Summary report provides details similar to the Dashboard. However, the Dashboard only displays data for the past 24 hours. Also, you can review more historical data using this report. You can evaluate this data to see consistent patterns in data. For example, you would expect heavier CPU usage when most employees start their work days. If you see inconsistencies in these trends, you can identify potential problems. The CPU Usage table lists the percentage of CPU usage for the different Cisco ISE functions. The output of the **show cpu usage** CLI command is presented in this table and you can correlate these values with the issues in your deployment to identify possible causes.	—

Report Name	Description	Logging Category
ISE Counters	The ISE Counters report lists the threshold values for various attributes. The values for these different attributes are collected at different intervals and the data is presented in a tabular format; one at 5-minute interval and another after 5 minutes. You can evaluate this data to see the trend, and if you find values that are higher than the threshold, you can correlate this information with the issues in your deployment to identify possible causes. By default, Cisco ISE collects the values for these attributes. You can choose to disable this data collection from the Cisco ISE CLI using the **application configure ise** command. Choose **option 14** to enable or disable counter attribute collection.	—
Key Performance Metrics	The Key Performance Metrics report provides statistical information about the number of endpoints that connect to your deployment and the amount of RADIUS requests that are processed by each of the PSNs on an hourly basis. This report lists the average load on the server, average latency per request, and the average transactions per second.	—

Report Name	Description	Logging Category
Misconfigured NAS	The Misconfigured NAS report provides information about NADs with inaccurate accounting frequency, typically when sending accounting information frequently. If you have taken corrective actions and fix the misconfigured NADs, the report displays fixed acknowledgment in the report. **Note** **RADIUS Suppression** should be enabled to run this report.	—
Misconfigured Supplicants	The Misconfigured Supplicants report provides a list of misconfigured supplicants along with the statistics because of failed attempts that are performed by a specific supplicant. If you have taken corrective actions and fix the misconfigured supplicant, the report displays fixed acknowledgment in the report. **Note** **RADIUS Suppression** should be enabled to run this report.	—
Network Device Session Status	The Network Device Session Status Summary report enables you to display switch configuration without logging in to the switch directly. Cisco ISE accesses these details using an SNMP query and requires that your network devices are configured with SNMP v1 or v2c. If a user is experiencing network issues, this report can help you identify if the issue is related to switch configuration or with Cisco ISE.	—

Report Name	**Description**	**Logging Category**
OCSP Monitoring	The OCSP Monitoring Report specifies the status of the Online Certificate Status Protocol (OCSP) services. It identifies whether Cisco ISE can successfully contact a certificate server, and provides certificate status auditing. It also provides a summary of all the OCSP certificate-validation operations performed by Cisco ISE. It retrieves information related to the good and revoked primary and secondary certificates from the OCSP server. Cisco ISE caches the responses and utilizes them for generating subsequent OCSP Monitoring Reports. In the event the cache is cleared, it retrieves information from the OCSP server.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and select **System Diagnostics**.
RADIUS Errors	The RADIUS Errors report enables you to check for RADIUS Requests Dropped (authentication or accounting requests that are discarded from unknown Network Access Device), EAP connection time outs, and unknown NADs. **Note** You can view the report only for the past 5 days.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and select **Failed Attempts**.

Report Name	Description	Logging Category
System Diagnostics	The System Diagnostic report provides details about the status of the Cisco ISE nodes. If a Cisco ISE node is unable to register, you can review this report to troubleshoot the issue. This report requires that you first enable several diagnostic logging categories. Collecting these logs can negatively impact Cisco ISE performance. So, these categories are not enabled by default, and you should enable them just long enough to collect the data. Otherwise, they are automatically disabled after 30 minutes.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and select the following logging categories: **Internal Operations Diagnostics**, **Distributed Management**, and **Administrator Authentication and Authorization**.
Endpoints and Users		
Agentless Posture	Lists all the endpoints that ran Agentless posture.	—
Authentication Summary	The Authentication Summary report is based on the RADIUS authentications. It enables you to identify the most common authentications and the reason for authentication failures, if any. For example, if one Cisco ISE server is handling significantly more authentications than others, you might want to reassign users to different Cisco ISE servers to better balance the load. **Note** Because the Authentication Summary report or dashboard collects and displays the latest data corresponding to failed or passed authentications, the contents of the report appear after a delay of a few minutes.	—

Report Name	Description	Logging Category
Client Provisioning	The Client Provisioning report indicates the client provisioning agents applied to particular endpoints. You can use this report to verify the policies applied to each endpoint, and in turn, use this to verify whether the endpoints have been correctly provisioned. **Note** The MAC address of an endpoint is not displayed in the **Endpoint ID** column if the endpoint does not connect with ISE (no session is established), or if a Network Address Translation (NAT) address is used for the session.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and select **Posture and Client Provisioning Audit** and **Posture and Client Provisioning Diagnostics**.
Current Active Sessions	The Current Active Sessions report enables you to export a report with details about who is on the network within a specified time period. If a user isn't getting network access, you can see whether the session is authenticated or terminated, or if there is another problem with the session.	—
Endpoint Scripts Provisioning Summary	The **Endpoint Scripts Provisioning Summary** window displays details of jobs run through the **Endpoint Scripts** window over the last 30 days.	—

Report Name	Description	Logging Category
External Mobile Device Management	The External Mobile Device Management report provides details about integration between Cisco ISE and the external Mobile Device Management (MDM) server. You can use this report to see which endpoints have been provisioned by the MDM server without logging into the MDM server directly. It also displays information such as registration and MDM-compliance status.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and select MDM.
Passive ID	The Passive ID report enables you to monitor the state of WMI connection to the domain controller and gather statistics related to it (such as amount of notifications received, amount of user login/logouts per second etc.) **Note** Sessions authenticated by this method do not have authentication details in the report.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and select Identity Mapping.
Manual Certificate Provisioning	The Manual Certificate Provisioning report lists all the certificates that are provisioned manually via the certificate provisioning portal.	—
Posture Assessment by Condition	The Posture Assessment by Condition report enables you to view records based on the posture policy condition configured in ISE to validate that the most up-to-date security settings or applications are available on client machines.	—

Report Name	Description	Logging Category
Posture Assessment by Endpoint	The Posture Assessment by Endpoint report provides detailed information, such as the time, status, and PRA Action, of an endpoint. You can click **Details** to view further information of an endpoint. **Note** The Posture Assessment by Endpoint report does not provide posture policy details of applications and hardware attributes of an endpoint. You can view this information only in the Context Visibility page.	—

Report Name	Description	Logging Category
Posture Script Remediation	Posture Script Remediation is used to check the status of the remediation script execution. The status is one of the following: • Remediation script execution was successful. • Remediation was attempted, and the script exited with failure. • Remediation was not attempted (default). • Remediation attempt failed. The script failed an integrity check as the policy included might have been tampered with. • Remediation attempt failed. Client failed to download the script. • Remediation attempt failed. The script failed an integrity test as the script might be corrupt or has been tampered with. • Remediation attempt failed. The script was executed but did not exit in time (timeout). • Remediation attempt failed. A generic internal system failure occurred. • Remediation attempt failed. The script type is not supported. • Remediation attempt failed. Failure with launching the script. • Certificate verification failure. Client could not verify the server certificate presented by Cisco ISE.	—

Report Name	**Description**	**Logging Category**
Profiled Endpoints Summary	The Profiled Endpoints Summary report provides profiling details about endpoints that are accessing the network. **Note** For endpoints that do not register a session time, such as a Cisco IP-Phone, the term Not Applicable is shown in the Endpoint session time field.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and select Profiler.
RADIUS Accounting	The RADIUS Accounting report identifies how long users have been on the network. If users are losing network access, you can use this report to identify whether Cisco ISE is the cause of the network connectivity issues. **Note** Radius accounting interim updates are included in the RADIUS Accounting report if the interim updates contain information about the changes to the IPv4 or IPv6 addresses for the given sessions.	
RADIUS Authentications	The RADIUS Authentications report enables you to review the history of authentication failures and successes. If users cannot access the network, you can review the details in this report to identify possible causes.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and select these logging categories: Passed Authentications and Failed Attempts.
Registered Endpoints	The Registered Endpoints report displays all personal devices registered by employees.	—

Report Name	Description	Logging Category
Rejected Endpoints	The Rejected Endpoints report lists all rejected or released personal devices that are registered by employees.	—
Supplicant Provisioning	The Supplicant Provisioning report provides details about the supplicants provisioned to employee's personal devices.	Posture and Client Provisioning Audit
Top Authorizations by Endpoint	The Top Authorization by Endpoint (MAC address) report displays how many times each endpoint MAC address was authorized by Cisco ISE to access the network.	Passed Authentications, Failed Attempts
Top Authorizations by User	The Top Authorization by User report displays how many times each user was authorized by Cisco ISE to access the network.	Passed Authentications, Failed Attempts
Top N Authentication by Access Service	The Top N Authentication by Access Service report displays the number of passed and failed authentications by the access service type for the specific period based on the selected parameters.	—
Top N Authentication by Failure Reason	The Top N Authentication by Failure Reason report displays the total number of authentications by failure reason for the specific period based on the selected parameters.	—
Top N Authentication by Network Device	The Top N Authentication by Network Device report displays the number of passed and failed authentications by the network device name for the specific period based on the selected parameters.	—

Report Name	Description	Logging Category
Top N Authentication by User	The Top N Authentication by User report displays the number of passed and failed authentications by the user name for the specific period based on the selected parameters.	—
Guest		
AUP Acceptance Status	The AUP Acceptance Status report provides details of AUP acceptances from all the Guest portals.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and select Guest.
Guest Accounting	The Guest Accounting report is a subset of the RADIUS Accounting report. All users assigned to the Activated Guest or Guest identity groups appear in this report.	—

Report Name	Description	Logging Category
Primary Guest Report	The Primary Guest Report combines data from various Guest Access reports and enables you to export data from different reporting sources. The Primary Guest report also provides details about the websites that guest users are visiting. You can use this report for security auditing purposes to demonstrate when guest users accessed the network and what they did on it. You must also enable HTTP inspection on the network access device (NAD) used for guest traffic. This information is sent back to Cisco ISE by the NAD. To check when the clients reach the maximum simultaneous sessions limit, from the Admin portal, choose **Administration > System > Logging > Logging Categories** and do the following: **1.** Increase the log level of "Authentication Flow Diagnostics" logging category from WARN to INFO. **2.** Change LogCollector Target from Available to Selected under the "Logging Category" of AAA Diagnostics.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and select Passed Authentications.
My Devices Login and Audit	The My Devices Login and Audit report provides details about the login activities and the operations performed by the users on the devices in My Devices Portal.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and select My Devices.

Report Name	Description	Logging Category
Sponsor Login and Audit	The Sponsor Login and Audit report provides details of guest users' login, add, delete, enable, suspend and update operations and the login activities of the sponsors at the sponsors portal. If guest users are added in bulk, they are visible under the column 'Guest Users.' This column is hidden by default. On export, these bulk users are also present in the exported file.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and select Guest.
SXP		
SXP Binding	The SXP Binding report provides information about the IP-SGT bindings that are exchanged over SXP connection.	—
SXP Connection	You can use this report to monitor the status of an SXP connection and gather information related to it, such as peer IP, SXP node IP, VPN name, SXP mode, and so on.	—
Trustsec		

Report Name	Description	Logging Category
RBACL Drop Summary	The RBACL Drop Summary report is specific to the TrustSec feature, which is available only with an Advanced Cisco ISE license. This report also requires that you configure the network devices to send NetFlow events for dropped events to Cisco ISE. If a user violates a particular policy or access, packets are dropped and indicated in this report. **Note** Flows for RBACL dropped packets are available only with the Cisco Catalyst 6500 series switches.	—
Top N RBACL Drops By User	The Top N RBACL Drops By User report is specific to the TrustSec feature, which is available only with an Advanced Cisco ISE license. This report also requires that you configure the network devices to send NetFlow events for dropped events to Cisco ISE. This report displays policy violations (based on packet drops) by specific users. **Note** Flows for RBACL dropped packets are available only with the Cisco Catalyst 6500 series switches.	—
TrustSec ACI	This report lists the SGTs and SXP mappings that are synchronized with the IEPGs, EEPGs, endpoints, and subnet configuration of APIC. These details are displayed only if the TrustSec APIC integration feature is enabled.	—

Report Name	Description	Logging Category
TrustSec Deployment Verification		—

Report Name	Description	Logging Category
	You can use this report to verify whether the latest TrustSec policies are deployed on all network devices or if there are any discrepancies between the policies configured in Cisco ISE and the network devices. Click the **Details** icon to view the results of the verification process. You can view the following details: • When the verification process started and completed • Whether the latest TrustSec policies are successfully deployed on the network devices. You can also view the names and IP addresses of the network devices on which the latest TrustSec policies are deployed. • Whether if there are any discrepancies between the policies configured in Cisco ISE and the network devices. It displays the device name, IP address, and the corresponding error message for each policy difference. You can view the TrustSec Deployment Verification alarms in the **Alarms** dashlet (under **Work Centers** > **TrustSec** > **Dashboard** and **Home** > **Summary**). **Note** • The time taken for reporting depends on the number of network devices and TrustSec groups in your deployment.	

Report Name	Description	Logging Category
	• The error message length in the TrustSec Deployment Verification report is currently limited to 480 characters. Error messages with more than 480 characters will be truncated and only the first 480 characters will be displayed in the report.	
Trustsec Policy Download	This report lists the requests sent by the network devices for policy (SGT/SGACL) download and the details sent by ISE. If the Workflow mode is enabled, the requests can be filtered for production or staging matrix.	To view this report, you must do the following: **1.** In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**. **2.** Choose **AAA Diagnostics** > **RADIUS Diagnostics**. **3.** Set the Log Severity Level to DEBUG for RADIUS Diagnostics.
Threat Centric NAC Service		
Adapter Status	The Adapter Status report displays the status of the threat and vulnerability adapters.	—
COA Events	When a vulnerability event is received for an endpoint, Cisco ISE triggers CoA for that endpoint. The CoA Events report displays the status of these CoA events. It also displays the old and new authorization rules and the profile details for these endpoints.	—

Report Name	Description	Logging Category
Threat Events	The Threat Events report provides a list of all the threat events that Cisco ISE receives from the various adapters that you have configured.	—
Vulnerability Assessment	The Vulnerability Assessment report provides information about the assessments that are happening for your endpoints. You can view this report to check if the assessment is happening based on the configured policy.	—

RADIUS Live Logs

The following table describes the fields in the Live logs window that displays the recent RADIUS authentications. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **RADIUS** > **Live Logs**. Note that you can view the RADIUS live logs only in the Primary PAN.

Table 47: RADIUS Live Logs

Field Name	Description
Time	Shows the time at which the log was received by the monitoring and troubleshooting collection agent. This column is required and cannot be deselected.
Status	Shows if the authentication succeeded or failed. This column is mandatory and cannot be deselected. Green is used to represent passed authentications. Red is used to represent failed authentications.
Details	Clicking the icon under the **Details** column opens the **Accounting Detail** report if an accounting event is processed for that session. If the session is in authenticated state, **Authentication Detail** report is displayed when you click the icon under the **Details** column. The **Response Time** in the **Authentication Detail** report is the total time taken by Cisco ISE to process the authentication flow. For example, if authentication consists of three roundtrip messages that took 300 ms for the initial message, 150 ms for the next message, and 100 ms for the last, **Response Time** is 300 + 150 + 100 = 550 ms. **Note** You cannot view the details for endpoints that are active for more than 7 days. You will see a window with the following message when you click the **Details** icon for endpoints that are active for more than 7 days: `No Data available for this record. Either the data is purged or authentication for this session record happened a week ago. Or if this is an 'PassiveID' or 'PassiveID Visibility' session, it will not have authentication details on ISE but only the session.`

Field Name	Description
Repeat Count	Shows the number of time the authentication requests were repeated in the last 24 hours, without any change in the context of identity, network devices, and authorization.
Identity	Shows the logged in username that is associated with the authentication. If the username is not present in any ID Store, it is displayed as `INVALID`. If the authentication fails due to any other reason, it is displayed as `USERNAME`. **Note** This is applicable only for users. This is not applicable for MAC addresses. To aid debugging, you can force Cisco ISE to display the invalid usernames. To do this, check the **Disclose Invalid Usernames** check box under **Administration** > **System** > **Settings** > **Security Settings**. You can also configure the **Disclose Invalid Usernames** option to time out, so that you do not have to manually turn it off.
Endpoint ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.
Endpoint Profile	Shows the type of endpoint that is profiled, for example, profiled to be an iPhone, Android, MacBook, Xbox, and so on.
Authentication Policy	Shows the name of the policy selected for specific authentication.
Authorization Policy	Shows the name of the policy selected for specific authorization.
Authorization Profiles	Shows the authorization profile that was used for authentication.
IP Address	Shows the IP address of the endpoint device.
Network Device	Shows the IP address of the Network Access Device.
Device Port	Shows the port number at which the endpoint is connected.
Identity Group	Shows the identity group that is assigned to the user or endpoint, for which the log was generated.
Posture Status	Shows the status of posture validation and details on the authentication.
Server	Indicates the policy service from which the log was generated.
MDM Server Name	Shows the name of the MDM server.
Event	Shows the event status.
Failure Reason	Shows the detailed reason for failure, if the authentication failed.
Auth Method	Shows the authentication method that is used by the RADIUS protocol, such as Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2), IEE 802.1x or dot1x, and so on.

Field Name	Description
Authentication Protocol	Shows the authentication protocol used, such as Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol (EAP), and so on.
Security Group	Shows the group that is identified by the authentication log.
Session ID	Shows the session ID.

Note In the **RADIUS Live Logs** and **TACACS+ Live Logs** window, a Queried PIP entry appears for the first attribute of each policy authorization rule. If all the attributes within the authorization rule are related to a dictionary that was already queried for previous rules, no additional Queried PIP entry appears.

You can do the following in the RADIUS **Live Logs** window:

- Export the data in CSV or PDF format.
- Show or hide the columns based on your requirements.
- Filter the data using the quick or custom filter. You can also save your filters for later use.
- Rearrange the columns and adjust the width of the columns.
- Sort the column values.

Note All the user customizations are stored as user preferences.

Authentication Latency

Authentication Latency is the average response time of the RADIUS authentication process from the time authetication process is initiated. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Dashboard** > **System Summary** dashlet..

You can select the following authentication latency timeframe from the drop-down list:

- **60 mins:** This option gives you the authentication latency for the authentication that was initiated in last 60 mins.
- **12 hrs:** This option gives you the authentication latency for the authentication process that was initiated in last 24 hrs.

The response time that is displayed is in millisecond (ms). To view a detailed report of authentication latenty, click on the latest log in the **Live Logs** window. To view this window, click the **Menu** icon (☰) and choose **Operations** > **RADIUS**.

RADIUS Live Sessions

The following table describes the fields in the RADIUS **Live Sessions** window, which displays live authentications. To view this window, click the **Menu** icon (☰) and chooseYou can view the RADIUS live sessions only in the Primary PAN.

Table 48: RADIUS Live Sessions

Field Name	Description
Initiated	Shows the timestamp when the session was initiated.
Updated	Shows the timestamp when the session was last updated because of a change.
Account Session Time	Shows the time span (in seconds) of a user's session.
Session Status	Shows the current status of an endpoint device.
Action	Click the **Actions** icon to reauthenticate an active RADIUS session or disconnect an active RADIUS session.
Repeat Count	Shows the number of times a user or endpoint is reauthenticated.
Endpoint ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.
Identity	Shows the username of an endpoint device.
IP Address	Shows the IP address of an endpoint device.
Audit Session ID	Shows a unique session identifier.
Account Session ID	Shows a unique ID provided by a network device.
Endpoint Profile	Shows the endpoint profile for a device.
Posture Status	Shows the status of posture validation and details of the authentication.
Security Group	Shows the group that is identified by the authentication log.
Server	Indicates the Policy Service node from which the log was generated.
Auth Method	Shows the authentication method that is used by the RADIUS protocol, such as Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), IEE 802.1x or dot1x, and so on.
Authentication Protocol	Shows the authentication protocol used, such as Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol (EAP), and so on.
Authentication Policy	Shows the name of the policy selected for specific authentication.
Authorization Policy	Shows the name of the policy selected for specific authorization.

Field Name	Description
Authorization Profiles	Shows an authorization profile that was used for authentication.
NAS IP Address	Shows the IP address of a network device.
Device Port	Shows the connected port to a network device.
PRA Action	Shows the periodic reassessment action taken on a client after it is successfully postured for compliance on your network.
ANC Status	Adaptive Network Control status of a device as **Quarantine, Unquarantine**, or **Shutdown**.
WLC Roam	Shows the boolean (Y/N) used to track if an endpoint has been handed off during roaming, from one Wireless Lan Controller (WLC) to another. It has the value of cisco-av-pair=nas-update =Y or N. **Note** Cisco ISE relies on the nas-update=true attribute from WLC to identify whether the session is in roaming state. When the original WLC sends an accounting stop attribute with nas-update=true, the session is not deleted in ISE to avoid reauthentication. If roaming fails, ISE clears the session after five days of inactivity.
Packets In	Shows the number of packets received.
Packets Out	Shows the number of packets sent.
Bytes In	Shows the number of bytes received.
Bytes Out	Shows the number of bytes sent.
Session Source	Indicates whether it is a RADIUS session or a Passive ID session.
User Domain Name	Shows the registered DNS name of a user.
Host Domain Name	Shows the registered DNS name of a host.
User NetBIOS Name	Shows the NetBIOS name of a user.
Host NetBIOS Name	Shows the NetBIOS name of a host.
License Type	Shows the type of license used.
License Details	Shows the license details.

Field Name	Description
Provider	Endpoint events are learned from different syslog sources. These syslog sources are referred to as providers. • Windows Management Instrumentation (WMI): WMI is a Windows service that provides a common interface and object model to access management information about operating system, devices, applications, and services. • Agent: A program that runs on a client on behalf of the client or another program. • Syslog: A logging server to which a client sends event messages. • REST: A client is authenticated through a terminal server. The TS Agent ID, Source Port Start, Source Port End, and Source First Port values are displayed for this syslog source. • Span: Network information is discovered using span probes. • DHCP: DHCP event. • Endpoint **Note** When two events from different providers are learned or obtained from an endpoint session, the providers are displayed as comma-separated values in the **Live Sessions** window.
MAC Address	Shows the MAC address of a client.
Endpoint Check Time	Shows the time at which an endpoint was last checked by the endpoint probe.
Endpoint Check Result	Shows the result of an endpoint probe. The possible values are: • Unreachable • User Logout • Active User
Source Port Start	(Values are displayed only for the REST provider) Shows the first port number in a port range.
Source Port End	(Values are displayed only for the REST provider) Shows the last port number in a port range.
Source First Port	(Values are displayed only for the REST provider) Shows the first port allocated by the Terminal Server Agent. A Terminal Server refers to a server or network device that allows multiple endpoints to connect to it without a modem or network interface and facilities the connection of the multiple endpoints to a LAN network. The multiple endpoints appear to have the same IP address, and therefore, it is difficult to identify the IP address of a specific user. Consequently, to identify a specific user, a Terminal Server Agent is installed in the server, which allocates a port range to each user. This helps create an IP address-port user mapping.

Field Name	Description
TS Agent ID	(Values are displayed only for the REST provider) Shows the unique identity of the Terminal Server Agent that is installed on an endpoint.
AD User Resolved Identities	(Values are displayed only for AD user) Shows the potential accounts that matched.
AD User Resolved DNs	(Values are displayed only for AD user) Shows the Distinguished Name of AD user, for example, CN=chris,CN=Users,DC=R1,DC=com

TACACS Live Logs

The following table describes the fields in the TACACS Live Logs window that displays the TACACS+ AAA details. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **TACACS** > **Live Logs**. You can view the TACACS live logs only in the Primary PAN.

Table 49: TACACS Live Logs

Field Name	Usage Guidelines
Generated Time	Shows the syslog generation time based on when a particular event was triggered.
Logged Time	Shows the time when the syslog was processed and stored by the Monitoring node. This column is mandatory and cannot be deselected.
Status	Shows if the authentication succeeded or failed. This column is required and cannot be deselected. Green is used to represent passed authentications. Red is used to represent failed authentications.
Details	Brings up a report when you click the magnifying glass icon, allowing you to drill down and view more detailed information about the selected authentication scenario. This column is required and cannot be deselected.
Session Key	Shows the session keys (found in the EAP success or EAP failure messages) returned by ISE to the network device.
Username	Shows the user name of the device administrator. This column is required and cannot be deselected.
Type	Consists of two Types—Authentication and Authorization. Shows names of users who have passed or failed authentication, authorization, or both. This column is mandatory and cannot be deselected.
Authentication Policy	Shows the name of the policy selected for specific authentication.
Authorization Policy	Shows the name of the policy selected for specific authorization.
ISE Node	Shows the name of the ISE node through which the access request is processed.

Field Name	Usage Guidelines
Network Device Name	Shows the names of network devices.
Network Device IP	Shows the IP addresses of network devices whose access requests are processed.
Network Device Groups	Shows the name of corresponding network device groups to which a network device belongs.
Device Type	Shows the device type policy that is used to process access requests from different network devices.
Location	Shows the location-based policy that is used to process access requests from network devices.
Device Port	Shows the device port number through which the access request is made.
Failure Reason	Shows the reason for rejecting an access request that is made by a network device.
Remote Address	Shows the IP address, MAC address, or any other string that uniquely identifies the end station.
Matched Command Set	Shows the MatchedCommandSet attribute value if it is present, or an empty value if the MatchedCommandSet attribute value is empty or the attribute itself does not exist in the syslog.
Shell Profile	Shows the privileges that were granted to a device administrator for executing commands on the network device.

You can do the following in the **TACACS Live Logs** window:

- Export the data in CSV or PDF format.
- Show or hide the columns based on your requirements.
- Filter the data using the quick or custom filter. You can also save your filters for later use.
- Rearrange the columns and adjust the width of the columns.
- Sort the column values.

Note All the user customizations are stored as user preferences.

Export Summary

You can view the details of the reports exported by all the users in the last seven days, along with the status. The export summary includes both the manual and scheduled reports. The **Export Summary** window is automatically refreshed every two minutes. Click the **Refresh** icon to refresh the **Export Summary** window manually.

The super admin can cancel the export that is **In-Progess** or in **Queued** state. Other users are allowed only to cancel the export process that they have initiated.

By default, only three manual export of reports can run at a given point of time; the remaining triggered manual export of reports are queued. There are no such limits for the scheduled export of reports.

Note All the reports in the queued state are scheduled again and the reports in the **In-Progress** or **Cancellation-in-progress** state are marked as failed when the Cisco ISE server is restarted. If the primary MnT node is down, the scheduled report export job runs on secondary MnT node.

The following table describes the fields in the **Export Summary** window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Export Summary**.

Table 50: Export Summary

Field Name	Description
Report Exported	Displays the name of the report.
Exported By	Shows the role of the user who initiated the export process.
Scheduled	Shows whether the report export is a scheduled one.
Triggered On	Shows the time at which the export process has been triggered in the system.
Repository	Displays the name of the repository where the exported data will be stored.
Filter Parameters	Shows the filter parameters selected while exporting the report.
Status	Shows the status of the exported reports. It can be one of the following: • Queued • In-progress • Completed • Cancellation-in-progress • Cancelled • Failed • Skipped **Note** Failed status indicates the reason for failure. Skipped status indicates that the scheduled export of reports is skipped because the primary MnT node is down.

You can do the following in the **Export Summary** window:

- Show or hide the columns based on your requirements.
- Filter the data using quick or custom filter. You can also save your filters for later use.
- Rearrange the columns and adjust the width of the columns.

RADIUS Live Logs

The following table describes the fields in the Live logs window that displays the recent RADIUS authentications. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **RADIUS** > **Live Logs**. Note that you can view the RADIUS live logs only in the Primary PAN.

Table 51: RADIUS Live Logs

Field Name	Description
Time	Shows the time at which the log was received by the monitoring and troubleshooting collection agent. This column is required and cannot be deselected.
Status	Shows if the authentication succeeded or failed. This column is mandatory and cannot be deselected. Green is used to represent passed authentications. Red is used to represent failed authentications.
Details	Clicking the icon under the **Details** column opens the **Accounting Detail** report if an accounting event is processed for that session. If the session is in authenticated state, **Authentication Detail** report is displayed when you click the icon under the **Details** column. The **Response Time** in the **Authentication Detail** report is the total time taken by Cisco ISE to process the authentication flow. For example, if authentication consists of three roundtrip messages that took 300 ms for the initial message, 150 ms for the next message, and 100 ms for the last, **Response Time** is 300 + 150 + 100 = 550 ms. **Note** You cannot view the details for endpoints that are active for more than 7 days. You will see a window with the following message when you click the **Details** icon for endpoints that are active for more than 7 days: `No Data available for this record. Either the data is purged or authentication for this session record happened a week ago. Or if this is an 'PassiveID' or 'PassiveID Visibility' session, it will not have authentication details on ISE but only the session.`
Repeat Count	Shows the number of time the authentication requests were repeated in the last 24 hours, without any change in the context of identity, network devices, and authorization.
Identity	Shows the logged in username that is associated with the authentication. If the username is not present in any ID Store, it is displayed as `INVALID`. If the authentication fails due to any other reason, it is displayed as `USERNAME`. **Note** This is applicable only for users. This is not applicable for MAC addresses. To aid debugging, you can force Cisco ISE to display the invalid usernames. To do this, check the **Disclose Invalid Usernames** check box under **Administration** > **System** > **Settings** > **Security Settings**. You can also configure the **Disclose Invalid Usernames** option to time out, so that you do not have to manually turn it off.
Endpoint ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.

Field Name	Description
Endpoint Profile	Shows the type of endpoint that is profiled, for example, profiled to be an iPhone, Android, MacBook, Xbox, and so on.
Authentication Policy	Shows the name of the policy selected for specific authentication.
Authorization Policy	Shows the name of the policy selected for specific authorization.
Authorization Profiles	Shows the authorization profile that was used for authentication.
IP Address	Shows the IP address of the endpoint device.
Network Device	Shows the IP address of the Network Access Device.
Device Port	Shows the port number at which the endpoint is connected.
Identity Group	Shows the identity group that is assigned to the user or endpoint, for which the log was generated.
Posture Status	Shows the status of posture validation and details on the authentication.
Server	Indicates the policy service from which the log was generated.
MDM Server Name	Shows the name of the MDM server.
Event	Shows the event status.
Failure Reason	Shows the detailed reason for failure, if the authentication failed.
Auth Method	Shows the authentication method that is used by the RADIUS protocol, such as Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2), IEE 802.1x or dot1x, and so on.
Authentication Protocol	Shows the authentication protocol used, such as Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol (EAP), and so on.
Security Group	Shows the group that is identified by the authentication log.
Session ID	Shows the session ID.

Note In the **RADIUS Live Logs** and **TACACS+ Live Logs** window, a Queried PIP entry appears for the first attribute of each policy authorization rule. If all the attributes within the authorization rule are related to a dictionary that was already queried for previous rules, no additional Queried PIP entry appears.

You can do the following in the RADIUS **Live Logs** window:

- Export the data in CSV or PDF format.

- Show or hide the columns based on your requirements.
- Filter the data using the quick or custom filter. You can also save your filters for later use.
- Rearrange the columns and adjust the width of the columns.
- Sort the column values.

Note All the user customizations are stored as user preferences.

Authentication Latency

Authentication Latency is the average response time of the RADIUS authentication process from the time authetication process is initiated. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Dashboard** > **System Summary** dashlet..

You can select the following authentication latency timeframe from the drop-down list:

- **60 mins:** This option gives you the authentication latency for the authentication that was initiated in last 60 mins.
- **12 hrs:** This option gives you the authentication latency for the authentication process that was initiated in last 24 hrs.

The response time that is displayed is in millisecond (ms). To view a detailed report of authentication latenty, click on the latest log in the **Live Logs** window. To view this window, click the **Menu** icon (☰) and choose **Operations** > **RADIUS**.

RADIUS Live Sessions

The following table describes the fields in the RADIUS **Live Sessions** window, which displays live authentications. To view this window, click the **Menu** icon (☰) and chooseYou can view the RADIUS live sessions only in the Primary PAN.

Table 52: RADIUS Live Sessions

Field Name	Description
Initiated	Shows the timestamp when the session was initiated.
Updated	Shows the timestamp when the session was last updated because of a change.
Account Session Time	Shows the time span (in seconds) of a user's session.
Session Status	Shows the current status of an endpoint device.
Action	Click the **Actions** icon to reauthenticate an active RADIUS session or disconnect an active RADIUS session.

Field Name	Description
Repeat Count	Shows the number of times a user or endpoint is reauthenticated.
Endpoint ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.
Identity	Shows the username of an endpoint device.
IP Address	Shows the IP address of an endpoint device.
Audit Session ID	Shows a unique session identifier.
Account Session ID	Shows a unique ID provided by a network device.
Endpoint Profile	Shows the endpoint profile for a device.
Posture Status	Shows the status of posture validation and details of the authentication.
Security Group	Shows the group that is identified by the authentication log.
Server	Indicates the Policy Service node from which the log was generated.
Auth Method	Shows the authentication method that is used by the RADIUS protocol, such as Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), IEE 802.1x or dot1x, and so on.
Authentication Protocol	Shows the authentication protocol used, such as Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol (EAP), and so on.
Authentication Policy	Shows the name of the policy selected for specific authentication.
Authorization Policy	Shows the name of the policy selected for specific authorization.
Authorization Profiles	Shows an authorization profile that was used for authentication.
NAS IP Address	Shows the IP address of a network device.
Device Port	Shows the connected port to a network device.
PRA Action	Shows the periodic reassessment action taken on a client after it is successfully postured for compliance on your network.
ANC Status	Adaptive Network Control status of a device as **Quarantine, Unquarantine**, or **Shutdown**.

Field Name	Description
WLC Roam	Shows the boolean (Y/N) used to track if an endpoint has been handed off during roaming, from one Wireless Lan Controller (WLC) to another. It has the value of cisco-av-pair=nas-update =Y or N. **Note** Cisco ISE relies on the nas-update=true attribute from WLC to identify whether the session is in roaming state. When the original WLC sends an accounting stop attribute with nas-update=true, the session is not deleted in ISE to avoid reauthentication. If roaming fails, ISE clears the session after five days of inactivity.
Packets In	Shows the number of packets received.
Packets Out	Shows the number of packets sent.
Bytes In	Shows the number of bytes received.
Bytes Out	Shows the number of bytes sent.
Session Source	Indicates whether it is a RADIUS session or a Passive ID session.
User Domain Name	Shows the registered DNS name of a user.
Host Domain Name	Shows the registered DNS name of a host.
User NetBIOS Name	Shows the NetBIOS name of a user.
Host NetBIOS Name	Shows the NetBIOS name of a host.
License Type	Shows the type of license used.
License Details	Shows the license details.

Field Name	Description
Provider	Endpoint events are learned from different syslog sources. These syslog sources are referred to as providers. • Windows Management Instrumentation (WMI): WMI is a Windows service that provides a common interface and object model to access management information about operating system, devices, applications, and services. • Agent: A program that runs on a client on behalf of the client or another program. • Syslog: A logging server to which a client sends event messages. • REST: A client is authenticated through a terminal server. The TS Agent ID, Source Port Start, Source Port End, and Source First Port values are displayed for this syslog source. • Span: Network information is discovered using span probes. • DHCP: DHCP event. • Endpoint **Note** When two events from different providers are learned or obtained from an endpoint session, the providers are displayed as comma-separated values in the **Live Sessions** window.
MAC Address	Shows the MAC address of a client.
Endpoint Check Time	Shows the time at which an endpoint was last checked by the endpoint probe.
Endpoint Check Result	Shows the result of an endpoint probe. The possible values are: • Unreachable • User Logout • Active User
Source Port Start	(Values are displayed only for the REST provider) Shows the first port number in a port range.
Source Port End	(Values are displayed only for the REST provider) Shows the last port number in a port range.
Source First Port	(Values are displayed only for the REST provider) Shows the first port allocated by the Terminal Server Agent. A Terminal Server refers to a server or network device that allows multiple endpoints to connect to it without a modem or network interface and facilities the connection of the multiple endpoints to a LAN network. The multiple endpoints appear to have the same IP address, and therefore, it is difficult to identify the IP address of a specific user. Consequently, to identify a specific user, a Terminal Server Agent is installed in the server, which allocates a port range to each user. This helps create an IP address-port user mapping.

Field Name	Description
TS Agent ID	(Values are displayed only for the REST provider) Shows the unique identity of the Terminal Server Agent that is installed on an endpoint.
AD User Resolved Identities	(Values are displayed only for AD user) Shows the potential accounts that matched.
AD User Resolved DNs	(Values are displayed only for AD user) Shows the Distinguished Name of AD user, for example, CN=chris,CN=Users,DC=R1,DC=com

TACACS Live Logs

The following table describes the fields in the TACACS Live Logs window that displays the TACACS+ AAA details. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **TACACS** > **Live Logs**. You can view the TACACS live logs only in the Primary PAN.

Table 53: TACACS Live Logs

Field Name	Usage Guidelines
Generated Time	Shows the syslog generation time based on when a particular event was triggered.
Logged Time	Shows the time when the syslog was processed and stored by the Monitoring node. This column is mandatory and cannot be deselected.
Status	Shows if the authentication succeeded or failed. This column is required and cannot be deselected. Green is used to represent passed authentications. Red is used to represent failed authentications.
Details	Brings up a report when you click the magnifying glass icon, allowing you to drill down and view more detailed information about the selected authentication scenario. This column is required and cannot be deselected.
Session Key	Shows the session keys (found in the EAP success or EAP failure messages) returned by ISE to the network device.
Username	Shows the user name of the device administrator. This column is required and cannot be deselected.
Type	Consists of two Types—Authentication and Authorization. Shows names of users who have passed or failed authentication, authorization, or both. This column is mandatory and cannot be deselected.
Authentication Policy	Shows the name of the policy selected for specific authentication.
Authorization Policy	Shows the name of the policy selected for specific authorization.
ISE Node	Shows the name of the ISE node through which the access request is processed.

Field Name	Usage Guidelines
Network Device Name	Shows the names of network devices.
Network Device IP	Shows the IP addresses of network devices whose access requests are processed.
Network Device Groups	Shows the name of corresponding network device groups to which a network device belongs.
Device Type	Shows the device type policy that is used to process access requests from different network devices.
Location	Shows the location-based policy that is used to process access requests from network devices.
Device Port	Shows the device port number through which the access request is made.
Failure Reason	Shows the reason for rejecting an access request that is made by a network device.
Remote Address	Shows the IP address, MAC address, or any other string that uniquely identifies the end station.
Matched Command Set	Shows the MatchedCommandSet attribute value if it is present, or an empty value if the MatchedCommandSet attribute value is empty or the attribute itself does not exist in the syslog.
Shell Profile	Shows the privileges that were granted to a device administrator for executing commands on the network device.

You can do the following in the **TACACS Live Logs** window:

- Export the data in CSV or PDF format.
- Show or hide the columns based on your requirements.
- Filter the data using the quick or custom filter. You can also save your filters for later use.
- Rearrange the columns and adjust the width of the columns.
- Sort the column values.

Note All the user customizations are stored as user preferences.

Export Summary

You can view the details of the reports exported by all the users in the last seven days, along with the status. The export summary includes both the manual and scheduled reports. The **Export Summary** window is automatically refreshed every two minutes. Click the **Refresh** icon to refresh the **Export Summary** window manually.

The super admin can cancel the export that is **In-Progess** or in **Queued** state. Other users are allowed only to cancel the export process that they have initiated.

By default, only three manual export of reports can run at a given point of time; the remaining triggered manual export of reports are queued. There are no such limits for the scheduled export of reports.

Note All the reports in the queued state are scheduled again and the reports in the **In-Progress** or **Cancellation-in-progress** state are marked as failed when the Cisco ISE server is restarted. If the primary MnT node is down, the scheduled report export job runs on secondary MnT node.

The following table describes the fields in the **Export Summary** window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Export Summary**.

Table 54: Export Summary

Field Name	Description
Report Exported	Displays the name of the report.
Exported By	Shows the role of the user who initiated the export process.
Scheduled	Shows whether the report export is a scheduled one.
Triggered On	Shows the time at which the export process has been triggered in the system.
Repository	Displays the name of the repository where the exported data will be stored.
Filter Parameters	Shows the filter parameters selected while exporting the report.
Status	Shows the status of the exported reports. It can be one of the following: • Queued • In-progress • Completed • Cancellation-in-progress • Cancelled • Failed • Skipped **Note** Failed status indicates the reason for failure. Skipped status indicates that the scheduled export of reports is skipped because the primary MnT node is down.

You can do the following in the **Export Summary** window:

- Show or hide the columns based on your requirements.
- Filter the data using quick or custom filter. You can also save your filters for later use.
- Rearrange the columns and adjust the width of the columns.

CHAPTER 7

Device Administration

- TACACS+ Device Administration, on page 461
- Device Administration Work Center, on page 462
- Device Administration Deployment Settings, on page 463
- Device Admin Policy Sets, on page 463
- Create Device Administration Policy Sets, on page 464
- TACACS+ Authentication Settings and Shared Secret, on page 465
- Device Administration - Authorization Policy Results, on page 466
- Change the Enable Password Through the CLI, on page 473
- Configure Global TACACS+ Settings, on page 473
- Data Migration from Cisco Secure ACS to Cisco ISE, on page 474
- Monitor Device Administration Activity, on page 474

TACACS+ Device Administration

Cisco ISE supports device administration using the TACACS+ security protocol to control and audit the configuration of network devices. The network devices are configured to query Cisco ISE for authentication and authorization of device administrator actions, and send accounting messages for Cisco ISE to log the actions. It facilitates granular control of who can access which network device and change the associated network settings. A Cisco ISE administrator can create policy sets that allow TACACS results, such as command sets and shell profiles, to be selected in authorization policy rules in a device administration access service. The Cisco ISE Monitoring node provides enhanced reports that are related to device administration. The Work Center menu contains all the device administration pages, which act as a single start point for ISE administrators.

Cisco ISE requires a Device Administration license to use TACACS+.

There are two types of administrators for device administration:

- Device Administrator
- Cisco ISE Administrator

The device administrator is the user who logs into the network devices such as switches, wireless access points, routers, and gateways, (normally through SSH), to perform the configuration and maintenance of the administered devices. The Cisco ISE administrator logs into Cisco ISE to configure and coordinate the devices that a device administrator logs in to.

The Cisco ISE administrator is the intended reader of this document, who logs into Cisco ISE to configure the settings that control the operations of the device administrator. The Cisco ISE administrator uses the device administration features (In the Cisco ISE GUI, click the **Menu** icon (☰) and choose**Work centers > Device Administration**) to control and audit the configuration of the network devices. A device can be configured to query the Cisco ISE server using the TACACS security protocol. The Cisco ISE Monitoring node provides enhanced reports that are related to device administration. A Cisco ISE administrator can perform the following tasks:

- Configure network devices with the TACACS+ details (shared secret).
- Add device administrators as internal users and set their enable passwords as needed.
- Create policy sets that allow TACACS results, such as command sets and shell profiles, to be selected in authorization policy rules in a device administration access service.
- Configure the TACACS server in Cisco ISE to allow device administrators to access devices based on the policy sets.

The device administrator performs the task of setting up a device to communicate with the Cisco ISE server. When a device administrator logs on to a device, the device queries the Cisco ISE server, which in turn queries an internal or external identity store, to validate the details of the device administrator. When the validation is done by the Cisco ISE server, the device informs the Cisco ISE server of the final outcome of each session or command authorization operation for accounting and auditing purposes.

A Cisco ISE administrator can manage device administration using TACACS Plus (TACACS+).

Note You should check the **Enable Device Admin Service** check box in the **Administration** > **System** > **Deployment** > **General Settings** page to enable TACACS+ operations. Ensure that this option is enabled in each PSN in a deployment.

Due to a known limitation of TACACS+ protocol to create a secure connection between switch or router and Cisco ISE, ensure that IP Security protocol is deployed between the two parties.

ISE Community Resource

For information about device administration attributes, see ISE Device Administration Attributes.

For information about TACACS+ configuration for wireless LAN controllers, Cisco IOS network devices, Cisco NX-OS network devices, and network devices, see ISE Device Administration (TACACS+).

Device Administration Work Center

The Work Center menu contains all the device administration pages, which act as a single start point for Cisco ISE administrators. However, pages that are not specific to device administration such as Users, User Identity Groups, Network Devices, Default Network Devices, Network Device Groups, Authentication and Authorization Conditions, can still be accessed from their original menu options, such as Administration. The Work Centers option is available only if the correct TACACS+ license(s) are obtained and installed.

The Device Administration Menu contains the following menu options: Overview, Identities, User Identity Groups, Ext ID Stores, Network Resources, Network Device Groups, Policy Elements, Device Admin Policy Sets, Reports, and Settings.

Device Administration Deployment Settings

The Device Administration Deployment page (In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Overview** > **Deployment**) allows Cisco ISE administrators to centrally view the device administration system without seeing each node in the deployment section.

The Device Administration Deployment page lists the PSNs in your deployment. This simplifies the task of enabling the device admin service individually in each PSN in your deployment. You can collectively enable the device admin service for many PSNs by selecting an option below:

Table 55: List of options in the Device Administration Deployment Window

Option	Description
None	By default, the device administration service is disabled for all nodes.
All Policy Service Nodes	Enables the device administration service in all PSNs. With this option, new PSNs are automatically enabled for device admin when they are added.
Specific Nodes	Displays the ISE Nodes section that lists all the PSNs in your deployment. You can select the required nodes that need the device admin service to be enabled.

Note If the deployment is not licensed for TACACS+, the above options are disabled.

The TACACS Ports field allows you to enter a maximum of four TCP ports, which are comma-separated and port values range 1–65535. Cisco ISE nodes and their interfaces listen for TACACS+ requests on the specified ports and you must ensure that the specified ports are not used by other services. The default TACACS+ port value is 49.

When you click **Save**, the changes are synchronized with the nodes that are specified in the **Administration** > **System** > **Deployment Listing** window.

Device Admin Policy Sets

The Device Admin Policy Sets window (In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers > Device Administration > Device Admin Policy Sets**) contains the list of policy sets that a Cisco ISE administrator manages to control the authentication and authorization of TACACS+ Device administrators. Each policy can be in one of two modes: Regular and Proxy Sequence.

A Regular policy set comprises an authentication rule table and an authorization rule table. The authentication rule table contains a set of rules to select actions required to authenticate a network device.

The authorization rule table contains a set of rules to select the specific authorization results required to implement the authorization business model. Each authorization rule consists of one or more conditions that must be matched for the rule to be engaged, and a set of command sets, and/or a shell profile, which are selected to control the authorization process. Each rule table has an exception policy that can be used to override the rules for specific circumstances, often the exception table is used for temporary situations.

Note TACACS+ CHAP outbound authentication is not supported.

A Proxy Sequence policy set contains a single selected proxy sequence. If the policy set is in this mode then one or more remote proxy servers are used to process the requests (although local accounting may be configured by the Proxy Sequence).

Create Device Administration Policy Sets

To create a device administration policy set:

Before you begin

- Ensure that the Device Administration in the **Work Centers** > **Device Administration** > **Overview** > **Deployment** window is enabled for TACACS+ operations.
- Ensure that any User Identity Groups, (for example, System_Admin, Helpdesk) required for the policy are created. (In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **User Identity Groups** page). Ensure that the member users (for example, ABC, XYZ) are allocated to their corresponding groups. (In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Identities** > **Users** window).
- Ensure to configure TACACS settings on devices that must be administered. (In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Network Resources** > **Network Devices** > **Add** > **TACACS Authentication Settings** check box is enabled and the shared secret for TACACS and devices are identical to facilitate the devices to query Cisco ISE.)
- Ensure that the Network Device Group, based on the Device Type and Location, is created. (In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Network Resources** > **Network Device Groups** window)

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Device Admin Policy Sets**.

Step 2 From the **Actions** column on any row, click the cog icon and then from the drop-down list, insert a new policy set by selecting any of the insert or duplicate options, as necessary.
A new row appears in the Policy Sets table.

Step 3 Enter the name and description for the policy set.

Step 4 If necessary, from the **Allowed Protocols/Server Sequence** column, click the (+) symbol and select one of the following:

a) Create a New Allowed Protocol
b) Create a TACACS Server Sequence

Step 5 From the **Conditions** column, click the (+) symbol.

Step 6 Create the required conditions in the **Conditions Studio Page**. In the **Editor** section, click the **Click To Add an Attribute** text box, and select the required Dictionary and Attribute (for example, Device-Location Equals Europe).

You can drag and drop a Library condition to the **Click To Add An Attribute** text box.

Step 7 Click **Use**.

Step 8 From the View column, click › to access all the policy set details and to create the authentication and authorization policies as well as policy exceptions.

Step 9 Create the required Authentication policy, (for example, Rule Name: ATN_Internal_Users, Conditions: DEVICE:Location EQUALS Location #All Locations#Europe—The policy matches only devices that are in location Europe).

Step 10 Click **Save**.

Step 11 Create the required Authorization Policy.

Example 1: Rule Name: Sys_Admin_rule, Conditions: if SysAdmin and TACACS User Equals ABC then cmd_Sys_Admin AND Profile_priv_8—The policy matches system administrators with username ABC and allows the specified commands to be executed and assigns a privilege level of 8.

Example 2: Rule Name: HelpDesk AND TACACS User EQUALS XYZ then cmd_HDesk_show AND cmd_HDesk_ping AND Profile_priv_1—The policy matches system administrators with username XYZ and allows the specified commands to be executed and assigns a privilege level of 1.

In the above examples:

- The command sets, cmd_Sys_Admin and cmd_HDesk, are created in the **Work Centers** > **Device Administration** > **Policy Elements** > **Results**>**TACACS Command Sets** > **Add** window.
- The TACACS profiles, Profile_Priv_1 and Profile_priv_8, are created in the **Work Centers** > **Device Administration** > **Policy Elements** > **Results** >**TACACS Profiles** > **Add** window.

Note You can add IPv4 or IPv6 single address for the Device IP address attribute in the conditions that are used in authentication and authorization policies.

Step 12 Click **Save**.

TACACS+ Authentication Settings and Shared Secret

The following table describes the fields in the Network Devices window, which you can use to configure TACACS+ authentication settings for a network device. The navigation path is:

- (For Network Devices) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Network Resources** > **Network Devices** > **Add** > **TACACS Authentication Settings**.
- (For Default Devices) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Network Resources** > **Default Devices** > **TACACS Authentication Settings**. See Define a Default Network Device in Cisco ISE for more information.

Field Name	Usage Guidelines
Shared Secret	A string of text that is assigned to a network device when TACACS+ protocol is enabled. A user must enter the text before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret. This is not a mandatory field.

Field Name	Usage Guidelines
Retired Shared Secret is Active	Displayed when the retirement period is active.
Retire	Retires an existing shared secret instead of ending it. When you click **Retire**, a message box is displayed. You can either click **Yes** or **No**.
Remaining Retired Period	(Available only if you select **Yes** in the above message box) Displays the default value specified in the following navigation path: In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Settings** > **Connection Settings** > **Default Shared Secret Retirement Period.** You can change the default values. This allows a new shared secret to be entered and the old shared secret will remain active for the specified number of days.
End	(Available only if you select **Yes** in the above message box) Ends the retirement period and terminates the old shared secret.
Enable Single Connect Mode	Check to use a single TCP connection for all TACACS+ communication with the network device. Choose one of the following: • Legacy Cisco Devices • Or, TACACS+ Draft Compliance Single Connect Support. If you disable Single Connect Mode, ISE uses a new TCP connection for every TACACS+ request.

In summary, you can:

- Retire the old shared secret by specifying the retirement period as number of days (Range is 1–99) and at the same time set a new shared secret.
- Use the old and new shared secrets during the retirement period.
- Extend the retirement period before it expires.
- Use the old shared secret only until the end of the retirement period.
- Terminate the retirement period before it expires (click End and then Submit).

Note In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Devices** > **Add** window to access the TACACS+ Authentication Settings option.

Device Administration - Authorization Policy Results

Cisco ISE administrators can use the TACACS+ command sets and TACACS+ profiles (policy results) to control the privileges and commands that are granted to a device administrator. The policy works along with the network devices and so prevents accidental or malicious configuration changes that may be done. If such changes occur, you can use the device administration audit reports to track the device administrator who has executed a particular command.

Allowed Protocols in FIPS and Non-FIPS Modes for TACACS+ Device Administration

There are many allowed authentication protocol services that Cisco ISE offers for creating the policy results. However, authentication protocol services such as PAP/ASCII, CHAP, and MS-CHAPv1, that apply to the TACACS+ protocol, are disabled on FIPS-enabled Cisco ISE appliances for RADIUS. As a result, you cannot enable these protocols in the **Policy** > **Policy Elements** > **Results** > **Allowed Protocols** window to administer devices, when using a FIPS-enabled (**Administration** > **System Settings** > **FIPS Mode**) Cisco ISE appliance.

To configure PAP/ASCII, CHAP, and MS-CHAPv1 protocols in your device administration policy results, for both FIPS and non-FIPS modes, you must navigate to the **Work Centers** > **Device Administration** > **Policy Elements** > **Results** > **Allowed Protocols** window. Only the Default Device Admin allowed protocols setting may be used when FIPS mode is enabled. This option is not allowed in RADIUS.

TACACS+ Command Sets

Command sets enforce the specified list of commands that can be executed by a device administrator. When a device administrator issues operational commands on a network device, Cisco ISE is queried to determine whether the administrator is authorized to issue these commands. This is also referred to as command authorization.

Wildcards and Regex in Command Sets

A command line comprises the command and zero or more arguments. When Cisco ISE receives a command line (request), it handles the command and its arguments in different ways:

- It matches the command in the request with the commands that are specified in the command set list using the wildcard matching paradigm.

  Example: Sh?? or S*

- It matches the arguments in the request with the arguments that are specified in the command set list using regular expressions (regex) matching paradigm.

  Example: Show interface[1-4] port[1-9]:tty*

Command Line and Command Set List Match

To match a requested command line to a command set list that contains wildcards and regex:

1. Iterate over a command set list to detect matching commands.

   Wildcard matching permits:

   - Case insensitivity.
   - Any character in the command in the command set may be "?", which matches any individual character that must exist in the requested command.
   - Any character in the command in the command set may be "*", which matches zero or more characters in the requested command.

     Examples:

Request	Command Set	Matches	Comments
show	show	Y	—
show	SHOW	Y	Case insensitive
show	Sh??	Y	Matches any character
show	Sho??	N	Second "?" intersects with the character that does not exist
show	S*	Y	"*" matches any character
show	S*w	Y	"*" matches characters "ho"
show	S*p	N	Character "p" does not correspond

2. For each matching command, Cisco ISE validates the arguments.

   The command set list includes a space-delimited set of arguments for each command.

   Example: Show interface[1-4] port[1-9]:tty.*

   This command has two arguments.

   1. Argument 1: interface[1-4]

   2. Argument 2: port[1-9]:tty.*

   The command arguments in the request are taken in the position-significant order in which they appear in the packet. If all the arguments in the command definition match the arguments in the request, then this command or argument is considered to be a match. Any extraneous arguments in the request are ignored.

Note Use the standard Unix regular expressions in arguments.

Process Rules with Multiple Command Sets

1. If a command set contains a match for the command and its arguments, and the match has Deny Always, Cisco ISE designates the command set as Commandset-DenyAlways.
2. If a command set does not contain a Deny Always for a command match, Cisco ISE checks all the commands in the command set sequentially for the first match.
   a. If the first match has Permit, Cisco ISE designates the command set as Commandset-Permit.
   b. If the first match has Deny, Cisco ISE designates the command set as Commandset-Deny.
3. After Cisco ISE has analyzed all the command sets, it authorizes the command:

a. If Cisco ISE designated any command set as Commandset-DenyAlways, Cisco ISE denies the command.

b. If there is no Commandset-DenyAlways, Cisco ISE permits the command if any command set is Commandset-Permit; otherwise, Cisco ISE denies the command. The only exception is when the **Unmatched** check box is checked.

Create TACACS+ Command Sets

To create a policy set using the TACACS+ command sets policy results:

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Policy Elements** > **Results** > **TACACS Command Sets**.

You can also configure TACACS command sets in the **Work Centers** > **Device Administration** > **Device Admin Policy Sets** page.

Step 2 Click **Add**.

Step 3 Enter a name and description.

Step 4 Click **Add** to specify the Grant permission, Command, and Argument.

Step 5 In the **Grant** drop-down, you can choose one of the following:

- **Permit**: To allow the specified command, (for example, permit show, permit con* Argument terminal).
- **Deny**: To deny the specified command, (for example, deny mtrace).
- **Deny Always**: To override a command that has been permitted in any other command set, (for example, clear auditlogs)

Note Click the action icon to increase or decrease the column width of the Grant, Command, and Argument fields.

Step 6 Check the **Permit any command that is not listed below** check box to allow commands and arguments that are not specified as Permit, Deny or Deny Always in the Grant column.

TACACS+ Profile

TACACS+ profiles control the initial login session of the device administrator. A session refers to each individual authentication, authorization, or accounting request. A session authorization request to a network device elicits a Cisco ISE response. The response includes a token that is interpreted by the network device, which limits the commands that may be executed during a session. The authorization policy for a device administration access service can contain a single shell profile and multiple command sets. The TACACS+ profile definitions are split into two components:

- Common tasks
- Custom attributes

There are two views in the TACACS+ Profiles window (In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Policy Elements** > **Results** > **TACACS Profiles**), **Task**

Attribute View and **Raw View**. You can enter common tasks using the **Task Attribute View** and create custom attributes in the **Task Attribute View** and the **Raw View**.

The **Common Tasks** section allows you to select and configure the frequently used attributes for a profile. The attributes that are included here are those defined by the TACACS+ protocol draft specifications. However, the values can be used in the authorization of requests from other services. In the **Task Attribute View**, the Cisco ISE administrator can set the privileges that will be assigned to the device administrator. The common task types are:

- Shell
- Cisco WLC
- Cisco Nexus
- Generic

The **Custom Attributes** section allows you to configure extra attributes. It provides a list of attributes that are not recognized by the **Common Tasks** section. Each definition consists of the attribute name, an indication of whether the attribute is mandatory or optional, and the value for the attribute.

Note You can define a total of 24 task attributes for TACACS-enabled network devices. If you define more than 24 task attributes, none of them are sent to TACACS-enabled network devices.

In the **Raw View**, you can enter the mandatory attributes using an equal to (=) sign between the attribute name and its value and optional attributes are entered using an asterisk (*) between the attribute name and its value. The attributes that are entered in the **Raw View** section are reflected in the **Custom Attributes** section in the **Task Attribute View** and vice versa. The **Raw View** section is also used to copy and paste the attribute list (for example, another product's attribute list) from the clipboard onto Cisco ISE. Custom attributes can be defined for nonshell services.

Create TACACS+ Profiles

To create a TACACS+ profile:

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Policy Elements** > **Results** > **TACACS Profiles**.

You can also configure TACACS command sets in the **Work Centers** > **Device Administration** > **Device Admin Policy Sets** page.

Step 2 Click **Add**.

Step 3 In the **TACACS Profile** section, enter a name and description.

Step 4 In the **Task Attribute View** tab, check the required **Common Tasks**. See the Common Tasks Settings, on page 471 page.

Step 5 In the **Task Attribute View** tab, in the **Custom Attributes** section, click **Add** to enter the required attributes.

Common Tasks Settings

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Policy Elements** > **Results** > **TACACS Profiles** > **Add** to view the common tasks settings window. The Common Task Types are Shell, Cisco WLC, Cisco Nexus, and Generic.

Shell

The following options are available for the Cisco ISE administrator to set the device administrator's privileges.

Option	Description
Default Privilege	Enable the default (initial) privilege level for a device administrator for the shell authorization. Select any one of the following options: • Select values between 0 through 15. • Select the required Identity Store Attribute.
Maximum Privilege	Enable the maximum privilege level for Enable authentication. You can select values between 0 through 15.
Access Control List	Select an ASCII String (1-251*) or the required Identity Store Attribute.
Auto Command	Select an ASCII String (1-248*) or the required Identity Store Attribute.
No Escape	Select any one of the following options for escape characters: • True: Specifies that escape prevention is enabled. • False: Specifies that escape prevention is not enabled. • Select the required Identity Store Attribute.
Timeout	Select values between 0 through 9999 or the required Identity Store Attribute.
Idle Time	Select values between 0 through 9999 or the required Identity Store Attribute.

Cisco WLC

The following options are available for the Cisco ISE administrator to control a device administrator's access to the Cisco WLC application tabs. The Cisco WLC application contains the following tabs: WLAN, Controller, Wireless, Security, Management, and Commands.

Option	Description
All	Device administrators have full access to all the Cisco WLC application tabs.
Monitor	Device administrators have only read-only access to the Cisco WLC application tabs.
Lobby	Device administrators have only limited configuration privileges.
Selected	Device administrators have access to the tabs as checked by the Cisco ISE administrator from the following check boxes: WLAN, Controller, Wireless, Security, Management, and Commands.

Nexus

The following options are available for the Cisco ISE administrator to control a device administrator's access to the Cisco Nexus switches.

Option	Description
Set Attribute As	A Cisco ISE administrator can specify the Nexus attributes generated by the common tasks as Optional or Mandatory.
Network Role	When a Nexus is configured to authenticate using Cisco ISE, the device administrator, by default, has read-only access. Device administrators can be assigned to one of these roles. Each role defines the operations that is allowed: • None: No privileges. • Operator (Read Only): Complete read access to the entire NX-OS device. • Administrator (Read/Write): Complete read-and-write access to the entire NX-OS device.
Virtual Device Context (VDC)	None: No privileges. Operator (Read Only): Read access limited to a VDC Administrator (Read/Write): Read-and-write access that is limited to a VDC.

Generic

The Cisco ISE administrator uses the option to specify custom attributes that are not available in the common tasks.

Change the Enable Password Through the CLI

To change Enable password, perform the following steps:

Before you begin

Some commands are assigned to privileged mode. Therefore, they can only be executed when the device administrator has authenticated into this mode.

The device sends a special enable authentication type when the device administrator attempts to enter the privileged mode. Cisco ISE supports a separate enable password to validate this special enable authentication type. The separate enable password is used when the device administrator is authenticated with internal identity stores. For authentication with external identity stores, the same password is used as for regular login.

Step 1 Log in to the switch.

Step 2 Press Enter to display the following prompt:

```
Switch>
```

Step 3 Execute the following commands to configure the Enable password.

```
Switch> enable
Password: (Press Enter to leave the password blank.)
Enter Old Password: (Enter the old password.)
Enter New Password: (Enter the new password.)
Enter New Password Confirmation: (Confirm the new password.)
```

Note If password lifetime is configured for the Login password and Enable password, the user account will be disabled if the passwords are not changed within the specified time period. If Cisco ISE is configured as TACACS+ server and the **Enable Bypass** option is configured on the network device, you cannot change the Enable password from the CLI (via telnet). In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **Identities** > **Users** to change the Enable password for internal users.

Configure Global TACACS+ Settings

To configure global TACACS+ settings:

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Settings**.

In the **Connection Settings** tab, you can change the default values for the required fields.

- In the **Authorization cache timeout** field, you can set the Time-To-Live (TTL) value for which certain attributes of an internal user are cached upon the first authorization request. The cached attributes include username, and user-specific attributes, such as UserGroup. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **System Administration > Configuration > Dictionaries > Identity > Internal Users** to create attributes. The default value is 0, which means the authorization cache is disabled.

- **Single Connect Support**: If you disable Single Connect Mode, ISE uses a new TCP connection for every TACACS+ request.

Step 2 In the **Password Change Control** tab, define the required fields to control whether password update is permitted through TACACS+.

The prompts in the **Enable Telnet Change Password** section are enabled only when this option is selected. Or else, the prompts in the **Disable Telnet Change Password** are enabled. The password prompts are fully customizable and can be modified as needed.

In the **Password Policy Violation Message** field, you can display an appropriate error message for the password set by the internal users if the new password does not match the specified criteria.

Step 3 In the **Session Key Assignment** tab, select the required fields to link TACACS+ requests into a session.

The session key is used by the Monitoring node to link AAA requests from clients. The default settings are for NAS-Address, Port, Remote-Address, and User fields to be enabled.

Step 4 Click **Save**.

Related Topics

TACACS+ Authentication Settings and Shared Secret, on page 465

Data Migration from Cisco Secure ACS to Cisco ISE

You can use the migration tool to import data from Cisco Secure ACS 5.5 and later, and set a default TACACS+ secret for all network devices. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Overview** and in the **Prepare** section, click **Download Software Webpage** to download the migration tool. Save the tool to your PC, and from the migTool folder, run the migration.bat file to start the migration process. For complete information related to the migration, see the Migration Guide for your version of Cisco ISE.

Monitor Device Administration Activity

Cisco ISE provides various reports and logs that allow you to view information that is related to accounting, authentication, authorization, and command accounting of devices configured with TACACS+. You can run these reports either on demand or on a scheduled basis.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Reports** > **Reports.**.

You can also view the reports in another location. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Reports** page.

Step 2 In the **Report Selector**, expand **Device Administration** to view **Authentication Summary**, **TACACS Accounting**, **TACACS Authentication**, **TACACS Authorization** , **TACACS Command Accounting**, **Top N Authentication by Failure Reason**, **Top N Authentication by Network Device**, **Top N Authentication by User** reports.

Step 3 Select the report and choose the data with which you want to search using the **Filters** drop-down list.

Step 4 Select the **Time Range** during which you want to view the data.

Step 5 Click **Run**.

TACACS Live Logs

The following table describes the fields in the TACACS Live Logs window that displays the TACACS+ AAA details. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **TACACS** > **Live Logs**. You can view the TACACS live logs only in the Primary PAN.

Table 56: TACACS Live Logs

Field Name	Usage Guidelines
Generated Time	Shows the syslog generation time based on when a particular event was triggered.
Logged Time	Shows the time when the syslog was processed and stored by the Monitoring node. This column is mandatory and cannot be deselected.
Status	Shows if the authentication succeeded or failed. This column is required and cannot be deselected. Green is used to represent passed authentications. Red is used to represent failed authentications.
Details	Brings up a report when you click the magnifying glass icon, allowing you to drill down and view more detailed information about the selected authentication scenario. This column is required and cannot be deselected.
Session Key	Shows the session keys (found in the EAP success or EAP failure messages) returned by ISE to the network device.
Username	Shows the user name of the device administrator. This column is required and cannot be deselected.
Type	Consists of two Types—Authentication and Authorization. Shows names of users who have passed or failed authentication, authorization, or both. This column is mandatory and cannot be deselected.
Authentication Policy	Shows the name of the policy selected for specific authentication.
Authorization Policy	Shows the name of the policy selected for specific authorization.
ISE Node	Shows the name of the ISE node through which the access request is processed.
Network Device Name	Shows the names of network devices.
Network Device IP	Shows the IP addresses of network devices whose access requests are processed.
Network Device Groups	Shows the name of corresponding network device groups to which a network device belongs.

Field Name	Usage Guidelines
Device Type	Shows the device type policy that is used to process access requests from different network devices.
Location	Shows the location-based policy that is used to process access requests from network devices.
Device Port	Shows the device port number through which the access request is made.
Failure Reason	Shows the reason for rejecting an access request that is made by a network device.
Remote Address	Shows the IP address, MAC address, or any other string that uniquely identifies the end station.
Matched Command Set	Shows the MatchedCommandSet attribute value if it is present, or an empty value if the MatchedCommandSet attribute value is empty or the attribute itself does not exist in the syslog.
Shell Profile	Shows the privileges that were granted to a device administrator for executing commands on the network device.

You can do the following in the **TACACS Live Logs** window:

- Export the data in CSV or PDF format.
- Show or hide the columns based on your requirements.
- Filter the data using the quick or custom filter. You can also save your filters for later use.
- Rearrange the columns and adjust the width of the columns.
- Sort the column values.

Note All the user customizations are stored as user preferences.

CHAPTER 8

Guest and Secure WiFi

- Cisco ISE Guest Services, on page 477
- Guest and Sponsor Accounts, on page 478
- Guest Portals, on page 497
- Sponsor Portals, on page 512
- Monitor Guest and Sponsor Activity, on page 526
- Guest Access Web Authentication Options, on page 527
- Guest Portal Settings, on page 534
- Sponsor Portal Application Settings, on page 550
- Global Settings for Guest and Sponsor Portals, on page 557
- Guest Type Settings, on page 558
- Sponsor Group Settings, on page 560
- End-User Portals , on page 563
- Customization of End-User Web Portals , on page 563
- Portal Content Types, on page 565
- Basic Customization of Portals, on page 565
- Advanced Customization of Portals , on page 573
- Portal Language Customization, on page 589
- Customization of Guest Notifications, Approvals, and Error Messages, on page 592
- Portal Pages Titles, Content and Labels Character Limits, on page 595
- Portal Customization, on page 597
- HTML Support for a Portal Language File, on page 598

Cisco ISE Guest Services

Cisco Identity Services Engine (Cisco ISE) guest services enable you to provide secure network access to guests such as visitors, contractors, consultants, and customers. You can support guests with basic Cisco ISE licenses, and you can choose from several deployment options depending on your company's infrastructure and feature requirements.

Cisco ISE provides web-based and mobile portals to provide on-boarding for guests and employees to your company's network and internal resources and services.

From the Admin portal, you can create and edit guest and sponsor portals, configure guest access privileges by defining their guest type, and assign sponsor privileges for creating and managing guest accounts.

- Guest Portals, on page 497
- Guest Types and User Identity Groups, on page 479
- Sponsor Portals, on page 512
- Sponsor Groups, on page 514

ISE Community Resource

For the complete list of ISE community resources for ISE Guest and Web Authentication, see ISE Guest Access - ISE Guest and Web Authentication.

End-User Guest and Sponsor Portals in Distributed Environment

Cisco ISE end-user web portals depend on the Administration, Policy Services, and Monitoring personas to provide configuration, session support, and reporting.

- **Policy Administration node (PAN)**: Configuration changes that you make to the users, devices, and end-user portals are written to the PAN.
- **Policy Service node (PSN)**: The end-user portals run on a PSN, which handles all session traffic, including: network access, client provisioning, guest services, posture, and profiling. If a PSN is part of a node group, and one node fails, the other nodes detect the failure and reset any pending sessions.
- **Monitoring node (MnT node)**: The MnT node collects, aggregates, and reports data about the end-user and device activity on the My Devices, Sponsor, and Guest portals. If the primary MnT node fails, the secondary MnT node automatically becomes the primary MonT node.

Guest and Sponsor Accounts

- **Guest Accounts**: Guests typically represent authorized visitors, contractors, customers, or other users who require temporary access to your network. You can also use guest accounts for employees if you prefer to use one of the guest deployment scenarios to allow employees to access the network. You can access the Sponsor portal to view guest accounts created by a sponsor and by self-registering guests.
- **Sponsor Accounts**: Use the Sponsor portal to create temporary accounts for authorized visitors to securely access your corporate network or the Internet. After creating the guest accounts, you can also use the Sponsor portal to manage these accounts and provide account details to the guests.

Guest accounts can be created by:

- **Sponsors**: On the Admin portal, you can define the access privileges and feature support for sponsors, who can access the Sponsor portal to create and manage guest accounts.
- **Guests**: Guests can also create their own accounts by registering themselves on the Self-Registered Guest portal. Based on the portal configuration, these self-registering guests may need sponsor approval before they receive their login credentials.

  Guests can also choose to access the network using the Hotspot Guest portal, which does not require the creation of guest accounts and login credentials, such as username and password.

- **Employees**: Employees who are included in identity stores (such as Active Directory, LDAP, Internal Users) can also gain access through the credentialed Guest portals (Sponsored-Guest and Self-Registered Guest portals), if configured.

Devices onboarded through the Bring Your Own Device (BYOD) workflow will not be treated as a Guest device and the Endpoint Identity Group that is configured will not be changed. For more information on Bring Your Own Device (BYOD), see Bring Your Own Device (BYOD).

After their guest accounts are created, guests can use the Sponsored-Guest portal to log in and gain access to the network.

Note During a successful guest flow, inside *Access-Accept*, Cisco ISE sends a RADIUS Session-Timeout Attribute with the value set to the remaining seconds of guest account duration. However, the Custom Session-Timeout attribute in the appropriate Authorization Profile takes precedence over the behavior of the RADIUS Session-Timeout Attribute.

Guest Types and User Identity Groups

Each guest account must be associated with a guest type. Guest types allow a sponsor to assign different levels of access and different network connection times to a guest account. These guest types are associated with particular network access policies. Cisco ISE includes these default guest types:

- Contractor: Users who need access to the network for an extended amount of time, up to a year.
- Daily: Guests who need access to the resources on the network for just 1 to 5 days.
- Weekly: Users who need access to the network for a couple of weeks.

When creating guest accounts, certain sponsor groups can be restricted to using specific guest types. Members of such a group can create guests with only the features specified for their guest type. For instance, the sponsor group, ALL_ACCOUNTS, can be set up to use only the Contractor guest type, and the sponsor groups, OWN_ACCOUNTS and GROUP_ACCOUNTS, can be set up to use Daily and Weekly guest types. If the self-registering guests using the Self-Registered Guest portal typically need access for just a day, you can assign them the Daily guest type.

The guest type defines the user identity group for a guest.

For more information, see:

- User Identity Groups, on page 624
- Create a User Identity Group, on page 632

Create or Edit Guest Types

You can edit the default Guest Types and their default access privileges and settings, or you can create new Guest Types. Changes you make are applied to existing Guest accounts that were created using this particular Guest Type. Guest users who are logged in will not see these changes until they log out and log back in. You can also duplicate Guest Types to create additional Guest Types with the same access privileges.

Each Guest Type has a name, description, and a list of sponsor groups that can create Guest Accounts with this Guest Type. You can designate some Guest Types—use just for self-registering guests, or do not use to create Guest Accounts (by any sponsor group).

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Guest Access** > **Configure** > **Guest Types**, and enter the required details.

Use these settings to create the types of guests who can access your network, and their access privileges. You can also specify which Sponsor Groups can create a Guest Type.

Field Name	**Usage Guidelines**
Guest Type Name	Provide a name (from 1 to 256 characters) that distinguishes this Guest Type from the default Guest Types and others that you create.
Description	Provide additional information (maximum of 2000 characters) about the recommended use of this Guest Type, for example, use for self-registering guests, Do not use for guest account creation, and so on.
Language File	Export or import the language file to use for portals using this Guest Type.
Collect Additional Data	Select custom fields to collect additional information from guests. To view this window, click the **Menu** icon (☰) and choose **Guest Access** > **Settings** > **Custom Fields**.
Maximum Access Time—Account Duration Starts	**From First Login**: The account start time starts when the guest user first logs in to the guest portal, and the end time equals the specified duration time. If the guest user never logs in, the account remains in the Awaiting First login state until the account is removed by the Guest Account Purge Policy. Self-registered and Sponsor-created user accounts start when they create their acoounts and log in to them. **Note** If you choose **Allow access only on these days and times**, the location is used to establish context of these times. If you do not want **From First Login** access to be based on location, do not set days and times for access. **From sponsor-specified date**: Specify the maximum number of days, from 1 to 999, hours or minutes, that guests of this Guest Type can access and stay connected to the network. If you change this setting, your changes will not apply to existing guest accounts created using this Guest Type.

Field Name	Usage Guidelines
Allow Access only on these Days and Times	Enter the time range and select the days of the week to specify when this Guest Type can access the network. If this Guest Type remains connected outside these time parameters, they will be logged out. The time ranges are related to the time zones defined by the locations assigned to the guests using this Guest Type. Click **+** or **-** for adding or deleting restricted access times.
Configure Guest Account Purge Policy	You can schedule an endpoint purge job. The endpoint purge schedule is enabled by default and Cisco ISE deletes endpoints that are older than 30 days. See Endpoints Purge Settings, on page 381 for more information.
Login Options—Maximum simultaneous logins	Enter the maximum number of user sessions that this Guest Type can have running concurrently.
When Guest Exceeds Limit	When you select **Maximum simultaneous logins**, you must also select the action to take when a user connects after that limit is reached. **When the guest exceeds limit**: • **Disconnect the oldest connection** • **Disconnect the newest connection** • **Redirect user to a portal page showing an error message**: An error message is displayed for a period of time that can be configured. After this, the session is disconnected, and the user is redirected to the Guest portal. The error page's content is configured on the **Portal Page Customization** dialog box, under the **Messages** > **Error Messages** tab.
Maximum Devices Guests can Register	Enter the maximum number of devices that can be registered to each guest. You can set the limit to a number lower than what is already registered for the guests of this Guest Type. This will only affect newly created guest accounts. When guest users reach the maximum number of devices they can register, they view a notification that informs them that they can proceed in one of the following ways: • Select a registered device to remove from their device list and then add a new device. • Proceed with registering a new device. In this scenario, the oldest registered device on their list is automatically deregistered.

Field Name	Usage Guidelines
Assign Endpoint Identity Groups for Guest Devices	You must assign endpoint identity groups for guest device registration workflows. Click the corresponding radio button to assign a **Standard** endpoint identity group or a **Dynamic** endpoint identity group respectively: • **Standard**: From the **identitygroup** drop-down list, choose the required endpoint identity group. • **Dynamic**: You can only assign LDAP user groups through the dynamic option. If a user belongs to multiple user groups, Cisco ISE checks the following list sequentially and proceeds with the first user group (with its configured identity group) that the user matches with. • From the **User Group** drop-down list, choose the required LDAP user group. • From the **Identity Group** drop-down list, choose the required endpoint identity group.
Allow Guest to bypass the Guest portal	Allows users to bypass the credentialed Guest captive portal (web authentication page) and access the network by providing credentials to wired and wireless (dot1x) supplicants or VPN clients. Guest accounts go to Active state bypassing the Awaiting Initial Login state and the AUP page, even if it is required. If you do not enable this setting, users must first log in through the credentialed Guest captive portal before they will be able to access other parts of the network.
Account Expiration Notification—Send account expiration notification __ days before account expires	Send a notification to Guests before their account expires and specify how many days, hours or minutes in advance of the expiration.
View messages in	Specify the language to use when displaying email or SMS notifications as you set them up.
Email	Select email as the method used for account expiry notification.
Use customization from	Select email customization from another portal.
Messages	Enter the text to use for account expiry notification.
Copy text from	Reuse email text that you created for another Guest Type for account expiry notification.

Field Name	Usage Guidelines
Send test email to me at	Ensure that the email notification displays as it should by sending it to your email address.
SMS	Select text (SMS) as the method used for account expiry notification.
Messages	Enter the text to use for account expiry notification.
Copy text from	Reuse text messages that you created for another Guest Type.
Send test SMS to me at	Ensure that the text notification displays as it should by sending it to your cell phone.
These sponsor groups can create this guest type	Select which sponsor groups can create Guest accounts with this Guest Type. If you want to disable use of this Guest Type, do not assign it to any sponsor group. If you want to discontinue use of this Guest Type, delete the sponsor groups listed.

What to do next

- Create or modify sponsor groups to use this guest type.
- If appropriate, assign this guest type to self-registering guests in the Self-Registered Guest portal.

Disable a Guest Type

You cannot delete the last remaining guest type or guest types that are being used by guest accounts. If you want to delete a guest type that is in use, first ensure that it is no longer available for use. Disabling a guest type does not affect guest accounts that were created with that guest type.

The following steps explain how to prepare for and disable a target guest type.

Step 1 Identify the sponsor groups that allow the sponsor to create guests using the target guest type. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Configure** > **Portals and Components** > **Sponsor Groups**. Open each sponsor group and examine the **This sponsor group can create accounts using these guest types list**.

Step 2 Identify the Self-Registered portals that assign the target guest type. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Configure** > **Portals and Components** > **Guest Portals**. Open each Self-Registered Guest portal. If the portal uses the specific guest type, expand **Portal Settings**, and change the assigned Guest Type in the **Employees using this portal as guests inherit login options and dynamic endpoint group assignment from:** field.

Step 3 Open the guest type you wish to delete, and delete all sponsor groups that you identified in the previous steps. This action effectively prevents all sponsors from using creating a new guest account with this guest type. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Configure** > **Portals and Components** > **Guest Type**.

Configure Maximum Simultaneous Logins for Endpoint Users

You can configure the maximum number of simultaneous logins that are allowed for a guest.

When the user logs in to a guest portal, and is successfully authenticated, that user's number of existing logins is checked to see if the user has already reached the maximum number of logins. If yes, the Guest user is redirected to an error page. An error page is displayed, and the session is stopped. If that user tries to access the internet again, the user's connection is redirected to the guest portal's login page.

Before you begin

Make sure that the authorization profile that you are using in the authorization policy for this portal has **Access Type** set to *Access_Accept*. If **Access Type** is set to *Access_Reject*, then maximum simultaneous logins is not enforced.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Type**. Under **Login Options**:

a) Check the **Maximum simultaneous logins** check box and enter the maximum number of simultaneous logins allowed.
b) Under **When guest exceeds limit**, click the **Disconnect the newest connection** option.
c) Check the **Redirect user to a portal page showing an error message** check box.

Step 2 Choose **Policy** > **Policy Elements** > **Results**, and create an authorization profile:

a) Under **Common Tasks**, check **Web Redirection** and do the following:
    - In the first drop-down, choose **Centralized Web Auth**.
    - Enter the **ACL** you created as part of the prerequisite.
    - For **Value**, select the guest portal to be redirected to.
b) Scroll down in **Common Tasks**, and check the **Reauthentication** check box and do the following:
    - In **Timer**, enter the amount of time you want the error page to display before redirecting the user to the guest portal.
    - In **Maintain Connectivity During Reauthentication**, choose **Default**.

Step 3 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Sets**. Create an authorization policy so that when the attribute NetworkAccess.SessionLimitExceeded is true, the user is redirected to the portal.

What to do next

You can customize the text of the error page on the Portal Page Customization tab. Choose **Messages** > **Error Messages** and change the text of the error message key *ui_max_login_sessions_exceeded_error*.

Schedule When to Purge Expired Guest Accounts

When an active or suspended guest account reaches the end of its account duration (as defined by the sponsor when creating the account), the account expires. When guest accounts expire, the affected guests cannot access the network. Sponsors can extend expired accounts before they are purged. However, after an account is purged, sponsors must create new accounts.

When expired guest accounts are purged, the associated endpoints and reporting and logging information are retained.

Cisco ISE automatically purges expired guest accounts every 15 days, by default. The **Date of next purge** indicates when the next purge will occur. You can also:

- Schedule a purge to occur every X days. The first purge will occur in X days at **Time of Purge**, then purges occur every X days.
- Schedule a purge on a given day of the week every X weeks. The first purge occurs on the next **Day of Week** at **Time of Purge**, then purges occur every configured number of weeks on that day and time. For example, on Monday you set purges to occur on Thursday every 5 weeks. The next purge will be the Thursday of this week, not the Thursday 5 weeks from now.
- Force a purge to happen immediately by clicking **Purge Now**.

If the Cisco ISE server is down when the purge is scheduled to run, the purge is not executed. The purge process will run again at the next scheduled purge time, assuming the server is operational at that time.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Settings** > **Guest Account Purge Policy**.

Step 2 Choose one of these options:

- Click **Purge Now** to immediately purge the expired guest account records.
- Check **Schedule purge of expired guest accounts** to schedule a purge.

Note After each purge is completed, the **Date of next purge** is reset to the next scheduled purge.

Step 3 Specify the number of days of inactivity to expire users in **Expire portal-user information after**. This setting prevents LDAP and Active Directory accounts that were never used from staying in the ISE database indefinitely.

If a first login does not happen, on expiry of the specified time period, the guest account is moved to the expired state and is then purged, based on the configured purge policy.

You can also specify the frequency (in days or weeks) at which the expired guest accounts must be purged. If you have selected the **Purge occurs every _ weeks** option, you can also specify the day and time for purging the expired accounts.

Step 4 Click **Save**. If you do not want to save any updates you made to the settings, click **Reset** to revert to the last saved values.

Add Custom Fields for Guest Account Creation

When providing guest access, you may want to collect information from your guests beyond just their names, email addresses, and phone numbers. Cisco ISE provides custom fields that you can use to collect additional information about guests that is specific to your company's needs. You can associate the custom fields with guest types and with the Self-Registered Guest and Sponsor portals. Cisco ISE does not provide any default custom fields.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Guest Access** > **Settings** > **Custom Fields**.

Step 2 Enter the **Custom Field Name**, pick a **Data Type** from the drop-down list, and enter **Tip Text** to help provide additional information about the custom field. For instance, if you enter Date of Birth, pick Date-MDY, and enter a tip for the date format as MM/DD/YYYY.

Step 3 Click **Add**.

The custom field appears in the list in alphabetical order or in the context of the sorted order.

Step 4 Click **Save**. If you do not want to save any updates you made to the settings, click **Reset** to revert to the last saved values.

Note If you delete a custom field, it will no longer be available for selection in the **Custom Fields** list for guest types and in the Self-Registered Guest and Sponsor portals settings. If the field is being used, **Delete** will be disabled.

What to do next

You can include the desired custom fields:

- When defining a guest type so that accounts created with that guest type will include this information. See Create or Edit Guest Types.
- When configuring the Sponsor portal for sponsors to use when creating guest accounts. See Customize Sponsor Portals, on page 522.
- When requesting information from self-registering guests using a Self-Registered Guest portal. See Create a Self-Registered Guest Portal, on page 506.

Specify Email Addresses and SMTP Servers for Email Notifications

Cisco ISE allows you to send emails to sponsors and guests, notifying them of information and instructions. You can configure SMTP servers to deliver these email notifications. You can also specify the email address from which the notifications will be sent to guests.

Note Guest notifications require an UTF-8 compatible e-mail client.

HTML-capable e-mail client (with functionality enabled) is needed to use the single click sponsor approval feature.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Settings** > **Guest Email Settings**.

Step 2 **Enable email notifications to guests** is checked by default. If you disable this setting, guests will not receive email notifications regardless of any other settings you may have enabled while configuring Guest and Sponsor portals.

Step 3 Enter the **Default "From" email address** that is designated for sending email notifications to guests. For example, donotreply@ *yourcompany*.com.

Step 4 Do one of the following:

- Check **Send notifications from sponsor's email address (if sponsored)** if you want guests to receive notifications from the sponsor who created their accounts. Self-registering guests will receive notifications from the default email address.
- Check **Always send notifications from the default email address** if you want guests to receive notifications, regardless of whether they are sponsored and self-registering.

Step 5 Click **Save**. If you do not want to save any updates you made to the settings, click **Reset** to revert to the last saved values.

Assign Guest Locations and SSIDs

A Guest Location defines a name for a time zone, and is used by ISE to enforce time-related settings of logged on Guests. Guest Locations are assigned to Guest accounts by Sponsors creating a Guest account, and by self-registering Guests. The default Guest Location is San Jose. If no other Guest Locations are added, all accounts are assigned this Guest Location. You can't delete the San Jose Guest Location unless you create one or more new Locations. Unless all your Guests will be in the same time-zone as San Jose, create at least one Guest Location with the required time-zone.

Note Guest access times are based on the Guest Location's time zone. A Guest user may not be able to login if the Guest Location's time zone doesn't match the system time zone. In this case, the Guest user may get an "Authentication Failed" error. You might see the "Guest active time period not yet started" error message in the debug report. As a workaround, you can adjust the Guest access start time to match the local time zone of the Guest user by using the Manage Accounts option.

The SSIDs you add here are available to Sponsor Portals, so Sponsors can tell the Guest which SSID to connect to.

You can't delete a Guest Location or a SSID if it is configured in a Sponsor portal or assigned to a Guest account.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Portals & Components** > **Settings** > **Guest Locations and SSIDs**.

Step 2 For **Guest Locations**:

a) For each time-zone that you need to support, enter a **Location name** and pick a **Time zone** from the drop-down list.

b) Click **Add**.

Note In a Guest Location, the name of the place, the name of the time zone, and the GMT offset are static; you cannot change them. The GMT offset does not change with daylight savings time changes. The GMT offsets are the opposite of what is shown in the list. For example, *Etc/GMT+3* is actually GMT-3.

Note For From First-login guest type, ensure that you configure a Guest Location (time zone) only if you intend to configure the access time restrictions in the **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Types** page.

Step 3 For **Guest SSIDs**:

a) Enter the **SSID** names of the networks that will be available for guests to use at the Guest Locations.

b) Click **Add**.

Step 4 Click **Save**. To revert to the last saved values, click **Reset**.

What to do next

If you added a new Guest Location or SSID, you can:

- Provide the SSIDs for Sponsors to use when creating Guest accounts. See Portal Settings for Sponsor Portals, on page 551.
- Add the Guest Locations to Sponsor Groups, so that Sponsors assigned to that group can use them when creating guest accounts. See Configure Sponsor Groups, on page 515.
- Assign the Guest Locations available to self-registering guests using a Self-Registered Guest portal. See Create a Self-Registered Guest Portal, on page 506.
- For existing guest accounts, edit them manually to add SSIDs or Locations.

Rules for Guest Password Policies

Cisco ISE has the following built-in rules for guest passwords:

- The Guest password policy applies to sponsor portals, self registered portals, accounts uploaded in a CSV file, passwords created using the ERS API, and user created passwords.
- Changes to the guest password policy do not affect existing accounts, until the guests passwords have expired and need to be changed.
- Passwords are case sensitive.
- The special characters <, >, /, space, comma, and % cannot be used.
- Minimum length and minimum required characters apply to all passwords.
- Passwords cannot match usernames.
- New passwords cannot match current passwords.
- Guests do not receive notifications before password expiration, unlike guest account expiration. When guest passwords expire, either sponsors can reset the password to a random password or guests can log in using their current login credentials and then change their password.

Note The guest default username is four alpabetic and password is four numeric characters. Short, easy to remember usernames and passwords are adequate for short-term guests. You can change the username and password length in ISE, if you desire.

Set the Guest Password Policy and Expiration

You can define a password policy for all Guest portals. A Guest password policy determines how the password is generated for all guest accounts. A password can be a mixture of alphabetic, numeric, or special characters.

You can also set the number of days after which guest passwords will expire, requiring guests to reset their passwords.

The Guest password policy applies to sponsor portals, self registered portals, accounts uploaded in a CSV file, passwords created using the ERS API, and user created passwords.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Guest Access** > **Settings** > **Guest Password Policy**.

Step 2 Enter the **Minimum password length** (in characters) for the guest passwords.

Step 3 Specify the characters from each character set that can be used by guests to create passwords.

Choose one of the following options under **Allowed Characters and Minimums** to specify the password policy for guests:

- Use all the characters from each character set.
- To prevent the use of certain characters, choose **Custom** from the drop-down menu, and delete these characters from the predefined and complete sets.

Step 4 Enter the minimum number of characters to use from each set.

The total number of required characters across the four character sets should not exceed the overall **Minimum password length**.

Step 5 Choose one of the following options under **Password Expiration**:

- Specify the frequency (in days) when guests have to change their passwords after they first log in. If the guests do not reset their passwords before they expire, the next time they log in to the network using their original login credentials, they are prompted to change their passwords.
- Set the passwords to never expire.

Step 6 Click **Save**. If you do not want to save any updates you made to the settings, click **Reset** to revert to the last saved values.

What to do next

You should customize the error messages that are related to the password policy to provide the password requirements.

1. Choose **Guest Access** > **Portals & Components** > **Sponsored-Guest Portals or Self-Registered Guest Portals** > **Edit** > **Portal Page Customization** > **Error Messages**.
2. Search for the keyword policy.

Rules for Guest Username Policies

Cisco ISE has the following built-in rules for guest username policies:

- Changes to the guest username policy do not affect existing accounts, until the guest accounts have expired and need to be changed.
- The special characters <, >, /, space, comma, and % cannot be used.
- Minimum length and minimum required characters apply to all system-generated usernames, including usernames based on email addresses.
- Passwords cannot match usernames.

Set the Guest Username Policy

You can configure rules for how guest usernames are created. A generated username can be created based on the email address, or based on the first name and last name of the guest. The Sponsor can also create a random number of guest accounts to save time when creating multiple guests, or when guest names and email addresses are not available. Randomly generated guest usernames consist of a mixture of alphabetic, numeric, and special characters. These settings affect all guests.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Portals & Components** > **Settings** > **Guest Username Policy**.

Step 2 Enter the **Minimum username length** (in characters) for the guest usernames.

Step 3 Choose one of the options under **Username Criteria for Known Guests** to specify the policy for creating usernames for known guests.

Step 4 Choose one of the following options under **Characters Allowed in Randomly-Generated Usernames** to specify the policy for creating random usernames for guests:

- Use all characters from each character set.
- To prevent the use of certain characters, choose **Custom** from the drop-down menu, and delete these characters from the predefined and complete sets.

Step 5 Enter the minimum number of characters to use from each set.

The total number of characters from the three character sets should not exceed the number specified in **Minimum username length**.

Step 6 Click **Save**. If you do not want to save any updates you made to the settings, click **Reset** to revert to the last saved values.

What to do next

You should customize the error messages that are related to the username policy to provide the username requirements.

1. Choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsored-Guest Portals, Self-Registered Guest Portals, Sponsor Portals, or My Devices Portals** > **Edit** > **Portal Page Customization** > **Error Messages**.
2. Search for the keyword `policy`.

SMS Providers and Services

SMS services send SMS notifications to guests that are using credentialed Guest portals. If you plan to send SMS messages, enable this service. Whenever possible, configure and provide free SMS service providers to lower your company's expenses.

Cisco ISE supports a variety of cellular service providers that provide free SMS services to their own subscribers. You can use these providers without a service contract and without configuring their account credentials in Cisco ISE. These include ATT, Orange, Sprint, T-Mobile, and Verizon.

You can also add other cellular service providers that offer free SMS services or a global SMS service provider, such as a Click-A-Tell. The default global SMS service provider requires a service contract and you must configure their account credentials in Cisco ISE.

- If self-registering guests pick their free SMS service provider on the Self-Registration form, SMS notifications with their login credentials are sent to them free of cost. If they do not pick an SMS service provider, then the default global SMS service provider that is contracted by your company sends the SMS notifications.
- To allow sponsors to send SMS notifications to guests whose accounts they created, customize the sponsor portal and select all the appropriate SMS service providers that are available. If you do not select any SMS service providers for the Sponsor portal, the default global SMS service provider that is contracted by your company provides the SMS services.

SMS providers are configured as SMS Gateways in Cisco ISE. Email from Cisco ISE is converted to SMS by the SMS gateway. The SMS gateway can be behind a proxy server.

Note Cisco ISE SMS gateway does not support authorization codes in JSON format.

Configure SMS Gateways to Send SMS Notifications to Guests

You must set up SMS gateways in Cisco ISE to enable:

- Sponsors to manually send SMS notifications to guests with their login credentials and password reset instructions.
- Guests to automatically receive SMS notifications with their login credentials after they successfully register themselves.
- Guests to automatically receive SMS notifications with actions to take before their guest accounts expire.

When entering information in the fields, you should update all text within **[ ]**, such as [USERNAME], [PASSWORD], [PROVIDER_ID], and so on, with information specific to your SMS provider's account.

Before you begin

Configure a default SMTP server to use for the SMS Email Gateway option.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **SMS Gateway** > **SMS Gateway Providers**.

Step 2 Click **Add**.

Step 3 Enter the following details to configure the SMS gateway:

Field Name	Usage Guidelines
SMS Gateway Provider Domain	Enter the provider domain, which is used as the host portion and the guest account's mobile number as the user portion of the email address to send the message to the provider's SMS/MMS gateway.

Field Name	Usage Guidelines
Provider account address	(Optional) Enter the account address, which is used as the FROM address (typically the account address) for the email and overrides the **Default Email Address** global setting in **Guest Access** > **Settings**.
SMTP API destination address	(Optional) Enter the SMTP API Destination Address, if you are using an SMTP SMS API that requires a specific account recipient address, such as Clickatell SMTP API. This is used as the TO address for the email and the guest account's mobile number is substituted into the message's body template.
SMTP API body template	(Optional) Enter the SMTP API Body Template, if you are using an SMTP SMS API that requires a specific email body template for sending the SMS, such as Clicketell SMTP API. The supported dynamic substitutions are $mobilenumber$, $timestamp$ (of format $YYYYMMDDHHMISSmimi$), and $message$. You can use $timestamp$$mobilenumber$ for SMS gateways that require a unique idenitifier in the URL.

Use these settings to configure sending SMS messages to guests and sponsors via an HTTP API (GET or POST method).

Field	Usage Guidelines
URL	Enter the URL for the API. This field is not URL encoded. The guest account's mobile number is substituted into the URL. The supported dynamic substitutions are $mobilenumber$ and $message$. If you are using HTTPS with the HTTP API, include HTTPS in the URL string and upload your provider's trusted certificates into Cisco ISE. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Trusted Certificates**.
Data (Url encoded portion)	Enter the Data (URL encoded portion) for the GET or POST request. This field is URL encoded. If using the default GET method, the data is appended to the URL specified above.
Use HTTP POST method for data portion	If you are using the POST method, check this option. The data specified above is used as the content of the POST request.

Field	Usage Guidelines
HTTP POST data content type	If you are using the POST method, specify the content type such as "plain/text" or "application/xml".
HTTPS Username HTTPS Password HTTPS Host name HTTPS Port number	Enter this information.

Step 4 (Optional) Check the **Enable Mobile Number Format** check box if you want to add a Javascript to format the mobile number before it is sent to the SMS provider.

Step 5 Click **Submit**.

What to do next

If you configured a new SMS gateway, you can:

- Select the SMS service provider to use when sending SMS notifications about expiring accounts to guests. See Create or Edit Guest Types.
- Specify which of the configured SMS providers should display on the Self-Registration form for self-registering guests to pick from. See Create a Self-Registered Guest Portal, on page 506.

Social Login for Self-Registered Guests

Guests can select a social media provider as a way to provide credentials as a self-registered guest, instead of entering username and password in the guest portal. To enable this, you configure a social media site as an external identity source, and configure a portal that allows users to use that external identity (social media provider). Additional information about social media login for Cisco ISE can be found here: https://community.cisco.com/t5/security-documents/how-to-configure-amp-use-a-facebook-social-media-login-on-ise/ta-p/3609532

After authenticating with social media, guests can edit the information retrieved from the social media site. Even though social media credentials are used, the social media site does not know that the user has used that site's information to log in. Cisco ISE still uses the information retrieved from the social media site internally for future tracking.

You can configure the guest portal to prevent users from changing the information retrieved from the social media site, or even suppress display of the registration form.

Social Login Guest Flow

Login flow varies, depending on how you configure the portal settings. You can configure social media login without user registration, with user registration, or with user registration and sponsor approval.

1. User connects to the self-registered portal, chooses to log in using social media. If you configured an access code, the user must also enter the access code on the login page.

2. The user is redirected to the social media site for authentication. The user must approve use of their social media site's basic profile information.
3. If the login to the social media site is successful, Cisco ISE retrieves additional information about the user from the social media site. Cisco ISE uses the social media information to log the user on.
4. After login, the user may have to accept the AUP, depending on configuration.
5. The next action in the login flow depends on the configuration:
   - Without registration: Registration is done behind the scenes. Facebook provides a token for the user's device to Cisco ISE for login.
   - With registration: The user is instructed to complete a registration form that has been prepopulated with information from the social media providers. This allows the user to correct and add missing information, and submit updated information for login. If you configured a registration code in the Registration Form Settings, the user must also enter the registration code.
   - With registration and sponsor approval: In addition to allowing the user to update the social media-provided information, the user is informed that they must wait for sponsor approval. The sponsor receives an email requesting approval or denial of the account. If the sponsor approves the account, Cisco ISE emails the user that they have access. The user connects the guest portal, and is automatically logged in with social media token.
6. Registration is successful. The user is directed to the option configured in **After submitting the guest form for self-registration, direct guest to** on **Registration Form Settings**. The user's account is added to the endpoint identity group configured for the portal's guest type.
7. The user has access until the guest account expires, or the user disconnects from the network.

   If the account expired, the only way to allow the user to log in is to reactivate the account, or to delete it. The user must go through the login flow again.

   If a user disconnects from the network, and reconnects, the action Cisco ISE takes depends on the authorization rules. If the user hits an authorization similar to:

   ```
   rule if guestendpoint then permit access
   ```

   and the user is still in the endpoint group, then the user is redirected to the logon page. If a user still has a valid token, they are automatically logged in. If not, the user must go through registration again.

   If the user is no longer in the endpoint group, the user is redirected to the guest page to go through registration.

Social Login Account Duration

Account re-authorization varies by connection method:

- For 802.1x, the default authorization rule

  ```
  if guestendpoint then permit access
  ```

  enables a guest to reconnect if the user device falls asleep, or if the user device roams to another building. When the user reconnects, the user is redirected back to guest page which either does auto login with a token, or starts registration again.

- For MAB, every time the user reconnects, the user is redirected to the guest portal, and needs to click the social media again. If Cisco ISE still has a token for that user's account (guest account hasn't expired), then the flow goes to log in success immediately, without having to connect with the social media provider.

  To prevent every reconnect redirecting to another social login, you can configure an authorization rule that remembers the device, and permits access until the account expires. When the account expires, it is removed from the endpoint group, and the flow is redirected back to the rule for guest redirect. For example:

  ```
  if wireless_mab and guest endpoint then permit access
  ```

  ```
  if wireless_mab then redirect to self-registration social media portal
  ```

Reporting and User Tracking

Cisco ISE Live Logs and Facebook

- **Authentication Identity Store**: This is the name of the application you created in your social media app for Cisco ISE.
- **Facebook username**: This is the username reported by Facebook. If you allow the user to change their username during registration, the name reported by Cisco ISE is the social media username.
- **SocialMediaIdentifier**: This is

  `https://facebook.com/<number>`

  where number identifies the social media user.

ISE Reports: The Guest username is the user's name on the social media site.

Facebook Analytics: You can see who is using your guest network through Facebook social logon by using analytics from Facebook.

Wireless and Facebook: The **User Name** on the Wireless controller is the unique Facebook ID, the same as the **SocialMediaIdentifier** on the Live Logs. To see the setting in the Wireless UI, choose **Monitor** > **Clients** > **Detail**, and look at the **User Name** field.

Block a Social Media-Authenticated Guest

You can create an authorization rule to block an individual social media user. This can be useful when using Facebook for authentication, when the token has not expired. The following example shows a Wi-Fi-connected guest user blocked by using their Facebook User Name.

Figure 12: WiFi-connected guest user is blocked by using their Facebook user name

Wi-Fi_Guest_Access

For information about configuring Social Login for Cisco ISE, see Configuring Social Login, on page 496.

Configuring Social Login

Before you begin

Configure the social media site so that Cisco ISE can connect to it. Only Facebook is supported currently.

Make sure the following HTTPS 443 URLs are open through your NADs so that Cisco ISE can access Facebook:

```
facebook.co
akamaihd.net
akamai.co
fbcdn.net
```

Note The social login URL for Facebook is HTTPS. Not all NADs support redirection to a HTTPS URL. See https://communities.cisco.com/thread/79494?start=0&tstart=0&mobileredirect=true.

Step 1 On Facebook, create a Facebook application:

a) Log on to https://developers.facebook.com and sign up as a developer.
b) Select **Apps** in the header and click **Add a New App**.

Step 2 Add a new **Product**, **Facebook Login**, of type **Web**. Click **Settings**, and set the following values:

- **Client OAuth Login**: NO
- **Web OAuth Login**: YES
- **Force Web OAuth Reauthentication**: NO
- **Embedded Browser OAuth Login**: NO
- **Valid OAuth redirect URIs**: Add the automated redirect URLs from the Cisco ISE
- **Login from Devices**: NO

Step 3 Click **App Review**, and select *Yes* for **Your app is currently live and available to the public**.

Step 4 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **Social Login**. Click **Add** to create a new social login external identity source.

- **Type**: Select the type of Social Login provider. Facebook is currently the only option.
- **App ID**: Enter the App ID from the Facebook application.
- **App Secret**: Enter the App Secret from the Facebook application.

Step 5 In Cisco ISE, enable **Social Media Login** in a self-registered portal. On the portal page, choose **Portal & Page Settings** > **Login Page Settings**, check the **Allow Social Login**check box, and enter the following details:

- **Show registration form after social login**: This allows the user to change the information provided by Facebook.
- **Require guests to be approved**: This informs the user that a sponsor must approve their account, and will send them credentials for login.

Step 6 Choose **Administration** > **External Identity Sources**, select the **Facebook Login** window, and edit your Facebook external identity source.
This creates redirect URIs, which you add to the Facebook application.

Step 7 In Facebook, add the URIs from the previous step to your Facebook application.

What to do next

In Facebook, you can display data about your app, which shows the guest activity with the Facebook Social Login.

Guest Portals

When people visiting your company wish to use your company's network to access the internet, or resources and services on your network, you can provide them network access through a Guest portal. Employees can use these Guest portals to access your company's network, if configured.

There are three default Guest portals:

- Hotspot Guest portal: Network access is granted without requiring any credentials. Usually, an Acceptance of User Policy (AUP) must be accepted before network access is granted.

- Sponsored-Guest portal: Network access is granted by a sponsor who creates accounts for guests, and provides the guest with login credentials.
- Self-Registered Guest portal: Guests can create their own account credentials, and may need sponsor approval before they are granted network access.

Cisco ISE can host multiple Guest portals, including a predefined set of default portals.

The default portal themes have standard Cisco branding that you can customize through the Admin portal.

Wireless Setup has its own default theme (CSS) and you are able to modify some basic settings such as logo, banner, background image, coloring and fonts. In Cisco ISE, you can also choose to further customize your portal by changing more settings and going into advanced customizations.

Credentials for Guest Portals

Cisco ISE provides secured network access by requiring guests to log in using various types of credentials. You can require that guests log in using one or a combination of these credentials.

- Username: Required. Applies to all guests using end-user portals (except Hotspot Guest portals) and is derived from the username policy. The username policy applies only to system-generated usernames and not to usernames specified using the Guest API programming interface or the self-registering process. You can configure the policy settings that apply to usernames at **Work Centers** > **Guest Access** > **Settings** > **Guest Username Policy**. Guests can be notified of their username in an email, SMS, or in printed form.
- Password: Required. Applies to all guests using end-user portals (except Hotspot Guest portals) and is derived from the password policy. You can configure the policy settings that apply to passwords at **Work Centers** > **Guest Access** > **Settings** > **Guest Password Policy**. Guests can be notified of their password in an email, SMS, or in printed form.
- Access code: Optional. Applies to guests using the Hotspot Guest and Credentialed Guest portals. An access code is primarily a locally known code that is given to physically present guests (either visually via a whiteboard or verbally by a lobby ambassador). It would not be known and used by someone outside the premises to gain access to the network. If the Access code setting is enabled:
    - Sponsored guests are prompted to enter it on the Login page (along with a username and password).
    - Guests using the Hotspot Guest portal are prompted to enter it on the Acceptable Use Policy (AUP) page.
- Registration code: Optional. Applies to self-registering guests and is similar to an access code in how it is provided to the self-registering guests. If the Registration code setting is enabled, self-registering guests are prompted to enter it on the Self-Registration form.

The username and password can be provided by a sponsor at your company (for sponsored guests), or a Credentialed Guest portal can be configured to allow guests to register themselves to obtain these credentials.

Note While doing bulk import of user entries in the guest portal, ensure that the phone numbers are provided in E.164 format. In addition, ensure that the format for the phone number column is set to Text in the Excel file.

Related Topics

Guest Types and User Identity Groups, on page 479

Guest Access with Hotspot Guest Portals

Cisco ISE provides network access functionality that includes “hotspots,” which are access points that guests can use to access the Internet without requiring credentials to log in. When guests connect to the hotspot network with a computer or any device with a web browser and attempt to connect to a website, they are automatically redirected to a Hotspot Guest portal. Both wired and wireless (Wi-Fi) connections are supported with this functionality.

The Hotspot Guest portal is an alternative Guest portal that allows you to provide network access without requiring guests to have usernames and passwords and alleviates the need to manage guest accounts. Instead, Cisco ISE works together with the network access device (NAD) and Device Registration Web Authentication (Device Registration WebAuth) to grant network access directly to the guest devices. Sometimes, guests may be required to log in with an access code. Typically, this is a code that is locally provided to guests who are physically present on a company’s premises.

If you support the Hotspot Guest portal:

- Based on the Hotspot Guest portal configuration and settings, guests are granted access to the network if the guest access conditions are met.
- Cisco ISE provides you with a default guest identity group, GuestEndpoints, which enables you to cohesively track guest devices.

Guest Access with Credentialed Guest Portals

You can use a credentialed Guest portal to identify and authorize temporary access for external users to internal networks and services, as well as to the Internet. Sponsors can create temporary usernames and passwords for authorized visitors who can access the network by entering these credentials in the portal's Login page.

You can set up a credentialed Guest portal so that guests can log in using a username and password that is obtained:

- From a sponsor. In this guest flow, guests are greeted by a sponsor, such as a lobby ambassador, when they enter company premises and are set up with individual guest accounts.
- After they register themselves, using an optional registration code or access code. In this guest flow, guests are able to access the Internet without any human interaction and Cisco ISE ensures that these guests have unique identifiers that can be used for compliance.
- After they register themselves, using an optional registration code or access code, but only after the request for a guest account is approved by a sponsor. In this guest flow, guests are provided access to the network, but only after an additional level of screening is done.

You can also force the user to enter a new password when logging in.

Cisco ISE enables you to create multiple credentialed Guest portals, which you can use to allow guest access based on different criteria. For example, you might have a portal for monthly contractors that is separate from the portal used for daily visitors.

Employee Access with Credentialed Guest Portals

Employees can also access the network using Credentialed Guest Portals by signing in using their employee credentials, as long as their credentials can be accessed by the identity source sequence configured for that portal.

Guest Device Compliance

When guests and non-guests access the network through credentialed Guest portals, you can check their devices for compliance before they are allowed to gain access. You can route them to a Client Provisioning window and require them to first download the posture agent that checks their posture profile and verifies if their device is compliant. You can do this by enabling the option in the **Guest Device Compliance Settings** in a credentialed Guest portal, which displays the Client Provisioning window as part of the guest flow.

Note Client posture assessment in guest flow supports only the Temporal agent.

The Client Provisioning service provides posture assessments and remediations for guests. The Client Provisioning portal is available only with a Central Web Authorization (CWA) guest deployment. The guest login flow performs a CWA, and the credentialed Guest portal is redirected to the Client Provisioning portal after performing acceptable-use-policy and change-password checks. The posture subsystem performs a Change of Authorization (CoA) on the network access device to reauthenticate the client connection once the posture has been assessed.

Guest Portals Configuration Tasks

You can use a default portal and its default settings such as certificates, endpoint identity group, identity source sequence, portal themes, images, and other details provided by Cisco ISE. If you do not want to use the default settings, you should create a new portal or edit an existing one to meet your needs. You can duplicate a portal if you want to create multiple portals with the same settings.

After creating a new portal or editing a default one, you must authorize the portal for use. Once you authorize a portal for use, any subsequent configuration changes you make are effective immediately.

If you choose to delete a portal, you must first delete any authorization policy rules and authorization profiles associated with it or modify them to use another portal.

Use this table for the tasks related to configuring the different Guest portals.

Task	Hotspot Guest Portal	Sponsored-Guest Portal	Self-Registered Guest Portal
Enable Policy Services, on page 501	Required	Required	Required
Add Certificates for Guest Portals, on page 501	Required	Required	Required
Create External Identity Sources, on page 502	Not applicable	Required	Required

Task	Hotspot Guest Portal	Sponsored-Guest Portal	Self-Registered Guest Portal
Create Identity Source Sequences, on page 503	Not applicable	Required	Required
Create Endpoint Identity Groups, on page 835	Required	Not required (defined by guest type)	Not required (defined by guest type)
Create a Hotspot Guest Portal, on page 504	Required	Not applicable	Not applicable
Create a Sponsored-Guest Portal, on page 504	Not applicable	Required	Not applicable
Create a Self-Registered Guest Portal, on page 506	Not applicable	Not applicable	Required
Authorize Portals, on page 510	Required	Required	Required
Customize Guest Portals, on page 511	Optional	Optional	Optional

Enable Policy Services

To support the Cisco ISE end-user web portals, you must enable the portal-policy services on the node on which you want to host them.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 2 Click the node and click **Edit**.

Step 3 Under the **General Settings** tab, enable the **Policy Service** toggle button.

Step 4 Check the **Enable Session Services** check box.

Step 5 Click **Save**.

Add Certificates for Guest Portals

If you do not want to use the default certificates, you can add a valid certificate and assign it to a certificate group tag. The default certificate group tag used for all end-user web portals is Default Portal Certificate Group.

Step 1

Step 2 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **System Certificates**.

Step 3 Add a system certificate and assign it to a certificate group tag that you want to use for the portal.

This certificate group tag will be available to select during portal creation or editing.

Step 4 Choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Create or Edit** > **Portal Settings**.

Step 5 Select the specific certificate group tag from the **Certificate group tag** drop-down list that is associated with the newly added certificate.

Create External Identity Sources

Cisco ISE can connect with external identity sources such as Active Directory, LDAP, RADIUS Token, and RSA SecurID servers to obtain user information for authentication and authorization. External identity sources also include certificate authentication profiles that you need for certificate-based authentications.

Note To work with passive identity services, which enable you to receive and share authenticated user identities, see Additional Passive Identity Service Providers, on page 690.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources**.

Step 2 Choose one of these options:

- **Certificate Authentication Profile** for certificate-based authentications.
- **Active Directory** to connect to an Active Directory as an external identity source. See Active Directory as an External Identity Source, on page 641 for more details.
- **LDAP** to add an LDAP identity source. See LDAP, on page 730 for more details.
- **RADIUS Token** to add a RADIUS Token server. See RADIUS Token Identity Sources, on page 752 for more details.
- **RSA SecurID** to add an RSA SecurID server. See RSA Identity Sources, on page 758 for more details.
- **SAML Id Providers** to add an identity provider (IdP), such as Oracle Access Manager. See SAMLv2 Identity Provider as an External Identity Source, on page 764 for more details.
- **Social Login** to add a Social Login, such as Facebook, as an external identity source. See Social Login for Self-Registered Guests, on page 493 for more details.

Configure Guest Portals to Redirect to SAML IDP Portals for Authentication

You can configure a Guest portal to allow users to be redirected to a SAML IDP portal for authentication.

Configuring the **Allow the following identity-provider guest portal to be used for login** option in a guest portal (self-registered or Sponsored Guest) enables a new login area in that portal. If a user selects that login option, they are redirected to the alternate identity portal (which they don't see), and then to the SAML IDP logon portal for authentication.

For example, the Guest portal could have a link for employee login. Instead of logging in on the existing portal, the user clicks the employee logon link, and is redirected to the SAML IDP single-signon portal. The employee is either reconnected using the token from the last logon with this SAML IDP, or logs in on that SAML site. That allows the same portal to handle both guests and employees from a single SSID.

The following steps show how to configure a Guest portal that calls another portal which is configured to use a SAML IDP for authentication.

Step 1 Configure an external identity source. See SAMLv2 Identity Provider as an External Identity Source, on page 764 for more details.

Step 2 Create a guest portal for the SAML provider. Set the **Authentication method** in Portal Settings to the SAML provider. The user will not see this portal, it is just a placeholder to direct the user to the SAML IDP logon page. Other portals can be configured to redirect to this sub-portal, as described next.

Step 3 Create a guest portal with the option to redirect to the guest portal for the SAML provider portal that you just created. This is the main portal, which will redirect to the sub-portal.

You may want to customize the look of this portal to make it look like the SAML provider.

a) On the Login Page Settings page of the main portal, **check Allow the following identity-provider guest portal to be used for login**.

b) Select the guest portal that you configured to use with the SAML provider.

Create Identity Source Sequences

Before you begin

Ensure that you have configured your external identity sources in Cisco ISE.

To perform the following task, you must be a Super Admin or System Admin.

For allowing guest users to authenticate through Local WebAuth, you must configure both the Guest portal authentication source and the identity source sequence to contain the same identity stores.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **Identity Source Sequences** > **Add**.

Step 2 Enter a name for the identity source sequence. You can also enter an optional description.

Step 3 Check the **Select Certificate Authentication Profile** check box and choose a certificate authentication profile for certificate-based authentication.

Step 4 Choose the database or databases that you want to include in the identity source sequence in the **Selected List** field.

Step 5 Rearrange the databases in the **Selected list** field in the order in which you want Cisco ISE to search the databases.

Step 6 If a selected identity store cannot be accessed for authentication, choose one of the following options in the **Advanced Search List** area:

- **Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError**
- **Treat as if the user was not found and proceed to the next store in the sequence**

  While processing a request, Cisco ISE searches these identity sources in sequence. Ensure that you have the identity sources in the Selected list field listed in the order in which you want Cisco ISE to search them.

Step 7 Click **Submit** to create the identity source sequence that you can then use in policies.

Create Endpoint Identity Groups

Cisco ISE groups endpoints that it discovers in to the corresponding endpoint identity groups. Cisco ISE comes with several system-defined endpoint identity groups. You can also create additional endpoint identity groups from the **Endpoint Identity Groups** window. You can edit or delete the endpoint identity groups that you have created. You can only edit the description of the system-defined endpoint identity groups. You cannot edit the name of these groups or delete them.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **Groups** > **Endpoint Identity Groups**.

Step 2 Click **Add**.

Step 3 Enter the **Name** for the endpoint identity group that you want to create (do not include spaces in the name of the endpoint identity group).

Step 4 Enter the **Description** for the endpoint identity group that you want to create.

Step 5 Click the **Parent Group** drop-down list to choose an endpoint identity group to which you want to associate the newly created endpoint identity group.

Step 6 Click **Submit**.

Create a Hotspot Guest Portal

You can provide a Hotspot Guest portal to enable guests to connect to your network without requiring a username and password to log in. An access code can be required to log in.

You can create a new Hotspot Guest portal, or you can edit or duplicate an existing one. You can delete any Hotspot Guest portal, including the default portal provided by Cisco ISE.

Any changes that you make to the Page Settings on the **Portal Behavior and Flow Settings** tab are reflected in the graphical flow in the Guest Flow diagram. If you enable a page, such as the AUP page, it appears in the flow and the guest will experience it in the portal. If you disable it, it is removed from the flow and the next enabled page displays for the guest.

All the Page Settings, except the Authentication Success Settings, are optional.

Before you begin

- Ensure that you have the required certificates and endpoint identity groups configured for use with this portal.
- Ensure that the WLC that guests connect to for the Hotspot portal is supported by Cisco ISE. See the Identity Services Engine Network Component Compatibility guide for your version of Cisco ISE.

What to do next

You must authorize the portal in order to use it. You can also customize your portal either before or after you authorize it for use.

Create a Sponsored-Guest Portal

You can provide a Sponsored-Guest portal to enable designated sponsors to grant access to guests.

You can create a new Sponsored-Guest portal, or you can edit or duplicate an existing one. You can delete any Sponsored-Guest portal, including the default portal provided by Cisco ISE.

Any changes that you make to the Page Settings on the **Portal Behavior and Flow Settings** tab are reflected in the graphical flow in the Guest Flow diagram. If you enable a page, such as the AUP page, it appears in the flow and the guest will experience it in the portal. If you disable it, it is removed from the flow and the next enabled page displays for the guest.

All these page settings enable you to display an Acceptable Use Policy (AUP) for a guest and require its acceptance:

- Login Page Settings
- Acceptable Use Policy (AUP) Page Settings
- BYOD Settings

Before you begin

Ensure that you have the required certificates, external identity sources, and identity source sequences configured for use with this portal.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Create, Edit or Duplicate**.

Step 2 If creating a new portal, in the **Create Guest Portal** dialog box, select **Sponsored-Guest Portal** as the portal type and click **Continue**.

Step 3 Provide a unique **Portal Name** and a **Description** for the portal.

Ensure that the portal name that you use here is not used for any other end-user portals.

Step 4 Use the **Language File** drop-down menu to export and import language files to use with the portal.

Step 5 Update the default values for ports, Ethernet interfaces, certificate group tags, identity source sequences, authentication method, and so on in **Portal Settings**, and define behavior that applies to the overall portal.

Step 6 Update the following settings, which apply to each of the specific pages:

- **Login Page Settings**: Specify guest credential and login guidelines. If you select the **Allow guests to create their accounts** option, users will be able to create their own guest accounts. If this option is not selected, sponsors will be required to create guest accounts.

  Note Login Page Settings option will be disabled if you have selected an identity provider (IdP) in the Authentication Method field.

- **Acceptable Use Policy (AUP) Page Settings**: Add a separate AUP page and define the acceptable use policy behavior for guests, including employees who use the credentialed Guest portals.
- **Employee Change Password Settings**: Require guests to change their password after the first time they log in.
- **Guest Device Registration Settings**: Select whether Cisco ISE automatically registers guest devices or displays a page where guests can manually register their devices.
- **BYOD Settings**: Let employees use their personal devices to access the network.
- **Post-Login Banner Page Settings**: Notify guests of additional information before they are granted network access.
- **Guest Device Compliance Settings**: Route guests to the Client Provisioning page and require them to first download the posture agent.
- **VLAN DHCP Release Page Settings**: Release the guest device IP address from the guest VLAN and renew it to access another VLAN on the network.

- **Authentication Success Settings**: Specify what guests should see once they are authenticated.
- **Support Information Page Settings**: Help guests provide information that the Help Desk can use to troubleshoot network access issues.

Step 7 Click **Save**. A system-generated URL displays as the **Portal test URL**, which you can use to access the portal and test it.

What to do next

Note The test portal does not support RADIUS sessions, so you won't see the entire portal flow for all portals. BYOD and Client Provisioning are examples of portals that depend on RADIUS sessions. For example, a redirect to an external URL will not work. If you have more than one PSN, ISE chooses the first active PSN.

You must authorize the portal in order to use it. You can also customize your portal either before or after you authorize it for use.

Create a Self-Registered Guest Portal

You can provide a Self-Registered Guest portal to enable guests to register themselves and create their own accounts so they can access the network. You can still require that these accounts be approved by a sponsor before access is granted.

You can create a new Self-Registered Guest portal, or you can edit or duplicate an existing one. You can delete any Self-Registered Guest portal, including the default portal provided by Cisco ISE.

Any changes that you make to the Page Settings on the **Portal Behavior and Flow Settings** tab are reflected in the graphical flow in the Guest Flow diagram. If you enable a page, such as the AUP page, it appears in the flow and the guest will experience it in the portal. If you disable it, it is removed from the flow and the next enabled page displays for the guest.

All these page settings enable you to display an Acceptable Use Policy (AUP) for a guest and require its acceptance:

- Login Page Settings
- Self-Registration Page Settings
- Self-Registration Success Page Settings
- Acceptable Use Policy (AUP) Page Settings
- BYOD Settings

Before you begin

Ensure that you have configured the required certificates, external identity sources, and identity source sequences for this portal.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Create, Edit or Duplicate.**.

Step 2 If creating a new portal, in the **Create Guest Portal** dialog box, select **Self-Registered Guest Portal** as the portal type and click **Continue**.

Step 3 Provide a unique **Portal Name** and a **Description** for the portal.

Ensure that the portal name that you use here is not used for any other end-user portals.

Step 4 Use the **Language File** drop-down menu to export and import language files to use with the portal.

Step 5 In **Portal Settings**, update the default values for ports, Ethernet interfaces, certificate group tags, identity source sequences, authentication method,, and other settings that define behavior of this portal.

For more information about Portal Settings fields, see Portal Settings for Credentialed Guest Portals, on page 538.

Step 6 Update the following settings, which apply to each of the specific pages:

- **Login Page Settings**: Specify guest credential and login guidelines. For more information, see Login Page Settings for Credentialed Guest Portals, on page 540.
- **Self-Registration Page Settings**: Specify the information self-registering guests will read and should enter on the Self-Registration form, in addition to the guest experience after they have submitted the form.
- **Acceptable Use Policy (AUP) Page Settings**: Add a separate AUP page and define the acceptable use policy behavior for guests, including employees who use the credentialed Guest portals. For more information, see Acceptable Use Policy (AUP) Page Settings for Credentialed Guest Portals, on page 545.
- **Employee Change Password Settings**: Require guests to change their password after the first time they log in.
- **Guest Device Registration Settings**: Select whether Cisco ISE automatically registers guest devices or displays a page where guests can manually register their devices.
- **BYOD Settings**: Let employees use their personal devices to access the network. For more information, see BYOD Settings for Credentialed Guest Portals, on page 546.
- **Post-Login Banner Page Settings**: Display additional information after the user successfully logs in, and before they are granted network access.
- **Guest Device Compliance Settings**: Redirects guests to the Client Provisioning page for posture assessment. For more information, see Guest Device Compliance Settings for Credentialed Guest Portals, on page 548.
- **VLAN DHCP Release Page Settings**: Release the guest device IP address from the guest VLAN and renew it to access another VLAN on the network. For more information, see BYOD Settings for Credentialed Guest Portals, on page 546.
- **Authentication Success Settings**: Specify where to direct guests after they are authenticated. If you redirect a Guest to an external URL after authentication, there may be a delay while the URL address is resolved and the session is redirected. For more information, see Authentication Success Settings for Guest Portals, on page 549.
- **Support Information Page Settings**: Help guests provide information that the Help Desk can use to troubleshoot network access issues.

Step 7 Click **Save**. A system-generated URL displays as the **Portal test URL**, which you can use to access the portal and test it.

What to do next

Note The test portal does not support RADIUS sessions, so you won't see the entire portal flow for all portals. BYOD and Client Provisioning are examples of portals that depend on RADIUS sessions. For example, a redirect to an external URL will not work. If you have more than one PSN, ISE chooses the first active PSN.

You must authorize the portal in order to use it. You can also customize your portal either before or after you authorize it for use.

Self-Registered Account Approval by a Sponsor

When you configure a registered guest to require approval of their account, Cisco ISE sends email to the approver to approve the account. The approver can either be the person being visited, or a sponsor user.

When the approver is a sponsor, you can configure the email to include links that deny or approve the account. The approval link contains a token, which ties the approval to the sponsor's email address. You can require the sponsor to authenticate, which ignores the token. The token can also time out, which requires the sponsor to authenticate before approving the account.

You configure account approval options on the Self-Registration Portal's **Registration Form Settings**. This feature is also called single-click sponsor approval.

When the sponsor opens the email, and clicks the approve link, the action varies depending on configuration of the approver.

If **Email approval request to** is configured as:

- **person being visited**
  - And the guest account **does not** require authentication: A single click approves the account.
  - And the guest account **does** require authentication: The sponsor is directed to the sponsor portal, where the sponsor must enter their credentials before they can approve the account.
- **Sponsor email addresses listed below**: Cisco ISE sends emails to all the provided email addresses. When one of those sponsors clicks the approve or deny link, they are directed to their sponsor portal. That sponsor enters their credentials, which are verified. If the sponsor group that they belong to allows them to approve the guest account, they can approve the account. If credentials fail, then Cisco ISE notifies the sponsor to log on to the sponsor portal, and approve the account manually.

Considerations

- If your are upgrading or restoring the database from previous version of Cisco ISE, you must manually insert approve or deny links. Open the Self-Registered guest portal and choose the Portal Page Customization tab. Scroll down and choose the Approval Request Email window. Click **Insert Approve/Deny Links** in the **Email Body** section of that window.
- Only Sponsor portals that authenticate with Active Directory and LDAP are supported. The sponsor group that the sponsor maps to must contain the Active Directory group that the sponsor belongs to.
- When there is a list of sponsors, the customization from the first portal is used, even if that is not the portal that the sponsor logs on to.
- The sponsor must use an HTM-capable email client to use the approve and deny links.
- If the email address for the sponsor is not for a valid sponsor, the approval email is not sent.

For more information about single-click sponsor approval, see the Cisco ISE community resource: **ISE Single Click Sponsor Approval FAQ**. This document also has a link to a video that explains the entire process.

Configuring Account Approval Email Links

You can require that a self-registered guest is approved before gaining access to the network. Cisco ISE uses the email address of the person being visited to notify the approver. The approver is either the person being visitited, or a sponsor. For more information about approval, see Self-Registered Account Approval by a Sponsor, on page 508.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Guest** > **Configure** > **Guest Portals**. Select the self-registered portal that you want to configure for email account approval links.

Step 2 Expand the **Self-Registration Page Settings** tab.

Step 3 Check **Require self-registered guests to be approved**.

Approve/Deny Link Settings section appears. It also populates the email configuration of the Approval Request Email with approve and deny links.

Enter the following details:

- **Require self-registered guests to be approved**: Specify that the self-registering guests using this portal require approval from a sponsor before receiving their guest credentials. Clicking this option displays more options for how sponsors approve a self-registered guest.
  - **Allow guests to login automatically from self-registration after sponsor's approval**: A self-registered guest will be logged in automatically after sponsor approval.
  - **Email approval request to**:
    - **Sponsor email addresses listed below**: Enter one or more email addresses of sponsors designated as approvers, or a mailer, to which all guest approval requests should be sent. If the email address is not valid, approval fails.
    - **Person being visited**: **Require sponsor to provide credentials for authentication** field is displayed, and the **Required** option in **Fields to include** is enabled (if it was previously disabled). These fields are displayed on the Self-Registration form requesting this information from the self-registering guests. If the email address is not valid, approval fails.
  - **Approve/Deny Link Settings**:
    - **Links are valid for**: You can set an expiration period for the account approval links.
    - **Require sponsor to provide credentials for authentication**: Check this to force the sponsor to enter credentials to approve the account, even if it is not required by the configuration in this section. This field is only visible if **Require self-registered guests to be approved** is set to **person being visited**.
    - **Sponsor is matched to a Sponsor Portal to verify approval privileges**: Click **Details** to select the portals that are searched to verify that the sponsor is a valid system user, a member of a sponsor group, and that the members of that group have authority to approve the account. Each sponsor portal has an identity source sequence, which is used to identify the sponsor. Portals are used in the order they are listed. The first portal in the list determines the style and customization used in the sponsor portal.

Authorize Portals

When you authorize a portal, you are setting up the network authorization profiles and rules for network access.

Before you begin

You must create a portal before you can authorize it.

Step 1 Set up a special authorization profile for the portal.

Step 2 Create an authorization policy rule for the profile.

Create Authorization Profiles

Each portal requires that you set up a special authorization profile for it.

Before you begin

If you do not plan to use a default portal, you must first create the portal so you can associate the portal name with the authorization profile.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.

Step 2 Create an authorization profile using the name of the portal that you want to authorize for use.

What to do next

You should create a portal authorization policy rule that uses the newly created authorization profile.

Create Authorization Policy Rules for Hotspot and MDM Portals

To configure the redirection URL for a portal to use when responding to the users' (guests, sponsors, employees) access requests, define an authorization policy rule for that portal.

The url-redirect takes the following form based on the portal type, where:

ip:port : the IP address and port number

PortalID: the unique portal name

For a Hotspot Guest portal: https://*ip:port*/guestportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=cwa&type=drw

For a Mobile Device Management (MDM) portal: https://*ip:port*/mdmportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=mdm

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Sets** to create a new authorization policy rule under **Standard** policies.

Step 2 For **Conditions**, select an endpoint identity group that you want to use for the portal validation. For example, for the Hotspot Guest portal, select the default **GuestEndpoints** endpoint identity group and, for the MDM portal, select the default **RegisteredDevices** endpoint identity group.

Note Reauthenticate and Terminate CoA types are supported by Hotspot Guest portals. You can use Network Access:UseCase EQUALS Guest Flow as one of the validation conditions in the Hotspot Guest authorization policy only when Reauthentication CoA type is chosen in the Hotspot Guest Portal.

Step 3 For **Permissions**, select the portal authorization profile that you created.

Note While creating an authorization condition using a dictionary attribute with the MAC option enabled, such as RADIUS.Calling-Station-ID, you must use a Mac operator (for example, Mac_equals) to support different MAC formats.

Customize Guest Portals

You can customize the portal appearance and user (guests, sponsors, or employees as applicable) experience by customizing the portal themes, changing UI elements on the portal pages, and editing error messages and notifications that are displayed to the users. For more information about customizing portals, see Customization of End-User Web Portals , on page 563.

Configure Periodic AUP Acceptance

Choose **Policy** > **Policy Sets**, and create a new authorization rule at the top of the list that redirects the Guest user to a credentialed portal when the AUP period has expired. Use conditions to compare LastAUPAcceptanceHours against the desired maximum hours, for example, LastAUPAcceptanceHours > 8. You can check for a range of hours from 1 to 999.

What to do next

To verify that the endpoint has received the AUP settings:

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identities** > **Endpoints**.
2. Click an endpoint to verify that the endpoint has the time that the AUP was last accepted (*AUPAcceptedTime*).

Forcing Periodic AUP

You can force a user to accept the AUP by using LastAUPAcceptance in a policy.

```
If LastAUPAcceptance >= 24: Hotspot Redirect
```

```
If LastAUPacceptance < 24: PermitAccess
```

```
If Wireless_MAB: Hotspot Redirect
```

This example shows how to force AUP on a hotspot portal every 24 hours.

1. If the user accepted AUP more than 24 hours ago, then the must accept AUP (start over).
2. If the user accepted AUP less than 24 hours ago, continue the session.
3. On the first access to the network (MAB), they must accept AUP.

The same rules can be used with a credentialed portal, as long as you enable AUP for that portal.

Note

- To ensure communication of the guest AUP page to the endpoint, add the LastAUPAcceptanceHours condition to the Redirection Authorization Rule for guest portal as follows:

```
If AUP <= "X hours": Add in the Permit Access Rule
```

```
If AUP > "X hours": Add in the Redirection Rule
```

- New users can configure the Redirection Authorization rule without the LastAUPAcceptanceHours condition.

Guest Remember Me

This feature enables Cisco ISE to show a guest's username instead of MAC address in reports and logs.

When a guest first authenticates, the MAC address of user device is saved in the endpoint group, and the username is used in reports. If the user disconnects, and then reconnects to the network, the MAC address is already in the endpoint group, so the user does not have to log back in again (authenticate). In this case, the username is not available, so the MAC address is used in reporting and logs.

Cisco ISE keeps the portal user ID, and uses it in some reporting. To disable this feature, go to **Guest** > **Settings** > **Logging**. It is enabled by default on new installations.

For more information about Remember Me logging issues, see the following Cisco ISE community resource: ISE 2.3+ Remember Me guest using guest endpoint group logging display.

For more information about configuring remember me, see the Cisco ISE Guest Access Deployment guide: https://communities.cisco.com/docs/DOC-77590

For more information about which reporting methods are supported in each release, see the release notes for that release.

Sponsor Portals

The Sponsor portal is one of the primary components of Cisco ISE guest services. Using the Sponsor portal, sponsors can create and manage temporary accounts for authorized visitors to securely access the corporate network or the Internet. After creating a guest account, sponsors also can use the Sponsor portal to provide account details to the guest by printing, emailing, or texting. Before providing self-registering guests access to the company network, sponsors may be requested via email to approve their guests' accounts.

Managing Guest Accounts on the Sponsor Portal

Sponsor Portal Log on Flow

A sponsor group specifies a set of permissions that are assigned to a sponsor user. When a sponsor logs in to a sponsor portal:

1. ISE verifies the sponsor's credentials.
2. If the sponsor authenticates successfully, Cisco ISE searches all the available sponsor groups to find the sponsor groups that the sponsor belongs to. A sponsor matches or belongs to a sponsor group if both:
    - The sponsor is a member of one of the configured Member Groups.
    - If you are using Other Conditions, all the conditions evaluate to true for that sponsor.
3. If the sponsor belongs to a sponsor group, then that sponsor gets the permissions from that group. A sponsor can belong to more than one sponsor group, in which case the permissions from those groups are combined. If the sponsor does not belong to any sponsor group, then the login to the sponsor portal fails.

Sponsor groups and their permissions are independent of the sponsor portals. The same algorithm for matching sponsor groups is used, regardless of which sponsor portal the sponsor logs in to.

Using a Sponsor Portal

Use a Sponsor portal to create temporary guest accounts for authorized visitors to securely access your corporate network or the Internet. After creating guest accounts, you can use a Sponsor portal to manage these accounts and to provide account details to the guests.

On a Sponsor portal, the sponsor can create new guest accounts individually, or import a group of users from a file.

Note An ISE administrator authorized from an external identity store, such as Active Directory, can be part of a Sponsor group. However, internal administrator accounts, for example, the default "admin" account, cannot be part of a Sponsor group.

There are several ways to open a Sponsor portal:

- In the Administrators console, using the **Manage Accounts** link. On the Administrators console, click **Guest Access > Manage Accounts**. When you click **Manage Accounts**, you are assigned to the default sponsor group with access to ALL_ACCOUNTS. You can create new guest accounts, but those guests cannot be notified, because there is no email address available to receive the account activation request from the guest. A Sponsor with the same privileges who logs on to the sponsor portal, and searches for those accounts, can send notification.

  This step requires that the FQDN that you configured on the sponsor portal's **Portal Behavior and Flow Settings** window is in your DNS server.

  If you are accessing the Sponsor portal through a NAT firewall, the connection uses port 9002.

- In the Administrators console, on the Sponsor Portal configuration window. Click **Guest Access** > **Portals & Components** > **Sponsor Portals**, open a sponsor portal, and click the **Portal Test URL** link to the right of the **Description** field.

- In a browser, by opening the URL (FQDN) configured in the sponsor portal's **Portal Settings** window, which must be defined in your DNS server.

What to do Next

For information aboouit how to use the Sponsor portal, see the Sponsor Portal User Guide for your version of ISE https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html.

Managing Sponsor Accounts

A sponsor user is an employee or contractor of your organization who creates and manages guest-user accounts through the sponsor portal. Cisco ISE authenticates sponsors through a local database, or through external Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory, or SAML identity stores. If you are not using an external source, you must create internal user accounts for sponsors.

Sponsor Groups

Sponsor groups control the permissions given to a sponsor when using any Sponsor portal. If a sponsor is a member of a sponsor group, then the sponsor receives the permissions defined in the group.

A sponsor is considered to be a member of a sponsor group if both of the following are true:

1. The sponsor belongs to at least one of the Member Groups defined in the sponsor group. A Member Group can be a User Identity Group, or a group selected from an external identity source, such as Active Directory.
2. The sponsor satisfies all of the Other Conditions specified in the sponsor group. The Other Conditions, which are optional, are conditions defined on dictionary attributes. These conditions are similar in behavior to those used in an Authorization Policy.

A sponsor can be a member of more than one sponsor group. If so, the sponsor receives the combined permissions from all of those groups, as follows:

- An individual permission such as "Delete guests' accounts" is granted if it is enabled in any of the groups.
- The sponsor can create guests using the Guest Types in any of the groups.
- The sponsor can create guests at the locations in any of the groups.
- For a numeric value such as a batch size limit, the largest value from the groups is used.

If a sponsor is not a member of any sponsor group, then the sponsor is not permitted to log in to any sponsor portal.

- ALL_ACCOUNTS: Sponsors can manage all guest accounts.
- GROUP_ACCOUNTS: Sponsors can manage the guest accounts created by sponsors from the same Sponsor Group.
- OWN_ACCOUNTS: Sponsors can manage only the Guest accounts that they created.

You can customize the features available to particular sponsor groups to limit or expand the functionality of the Sponsor portal.

Create Sponsor Accounts and Assign to Sponsor Groups

To create internal sponsor user accounts and specify the sponsors who can use the Sponsor portals:

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **Identities** > **Users**. Assign the internal sponsor user account to the appropriate user identity group.

Note The default Sponsor Groups have the default Identity Group Guest_Portal_Sequence assigned to them.

Step 2 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Groups** > **Create, Edit or Duplicate** and click **Members**. Map the sponsor user identity groups to sponsor groups.

What to do next

You can also create additional user identity groups specific to your organization to use with sponsors. Choose **Administration** > **Identity Management** > **Groups** > **User Identity Groups**.

Configure Sponsor Groups

Cisco provides default sponsor groups. If you do not want to use the default options, you can either create new sponsor groups or edit the default sponsor groups and change the settings. You can also duplicate a sponsor group to create more sponsor groups with the same settings and privileges.

You can disable a sponsor group, which prevents the members of the sponsor group from logging in to the Sponsor portal. You can delete any of the sponsor groups, except the default sponsor groups provided by Cisco ISE.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals and Components** > **Sponsor Groups** > **Create, Edit or Duplicate**.

Step 2 Enter the **Sponsor group name** and **Description**.

Step 3 Enter the following details in the **Match Criteria** section:

- **Member Groups**: Click **Members** to select one or more user (identity) groups and groups from external identity sources, and add those groups. In order for a user to be a member of this sponsor group, they must belong to at least one of the configured groups.
- **Other conditions**: Click **Create New Condition** to build one or more conditions that a sponsor must match to be included in this sponsor group. You can use authentication attributes from Active Directory, LDAP, SAML, and ODBC identity stores, but not RADIUS Token or RSA SecurID stores. You can also use internal user attributes. Conditions have an attribute, and operator, and a value.
    - To create a condition using the internal dictionary attribute *Name*, prefix the identity group name with User Identity Groups. For example:

      InternalUser:Name EQUALS bsmith

      This means that only internal users with the Name "bsmith" can belong to this sponsor group.
    - To create a condition using the ExternalGroups attribute of an Active Directory instance, select the AD “Primary Group” for the sponsor users you want to match. For example, *AD1:LastName EQUALS Smith* is true if the user’s name is Smith.

In addition to matching one or more of the configured member groups, a sponsor must also match **all** the conditions you create here. If an authenticating sponsor user meets the matching criteria for multiple sponsor groups, then that user is granted permissions as follows:

- An individual permission, such as Delete guests' accounts is granted if it is enabled in any of the matching groups.
- The sponsor can create guests using the Guest Types in any of the matching groups.
- The sponsor can create guests using the Guest Types in any of the matching groups.
- The sponsor can create guests at the locations in any of the matching groups.
- For a numeric value such as a batch size limit, the largest value from the matching groups is used.

You can create Matching Criteria that contain Member Groups only, or Other Conditions only. If you only specify Other Conditions, then membership of a sponsor in the sponsor group is determined solely by matching dictionary attributes.

Step 4 To specify which guest types that sponsors based on this sponsor group can create, click **This sponsor group can create accounts using these guest types**, and select one or more guest types.

You can create more guest types to assign to this sponsor group by clicking the link under **Create Guest Types at**. After you create a new guest type, save, close, and reopen the sponsor group before you can select that new guest type.

Step 5 Use **Select the locations that guests will be visiting** to specify the locations (used to set the guest time zones) that sponsors in this sponsor group can choose from when creating guest accounts.

You can add more locations to choose from by clicking the link under **Configure guest locations at** and adding guest locations. After you create a new guest location, save, close, and reopen the sponsor group before you can select that new guest location.

This does not restrict guests from logging in from other locations.

Step 6 Under **Automatic guest notification**, check **Automatically email guests upon account creation if email address is available** if you want to save your sponsors the step of clicking **Notify** after creating a user. This causes a window to popup saying that an email was sent. Checking this also adds a header to the sponsor portal that says **Guest notifications are sent automatically**.

Step 7 Under **Sponsor Can Create**, configure options that sponsors in this group have for creating guest accounts.

- **Multiple guest accounts assigned to specific guests (Import)**: Enable the sponsor to create multiple guest accounts by importing guest details such as first name and last name from a file.

  If this option is enabled, the **Import** option appears on the **Create Accounts** window of the Sponsor portal. The Import option is only available on desktop browsers (not mobile), such as Internet Explorer, Firefox, Safari, and so forth

- **Limit to batch of**: If this sponsor group is allowed to create multiple accounts simultaneously, specify the number of guest accounts that can be created in a single import operation.

  Although a sponsor can create a maximum of 10,000 accounts, we recommend that you limit the number of accounts you create, due to potential performance issues.

- **Multiple guest accounts to be assigned to any guests (Random)**: Enable the sponsor to create multiple random guest accounts as placeholders for guests who are not known as yet, or to create many accounts quickly.

  If this option is enabled, the **Random** option appears on the **Create Accounts** window of the Sponsor portal.

- **Default username prefix**: Specify a username prefix that sponsors can use when creating multiple random guest accounts. If specified, this prefix appears in the Sponsor Portal when creating random guest accounts. In addition, if **Allow sponsor to specify a username prefix** is:
    - Enabled: The sponsor can edit the default prefix in the Sponsor portal.
    - Not enabled: The sponsor cannot edit the default prefix in the Sponsor portal.

  If you do not specify a username prefix or allow the sponsor to specify one, then the sponsor will not be able to assign username prefixes in the Sponsor portal.

- **Allow sponsor to specify a username prefix**: If this sponsor group is allowed to create multiple accounts simultaneously, specify the number of guest accounts that can be created in a single import operation.

  Although a sponsor can create a maximum of 10,000 accounts, we recommend that you limit the number of accounts you create, due to potential performance issues.

Step 8 Under **Sponsor Can Manage**, you can restrict which guests accounts the members of this sponsor group can view and manage.

- **Only accounts sponsor has created**: Sponsors in this group can view and manage only the guest accounts that they have created, which is based on the Sponsor's email account.
- **Accounts created by members of this sponsor group**: Sponsors in this group can view and manage the guest accounts created by any sponsor in this sponsor group.
- **All guest accounts**: Sponsors view and manage all pending guest accounts.

Step 9 Under **Sponsor Can**, you can provide more privileges related to guest passwords and accounts to the members of this sponsor group.

- **Update guests' contact information (email, Phone Number)**: For guest accounts that they can manage, allow the sponsor to change a guest's contact information
- **View/print guests' passwords**: When this option is enabled, the sponsor can print passwords for guests. The sponsor can see the passwords for guests on the **Manage Accounts**window and in the details for a guest. When this is not checked, the sponsor can't print the password, but the user can still get the password through email or SMS, if configured.
- **Send SMS notifications with guests' credentials**: For guest accounts that they can manage, allow the sponsor to send SMS (text) notifications to guests with their account details and login credentials.
- **Reset guest account passwords**: For guest accounts that they can manage, allow the sponsor to reset passwords for guests to a random password generated by Cisco ISE.
- **Extend guests' accounts**: For guest accounts that they can manage, allow the sponsor to extend them beyond their expiration date. The sponsor is automatically copied on email notifications sent to guests regarding their account expiration.
- **Delete guests' accounts**: For guest accounts that they can manage, allow the sponsor to delete the accounts, and prevent guests from accessing your company's network.
- **Suspend guests' accounts**: For guest accounts that they can manage, allow the sponsor to suspend their accounts to prevent guests from logging in temporarily.

  This action also issues a Change of Authorization (CoA) Terminate to remove the suspended guests from the network.

  - **Require sponsor to provide a reason**: Require the sponsor to provide an explanation for suspending the guest accounts.

- **Approve and view requests from self-registering guests**: Sponsors who are included in this Sponsor Group can either view all pending account requests from self-registering guests (that require approval), or only the requests where the user entered the Sponsor's email address as the person being visited. This feature requires that the portal used by the Self-registering guest has **Require self-registered guests to be approved** checked, and the Sponsor's email is listed as the person to contact. This feature also requires that the **Email** attribute be properly configured in the Sponsor's identity source.
  - Any pending accounts: A sponsor belonging to this group an approve and review accounts that were created by any sponsor.
  - Only pending accounts assigned to this sponsor: A sponsor belonging to this group can only view and approve accounts that they created.

Note The **Email** attribute is part of **User Info Attributes**. For more information on the **Email** attribute, see:

- Configure Custom Schema, on page 661
- **Schema** and **User Info** attributes in the LDAP General Settings table in LDAP Identity Source Settings, on page 615.
- Step 8 in Configure SAML ID Provider, on page 767.

- **Access Cisco ISE guest accounts using the programmatic interface (Guest REST API)**: For guest accounts that they can manage, allow the sponsor to access guest accounts using the Guest REST API programming interface.

Step 10 Click **Save** and then **Close**.

Configure Account Content for Sponsor Account Creation

You can configure the type of user data that your guests and sponsors must provide to create a new guest account. Some fields are required to identify an ISE account, but you can eliminate other fields, and add your own custom fields.

To configure fields for account creation by Sponsors:

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals**, and edit your sponsor portal.
2. Select the **Portal Page Customization** tab.
3. Scroll down and select **Create Account for Known Guests**.
4. On the Preview display on the right, select **Settings**.

These settings determine which fields display and are required for guest accounts when they are created on the sponsor portal. This configuration applies to Known, Random, and Imported guest types. The template that the sponsor downloads to import new users is created dynamically, so that only the fields set in Known Guests are included.

Import Username and Password for Accounts

Sponsors can import username and password, but those rows are not added to the CSV template when the sponsor downloads it. The sponsor can add those headings. They must be named properly in order for the ISE to recognize the columns:

- Username—Can be either *User Name* or *UserName*.
- Password—Must be `password`.

Special Settings for the Sponsor Portal

The following settings are unique to the Create Account for Imported Guests page, on the Portal Page Customization tab, on the Sponsor Portal.

- **Allow sponsor to be copied in Guest Credentials email**: If you enable this option, then each email of guest credentials that is sent to a successfully imported guest is also sent to the sponsor. The default is to not send emails to the sponsor.
- **Allow sponsor to receive summary email**: When a sponsor imports a list of users, ISE sends one email with a summary of all the imported users. If you uncheck this option, the sponsor gets a separate email for each imported user.

Configure a Sponsor Portal Flow

You can use a default portal and its default settings such as certificates, endpoint identity group, identity source sequence, portal themes, images, and other details provided by Cisco ISE. If you do not want to use the default settings, you should create a new portal or edit an existing one to meet your needs. You can duplicate a portal if you want to create multiple portals with the same settings.

You may want to create multiple sponsor portals if your company has different branding for your corporate office and its retail locations, or if your company has different product brands, or if a city's offices want different themed portals for the fire, police, and other departments.

These are the tasks related to configuring a Sponsor portal.

Before you begin

Configure or edit existing sponsor groups for your site, as described in Configure Sponsor Groups, on page 515.

Step 1 Enable Policy Services, on page 520.

Step 2 Add Certificates for Guest Services, on page 520.

Step 3 Create External Identity Sources, on page 520.

Step 4 Create Identity Source Sequences, on page 521.

Step 5 Create a Sponsor Portal, on page 521.

Step 6 (Optional) Customize Sponsor Portals, on page 522.

Enable Policy Services

To support the Cisco ISE end-user web portals, you must enable the portal-policy services on the node on which you want to host them.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 2 Click the node and click **Edit**.

Step 3 Under the **General Settings** tab, enable the **Policy Service** toggle button.

Step 4 Check the **Enable Session Services** check box.

Step 5 Click **Save**.

Add Certificates for Guest Services

If you do not want to use the default certificates, you can add a valid certificate and assign it to a certificate group tag. The default certificate group tag used for all end-user web portals is Default Portal Certificate Group.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **System Certificates**.

Step 2 Add a system certificate and assign it to a certificate group tag that you want to use for the portal.

This certificate group tag will be available to select during portal creation or editing.

Step 3 Choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Create or Edit** > **Portal Settings**.

Step 4 Select the specific certificate group tag from the **Certificate Group Tag** drop-down list that is associated with the newly added certificate.

Create External Identity Sources

Cisco ISE can connect with external identity sources such as Active Directory, LDAP, RADIUS Token, and RSA SecurID servers to obtain user information for authentication and authorization. External identity sources also include certificate authentication profiles that you need for certificate-based authentications.

Note To work with passive identity services, which enable you to receive and share authenticated user identities, see Additional Passive Identity Service Providers, on page 690.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources**.

Step 2 Choose one of these options:

- **Certificate Authentication Profile** for certificate-based authentications.

- **Active Directory** to connect to an Active Directory as an external identity source. See Active Directory as an External Identity Source, on page 641 for more details.
- **LDAP** to add an LDAP identity source. See LDAP, on page 730 for more details.
- **RADIUS Token** to add a RADIUS Token server. See RADIUS Token Identity Sources, on page 752 for more details.
- **RSA SecurID** to add an RSA SecurID server. See RSA Identity Sources, on page 758 for more details.
- **SAML Id Providers** to add an identity provider (IdP), such as Oracle Access Manager. See SAMLv2 Identity Provider as an External Identity Source, on page 764 for more details.
- **Social Login** to add a Social Login, such as Facebook, as an external identity source. See Social Login for Self-Registered Guests, on page 493 for more details.

Create Identity Source Sequences

Before you begin

Ensure that you have configured your external identity sources in Cisco ISE.

To perform the following task, you must be a Super Admin or System Admin.

For allowing guest users to authenticate through Local WebAuth, you must configure both the Guest portal authentication source and the identity source sequence to contain the same identity stores.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **Identity Source Sequences** > **Add**.

Step 2 Enter a name for the identity source sequence. You can also enter an optional description.

Step 3 Check the **Select Certificate Authentication Profile** check box and choose a certificate authentication profile for certificate-based authentication.

Step 4 Choose the database or databases that you want to include in the identity source sequence in the **Selected List** field.

Step 5 Rearrange the databases in the **Selected list** field in the order in which you want Cisco ISE to search the databases.

Step 6 If a selected identity store cannot be accessed for authentication, choose one of the following options in the **Advanced Search List** area:

- **Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError**
- **Treat as if the user was not found and proceed to the next store in the sequence**

  While processing a request, Cisco ISE searches these identity sources in sequence. Ensure that you have the identity sources in the Selected list field listed in the order in which you want Cisco ISE to search them.

Step 7 Click **Submit** to create the identity source sequence that you can then use in policies.

Create a Sponsor Portal

You can provide a Sponsor portal to enable sponsors to create, manage, and approve accounts for guests who want to connect to your network to access the internet and internal resources and services.

Cisco ISE provides you with a default Sponsor portal that you can use without having to create another one. However, you can create a new Sponsor portal, or you can edit or duplicate an existing one. You can delete any of these portals, except the default Sponsor portal. IPv6 is not supported in Sponsor portal logins.

Any changes that you make to the Page Settings on the **Portal Behavior and Flow Settings** tab are reflected in the graphical flow in the Sponsor Flow diagram. If you enable a page, such as the AUP page, it appears in the flow and the sponsor will experience it in the portal. If you disable it, it is removed from the flow and the next enabled page displays for the sponsor.

Before you begin

Ensure that you have the required certificates, external identity sources, and identity source sequences configured for use with this portal.

Step 1 Configure the **Portal Settings** page, as described in Portal Settings for Sponsor Portals, on page 551.

Ensure that the portal name that you use here is not used for any other end-user portals.

Step 2 Configure the **Login Settings** page , as described in Login Settings for Sponsor Portals, on page 554.

Step 3 Configure the **Acceptable Use Policy (AUP) Page Settings** page, as described in Acceptable Use Policy (AUP) Settings for Sponsor Portals, on page 554 .

Step 4 Configure the **Sponsor Change Password Settings** option, as described in Sponsor Change Password Settings for Sponsor Portals, on page 555.

Step 5 Configure the **Post-Login Banner Page Settings** page, as described in Post-Login Banner Settings for Sponsor Portals, on page 555.

Step 6 Click **Sponsor Portal Application Settings** if you want to customize the portal.

Step 7 Click **Save**.

Customize Sponsor Portals

You can customize the portal appearance and user experience by customizing the portal themes, changing UI elements on the portal pages, and editing error messages and notifications that display to the users. For more information about customizing portals, see Customization of End-User Web Portals , on page 563.

Configuring Account Content for Sponsor Account Creation

You can configure the type of user data that your guests and sponsors must provide to create a new guest account. Some fields are required to identify an ISE account, but you can eliminate other fields, and add your own custom fields.

To configure fields for account creation by Sponsors:

1. Choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals**, and edit your sponsor portal.
2. Select the **Portal Page Customization** tab.
3. Scroll down and select **Create Account for Known Guests**.

   On the Preview display on the right, select **Settings**.These settings determine which fields display and are required for guest accounts when they are created on the sponsor portal.

This configuration applies to Known, Random, and Imported guest types. The template that the sponsor downloads to import new users is created dynamically, so that only the fields set in Known Guests are included.

Sponsor Import Usernames and Passwords for Accounts

Sponsors can import username and password, but those rows are not added to the template when the sponsor downloads it. The sponsor can add those headings. They must be named properly in order for the Cisco ISE to recognize the columns:

- **Username**: Can be either `User Name` or `UserName`
- **Password**: Must be password

Configuring the Time Settings Available to Sponsors

When sponsors create a new guest account, they configure the time that the account is active. You configure the options that are available to the sponsor, to allow them to set the account duration, and the start and end times. These options are configured by guest type. The sponsor sees the results under the heading **Access Information**.

The Guest Type settings that control sponsor portal account time options are under the heading **Maximum Access Time**, and are described below:

- **From first login**: The sponsor portal shows the duration for which the account is active after the first login.

  The guest type setting **Maximum Account Duration** determines which values the Sponsor can enter for duration.

- **From sponsor-specified date (or date of self-registration, if applicable)**: The sponsor can choose between setting the duration as End of business day, or, by unchecking that field, the duration, start and end times.

  The guest type settings to control the duration time and effective dates are under the heading **Allow access only on these days and times**.

  - The days of the week that you select limits the dates that are selectable in the Sponsor's calendar.
  - Maximum account duration is enforced in the sponsor portal when picking duration and dates.

Kerberos Authentication for the Sponsor Portal

You can configure Cisco ISE to use Kerberos to authenticate a sponsor user who is logged onto Windows for access to the sponsor portal. This process uses the Active Directory credentials of the logged in sponsor user in the Kerberos ticket. Kerberos SSO is performed inside the secure tunnel after the browser establishes the SSL connection with Cisco ISE.

The following items must be in the same Active Directory domain:

- Sponsor's PC
- ISE PSN
- FQDN configured for this sponsor portal

This requirement is because Microsoft does not support Kerberos SSO with 2-way trusts across Active Directory forests.

The sponsor user must be logged onto Windows.

Kerberos authentication is NOT supported for the Guest portal.

Configuring Kerberos

To enable Kerberos on the Sponsor portal, check the **Allow Kerberos SSO** check box in the **Sponsor Settings and Customization** window.

The sponsor's browser must also be configured properly. The following sections explain how to manually configure each browser.

Note The username in the Active Directory and User Principle Name must match. The SSO will depend on the User Principle Name to identify the session of the user.

While accessing the sponsor portal using the sponsor portal FQDN from your browser, Cisco ISE redirects the request to the PSN FQDN instead of the configured sponsor portal FQDN.

For example, if the sponsor portal FQDN is `sponsor.example.com` and the PSN FQDN is `psn.example.com`, when you try accessing `https://sponsor.example.com` from your browser, you will be redirected to `https://ise.example.com:8445/sponsorportal/PortalSetup.action?portal=b7e7d773-7bb3-442b-a50b-42837c12248a`.

This behavior occurs only when you enable the **Allow Kerberos SSO** option.

To Manually Configure Firefox

1. Enter `about:config` in the address bar.
2. Ignore warnings that appear, and click to continue.
3. Search for `negotiate` in the search bar.
4. Add the FQDN to `network.negotiate-auth.delegation-uris` and `network.negotiate-auth.trusted-uris`. The list of URLs for each attribute is separated by commas.
5. Close the tab. The browser is ready, no restart is required.

To Manually Configure Internet Explorer

1. Click the gear on the top right, and select **Internet Options**.
2. Click the **Security** tab.
3. Click **Local Intranet**.
4. Click **Sites** and then click **Advanced**.
5. Add in the string `<mydomain>.com`, where `<mydomain>` is a wild card for the Sponsor portal FQDN, or you can enter the FQDN.
6. Click **Close** and then click **OK**.
7. Click the **Advanced** tab.

8. Scroll down to the **Security** section and check the **Enable Integrated Windows Authentication** check box.
9. Restart the computer.

Chrome gets the configuration from Internet Explorer

Troubleshooting

- Run `set user` in the command prompt to verify that the machine is tied to proper AD domain.
- Run `klist` in the command prompt to see list of cached Kerberos tickets and the hostnames.
- Look at the SPNEGO token data. The NTLM password-based token string is much shorter than Kerberos token string; the correct token string should not fit on one line.
- Use Wireshark using the filter `kerberos` to capture Kerberos request, if it exists.

Note When the Kerberos SSO option is enabled, the user needs to access the sponsor portal by the node FQDN for Kerberos SSO to function properly. If a portal FQDN is configured for the sponsor portal, when the user connects to the portal FQDN, the user will be redirected to the portal by its node FQDN.

Sponsors Cannot Log In to the Sponsor Portal

Problem

The following error message appears when a sponsor tries to log in to the Sponsor portal:

```
“Invalid username or password. Please try again.”
```

Causes

- The sponsor has entered invalid credentials.
- The sponsor is not valid because the user record is not present in the database (Internal Users or Active Directory).
- The sponsor group to which the sponsor belongs is disabled.
- The Sponsor's user account is not a member of an active/enabled Sponsor Group, which means the Sponsor user's Identity Group is not a member of any Sponsor Group.
- The sponsor’s internal user account is disabled (suspended).

Solution

- Verify the user’s credentials.
- Enable the sponsor group.
- Reinstate the user account if disabled.
- Add the sponsor user's Identity Group as a member of a Sponsor Group.

Monitor Guest and Sponsor Activity

Cisco ISE provides various reports and logs that allow you to view endpoint and user management information and guest and sponsor activity.

You can run these reports either on demand or on a scheduled basis.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Reports**.

Step 2 Choose **Guest** or **Endpoints and Users** to view the various guest, sponsor, and endpoint related reports

Step 3 Choose the data with which you want to search using the **Filters** drop-down list.

Step 4 Select the **Time Range** during which you want to view the data.

Step 5 Click **Run**.

Metrics Dashboard

Cisco ISE provides an at-a-glance view of **Authenticated Guests** and **Active Endpoints** in the network in a metrics dashboard that appears on the Cisco ISE Home page.

Click the number displayed in **Active Endpoints** to launch the **Live Sessions** window that displays the details of the endpoints with active sessions.

Note For Hotspot flow, the endpoints are not displayed in the **Authenticated Guests** dashlet.

AUP Acceptance Status Report

The AUP Acceptance Status report displays the acceptance status of the Acceptable Use Policy (AUP) by guests from all the Guest portals. To view this window, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Guest** > **AUP Acceptance Status**.

You can use the report to track all the accepted and denied AUP connections for a given period of time.

Guest Accounting Report

The Guest Accounting report displays the guest login history for an indicated time period. To view this window, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Guest** > **Guest Accounting**.

Primary Guest Report

The Primary Guest Report combines data from various reports into a single view enabling you to export data from different reporting sources. You can add more data columns and remove the ones you do not want to view or export. To view this window, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Reports** > **Guest** > **Primary Guest Report**.

This report collects all guest activity and provides details about the websites that guest users visit. You can use this report for security auditing purposes to see when guest users accessed the network and what they did on it. To view the guests' Internet activity, such as the URLs of the websites that they visited, you must first:

- Enable the passed authentications logging category. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and select Passed authentications.
- Enable these options on the firewall used for guest traffic:
  - Inspect HTTP traffic and send data to Cisco ISE Monitoring node. Cisco ISE requires only the IP address and accessed URL for the Guest Activity report; so, limit the data to include just this information, if possible.
  - Send syslogs to Cisco ISE Monitoring node.

Sponsor Login and Audit Report

The Sponsor Login and Audit report is a combined report that tracks:

- Login activity by the sponsors at the Sponsor portal.
- Guest-related operations performed by the sponsors in the Sponsor portal.

To view this window, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Guest Access Reports** > **Sponsor Login and Audit**.

Audit Logging for Guest and Sponsor Portals

During specific actions within the Guest and Sponsor portals, audit log messages are sent to the underlying audit system. Use the command **show logging application localStore/iseLocalStore.log** to view these messages.

You can configure these messages to be sent by syslog to the monitoring and troubleshooting system and log collector. The monitoring subsystem presents this information in the appropriate sponsor and device audit logs and guest activity logs.

Guest login flow is logged in the audit logs regardless of whether the guest login has passed or failed.

Guest Access Web Authentication Options

Cisco ISE Guest and Web Authentication Services support several deployment options that enable secure guest access. You can provide wired or wireless guest connectivity using Local or Central Web Authentication and Device Registration Web Authentication.

- Central Web Authentication (Central WebAuth): Applies to all Guest portals. Uses Web authentication by a central Cisco ISE RADIUS server for both wired and wireless connection requests. Guests authenticate after by either entering an optional access code on the Hotspot Guest portals, or by entering a username and password on the Credentialed Guest portals.

Note During redirection, if the browser opens more than one tab, Cisco ISE redirects to every tab. The user can log in to the portal, but Cisco ISE can't authorize the session, and the user fails to gain access. To work around this issue, the user must close all but one tab on the browser.

- Local Web Authentication (Local WebAuth): Applies to the Credentialed Guest portals. The guest connects to a switch for a wired connections, or a wireless LAN controller (WLC) for a wireless connection. The network access device (NAD) directs them to web pages for authentication. The guest enters a username and password on the Credentialed Guest portals to authenticate.
- Device Registration Web Authentication (Device Registration WebAuth): Applies only to the Hotspot Guest portal. Cisco ISE registers and authorizes the guest device before Web authentication. When guests connect to a wired or wireless NAD, they are directed to the Hotspot Guest portal. Guests get network access without providing credentials (username and password).

ISE Community Resource

For information on how to configure Cisco ISE with Cisco Wireless Controller to provide guest access, see ISE Guest Access Prescriptive Deployment Guide.

Also see the following Tech Note: ISE Wireless Guest Setup Guide & Wizard.

NAD with Central WebAuth Process

In this scenario, the network access device (NAD) makes a new authorization request to the Cisco ISE RADIUS server from an unknown endpoint connection. The endpoint then receives a url-redirect to Cisco ISE.

Note webauth-vrf-aware command is supported only in IOS XE 3.7E, IOS 15.2(4)E or later versions. Other switches do not support WebAuth URL redirect in virtual routing and forwarding (VRF) environment. In such cases, as a workaround, you can add a route in the global routing table to leak the traffic back into the VRF.

If the guest device is connected to a NAD, the guest service interaction takes the form of a MAC Authentication Bypass (MAB) request that leads to a Guest portal Central WebAuth login. The following is an outline of the subsequent Central Web Authentication (Central WebAuth) process, which applies to both wireless and wired network access devices.

1. The guest device connects to the NAD through a hard-wired connection. There is no 802.1X supplicant on the guest device.
2. An authentication policy with a service type for MAB allows a MAB failure to continue and return a restricted network profile containing a url-redirect for the Central WebAuth user interface.
3. The NAD is configured to authenticate MAB requests to the Cisco ISE RADIUS server.
4. The Cisco ISE RADIUS server processes the MAB request and does not find an endpoint for the guest device.

   This MAB failure resolves to the restricted network profile and returns the url-redirect value in the profile to the NAD in an access-accept. To support this function, ensure that an authorization policy exists and features the appropriate wired or wireless MAB (under compound conditions) and, optionally, “Session:Posture Status=Unknown” conditions. The NAD uses this value to redirect all guest HTTPS traffic on the default port 8443 to the url-redirect value.

The standard URL value in this case is:

```
https://ip:port/guestportal/gateway?sessionId=NetworkSessionId&portal=<PortalID>&action=cwa
```

5. The guest device initiates an HTTP request to redirect URL via a web browser.
6. The NAD redirects the request to the url-redirect value returned from the initial access-accept.
7. The gateway URL value with action CWA redirects to the Guest portal login page.
8. The guest enters their login credentials and submits the login form.
9. The guest server authenticates the login credentials.
10. Depending on the type of flow, the following occurs:
    - If it is a non-posture flow (authentication without further validation), where the Guest portal is not configured to perform client provisioning, the guest server sends a CoA to the NAD. This CoA causes the NAD to reauthenticate the guest device using the Cisco ISE RADIUS server. A new access-accept is returned to the NAD with the configured network access. If client provisioning is not configured and the VLAN needs to be changed, the Guest portal performs VLAN IP renew. The guest does not have to re-enter login credentials. The username and password entered for the initial login are used automatically.
    - If it is a posture flow, where the Guest portal is configured to perform client provisioning, the guest device web browser displays the Client Provisioning page for posture agent installation and compliance. (You can also optionally configure the client provisioning resource policy to feature a “NetworkAccess:UseCase=GuestFlow” condition.)

The Guest portal redirects to the Client Provisioning portal (because there is no client provisioning or posture agent for Linux), which in turn redirects back to a guest authentication servlet to perform optional IP release/renew and then CoA.

With redirection to the Client Provisioning portal, the Client Provisioning service downloads a non-persistent web agent to the guest device and performs a posture check of the device. You can optionally configure the posture policy with a “NetworkAccess:UseCase=GuestFlow” condition.

If the guest device is non-compliant, ensure that you have configured an authorization policy that features “NetworkAccess:UseCase=GuestFlow” and “Session:Posture Status=NonCompliant” conditions.

When the guest device is compliant, ensure that you have an authorization policy configured with the conditions “NetworkAccess:UseCase=GuestFlow” and “Session:Posture Status=Compliant.” From here, the Client Provisioning service issues a CoA to the NAD. This CoA causes the NAD to reauthenticate the guest using the Cisco ISE RADIUS server. A new access-accept is returned to the NAD with the configured network access.

Note “NetworkAccess:UseCase=GuestFlow” can also apply for Active Directory and LDAP users who log in as guests.

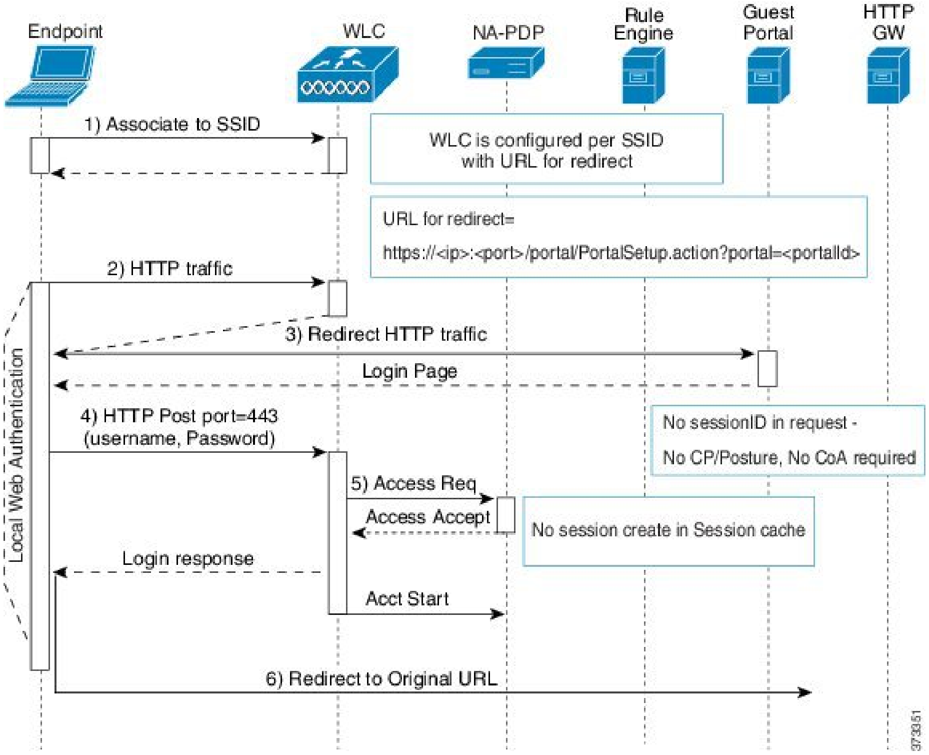
Wireless LAN Controller with Local WebAuth Process

In this scenario, the guest logs in and is directed to the wireless LAN controller (WLC). The WLC then redirects the guest to a Guest portal, where they are prompted to enter their login credentials, accept an optional Acceptable Use Policy (AUP), and perform an optional password change.

When this is complete, the guest device's browser is redirected back to the WLC to provide login credentials via a POST.

The WLC can now log the guest in via the Cisco ISE RADIUS server. When this is complete, the WLC redirects the guest device's browser to the original URL destination. The Wireless LAN Controller (WLC) and the network access devices (NAD) requirements to support the original URL redirect for guest portals are WLC 5760 and Cisco Catalyst 3850, 3650, 2000, 3000, and 4000 Series Access Switches running releases IOS-XE 3.6.0.E and 15.2(2)E.

Figure 13: WLC with Local WebAuth Non-Posture Flow


Endpoint
WLC
NA-PDP
Rule Engine
Guest Portal
HTTP GW
1) Associate to SSID
WLC is configured per SSID with URL for redirect
URL for redirect=
https://<ip>:<port>/portal/PortalSetup.action?portal=<portalId>
2) HTTP traffic
3) Redirect HTTP traffic
Login Page
Local Web Authentication
4) HTTP Post port=443 (username, Password)
No sessionID in request -
No CP/Posture, No CoA required
5) Access Req
Access Accept
No session create in Session cache
Login response
Acct Start
6) Redirect to Original URL
373351

Wired NAD with Local WebAuth Process

In this scenario, the Guest portal redirects the guest login request to the switch (wired NAD). The login request is in the form of an HTTPS URL posted to the switch and contains the login credentials. The switch receives the guest login request and authenticates the guest using the configured Cisco ISE RADIUS server.

1. Cisco ISE requires a login.html file with the HTML redirect to be uploaded to the NAD. This login.html file is returned to the browser of the guest device for any HTTPS request made.
2. The browser of the guest device is redirected to the Guest portal where the guest's login credentials are entered.

3. After the Acceptable Use Policy (AUP) and change password are processed, both of which are optional, the Guest portal redirects the browser of the guest device to post the login credentials on the NAD.
4. The NAD makes a RADIUS request to the Cisco ISE RADIUS server to authenticate and authorize the guest.

IP Address and Port Values Required for the Login.html Page

The IP address and port values must be changed in the following HTML code for the login.html page to those values being used by the Cisco ISE Policy Services nodes. The default port is 8443, but you can change this value, so ensure that the value you assign to the switch matches the setting in Cisco ISE.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<head>
<title>ISE Guest Portal</title>
<meta Http-Equiv="Cache-Control" Content="no-cache">
<meta Http-Equiv="Pragma" Content="no-cache">
<meta Http-Equiv="Expires" Content="0">
<meta http-equiv="content-type" content="text/html; charset=ISO-8859-1">

<meta http-equiv="REFRESH"
content="0;url=https://ip:port/portal/PortalSetup.action?switch_url=wired">

</HEAD>
<BODY>

<center>
Redirecting ... Login
<br>
<br>
<a href="https://ip:port/portal/PortalSetup.action?switch_url=wired">ISE Guest Portal</a>
</center>

</BODY>
</HTML>
```

The custom login page is a public web form, hence consider these guidelines:

- The login form must accept user entries for the username and password and must show them as **uname** and **pwd**.
- The custom login page should follow best practices for a web form, such as page timeout, hidden password, and prevention of redundant submissions.

HTTPS Server Enabled on the NAD

To use web-based authentication, you must enable the HTTPS server within the switch using the **ip http secure-server** command.

Support for Customized Authentication Proxy Web Pages on the NAD

You can upload custom pages for success, expiry, and failure to the NAD. Cisco ISE does not require any specific customization, so you can create these pages using the standard configuration instructions included with the NAD.

Configure Web Authentication on the NAD

You need to complete the web authentication on the NAD by replacing the default HTML pages with your custom files.

Before you begin

During web-based authentication, create four substitute HTML pages to use instead of the switch default HTML pages.

Step 1 To specify the use of your custom authentication proxy web pages, first store your custom HTML files on the switch flash memory. To copy your HTML files to the switch flash memory, run the following command on the switch:

copy tftp/ftp flash

Step 2 After copying your HTML files to the switch, perform the following commands in global configuration mode:

ip admission proxy http login page file device:*login-filename*	Specifies the location in the switch memory file system of the custom HTML file to use in place of the default login page. The device: is flash memory.
ip admission proxy http success page file device:*success-filename*	Specifies the location of the custom HTML file to use in place of the default login success page.
ip admission proxy http failure page file device:*fail-filename*	Specifies the location of the custom HTML file to use in place of the default login failure page.
ip admission proxy http login expired page file device:*expired-filename*	Specifies the location of the custom HTML file to use in place of the default login expired page.

Step 3 Configure the customized authentication proxy web pages following the guidelines provided by the switch.

Step 4 Verify the configuration of a custom authentication proxy web page, as shown in the following example:

```
Switch# show ip admission configuration
Authentication proxy webpage
 Login page           : flash:login.htm
 Success page         : flash:success.htm
 Fail Page            : flash:fail.htm
 Login expired Page   : flash:expired.htm

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

Device Registration WebAuth Process

Using Device Registration Web Authentication (Device Registration WebAuth) and the Hotspot Guest portal, you can allow guest devices to connect to a private network without requiring usernames and passwords.

In this scenario, the guest connects to the network with a wireless connection. See Figure 14: Wireless Device Registration Web Authentication Flow for an example of the Device Registration WebAuth process flow.

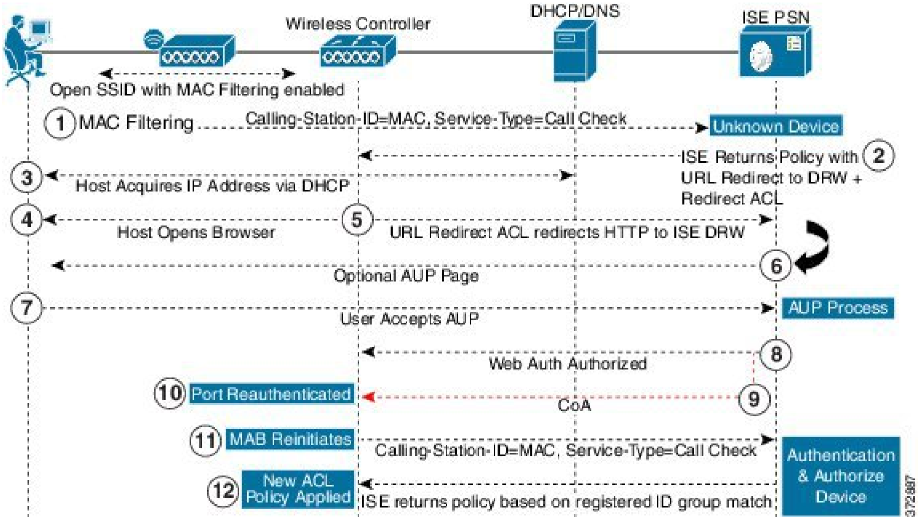
The following is an outline of the subsequent Device Registration WebAuth process, which is similar for both wireless and wired connections:

1. The network access device (NAD) sends a redirect to the Hotspot Guest portal.
2. If the MAC address of the guest device is not in any endpoint identity group or is not marked with an Acceptable Use Policy (AUP) accepted attribute set to true, Cisco ISE responds with a URL redirection specified in an authorization profile.
3. The URL redirection presents the guest with an AUP page (if enabled) when the guest attempts to access any URL.
   - If the guest accepts the AUP, the endpoint associated with their device MAC address is assigned to the configured endpoint identity group. This endpoint is now marked with an AUP accepted attribute set to true, to track the guest acceptance of the AUP.
   - If the guest does not accept the AUP or if an error occurs, for instance, while creating or updating the endpoint, an error message displays.
4. Based on the Hotspot Guest portal configuration, a post-access banner page (if enabled) with additional information may appear.
5. After the endpoint is created or updated, a Change of Authorization (CoA) termination is sent to the NAD.
6. After the CoA, the NAD re-authenticates the guest connection with a new MAC Auth Bypass (MAB) request. The new authentication finds the endpoint with its associated endpoint identity group, and returns the configured access to the NAD.
7. Based on the Hotspot Guest portal configuration, the guest is directed to the URL to which they requested access, or to a custom URL specified by the administrator, or to an Authentication Success Page.

The CoA type for both wired and wireless is Termination CoA. You can configure the Hotspot Guest portal to perform VLAN DHCP Release (and renew), thereby re-authorizing the CoA type for both wired and wireless to Change of Auth.

VLAN DHCP Release support is available for Windows devices only. It is not available for mobile devices. If the device being registered is mobile and the VLAN DHCP Release option is enabled, the guest is requested to manually renew their IP address. For mobile device users, we recommend using Access Control Lists (ACLs) on the WLC, rather than using VLANs.

Figure 14: Wireless Device Registration Web Authentication Flow


Wireless Controller
DHCP/DNS
ISE PSN
Open SSID with MAC Filtering enabled
1 MAC Filtering
Calling-Station-ID=MAC, Service-Type=Call Check
Unknown Device
ISE Returns Policy with URL Redirect to DRW + Redirect ACL 2
3 Host Acquires IP Address via DHCP
4 Host Opens Browser
5 URL Redirect ACL redirects HTTP to ISE DRW
6
Optional AUP Page
7 User Accepts AUP
AUP Process
Web Auth Authorized 8
10 Port Reauthenticated
CoA 9
11 MAB Reinitiates
Calling-Station-ID=MAC, Service-Type=Call Check
Authentication & Authorize Device
12 New ACL Policy Applied
ISE returns policy based on registered ID group match
372987

Guest Portal Settings

Portal Identification Settings

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals or Sponsor Portals** > **Create, Edit or Duplicate** > **Guest Portals or Sponsor Portals Settings and Customization**.

- **Portal Name**: Enter a unique portal name to access this portal. Do not use this portal name for any other Sponsor, Guest, or nonguest portals, such as Blocked List, Bring Your Own Device (BYOD), Client Provisioning, Mobile Device Management (MDM), or My Devices portals.

  This name appears in the authorization profile portal selection for redirection choices. It is applied to the list of portals for easy identification among other portals.

- **Description**: Optional.

- **Portal Test URL**: A system-generated URL displays as a link after you click **Save**. Use it to test the portal.

  Click the link to open a new browser tab that displays the URL for this portal. Policy Services Node (PSN) with Policy Services must be turned on. If Policy Services are disabled, the PSN only displays the Admin portal.

Note The test portal does not support RADIUS sessions, so you won't see the entire portal flow for all portals. BYOD and Client Provisioning are examples of portals that depend on RADIUS sessions. For example, a redirect to an external URL will not work. If you have more than one PSN, Cisco ISE chooses the first active PSN.

- **Language File**: Each portal type supports 15 languages by default, which are available as individual properties files bundled together in a single zipped language file. Export or import the zipped language file to use with the portal. The zipped language file contains all the individual language files that you can use to display text for the portal.

  The language file contains the mapping to the particular browser locale setting along with all of the string settings for the entire portal in that language. A single language file contains all the supported languages, so that it can easily be used for translation and localization purposes.

  If you change the browser locale setting for one language, the change is applied to all the other end-user web portals. For example, if you change the French.properties browser locale from fr,fr-fr,fr-ca to fr,fr-fr in the Hotspot Guest portal, the changes also apply to the My Devices portal.

  An alert icon displays when you customize any of the text on the **Portal Page Customizations** tab. The alert message reminds you that any changes made to one language while customizing the portal must also be added to all the supported languages properties files. You can manually dismiss the alert icon using the drop-down list option; or it is automatically dismissed after you import the updated zipped language file.

Portal Settings for Hotspot Guest Portals

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Portal Settings**.

- **HTTPS Port**: Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blocked List Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you modify this window. If you modify this window, update the port setting to comply with this restriction.

  If you assign ports used by a non-guest (such as My Devices) portal to a guest portal, an error message appears.

  For posture assessments and remediation only, the Client Provisioning portal also uses ports 8905 and 8909. Otherwise, it uses the same ports assigned to the Guest portal.

  Portals assigned to the same HTTPS port can use the same Gigabit Ethernet interface or another interface. If they use the same port and interface combination, they must use the same certificate group tag. For example:

  - Valid combinations include, using the Sponsor portal as an example:
    - Sponsor portal: Port **8443**, Interface **0**, Certificate tag **A** and My Devices portal: Port **8443**, Interface **0**, Certificate group **A**.
    - Sponsor portal: Port **8443**, Interface **0**, Certificate group **A** and My Devices portal: Port **8445**, Interface **0**, Certificate group **B**.
    - Sponsor portal: Port **8444**, Interface **1**, Certificate group **A** and Blocked List portal: Port **8444**, Interface **0**, Certificate group **B**.
  - Invalid combinations include:
    - Sponsor portal: Port **8443**, Interface **0**, Certificate group **A** and My Devices portal: **8443**, Interface **0**, Certificate group **B**.

  - Sponsor portal: Port **8444**, Interface **0**, Certificate tag **A** and Blocked List portal: Port **8444**, Interface **0**, Certificate group **A**.

Note We recommend that you use interface 0 for Guest services for best performance. You can either configure only interface 0 in the **Portal Settings**, or you can use the CLI command **ip host** to map a hostname or FQDN to the IP address of interface 0.

- **Allowed Interfaces**: Select the PSN interfaces which a PAN can use to run a portal. When a request to open a portal is made on the PAN, the PAN looks for an available allowed port on the PSN. You must configure the Ethernet interfaces using IP addresses on different subnets.

  These interfaces must be available on all the PSNs, including VM-based ones, that have Policy Services turned on. This is a requirement because any of these PSNs can be used for the redirect at the start of the guest session.

  - The Ethernet interfaces must use IP addresses on different subnets.
  - The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
  - The portal certificate Subject Name or Alternate Subject Name must resolve to the interface IP address.
  - Configure **ip host x.x.x.x yyy.domain.com** in Cisco ISE CLI to map the secondary interface IP address to the FQDN, which is used to match the certificate Subject Name or Alternate Subject Name.
  - If only the bonded NIC is selected, when the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN logs an error and exits. The PSN will not try to start the portal on the physical interface.
  - NIC Teaming or bonding is a configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based in the **Portal Settings** configuration. If both physical NICs and the corresponding bonded NIC are configured, when the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.

- **Certificate Group tag**: Pick a certificate group tag that specifies the certificate to be used for the portal’s HTTPS traffic.
- **Endpoint Identity Group**: Choose an endpoint identity group to track guest devices. Cisco ISE provides the **GuestEndpoints** endpoint identity group to use as a default. You can also create more endpoint identity groups if you choose to not use the default.

  Choose an endpoint identity group to track employee devices. Cisco ISE provides the **RegisteredDevices** endpoint identity group to use as a default. You can also create more endpoint identity groups if you choose to not use the default.

- **Purge Endpoints in this Identity Group when they Reach __ Days**: Specify the number of days after which the device is purged from the Cisco ISE database. Purging is done on a daily basis and the purge activity is synchronized with the overall purge timing. The change is applied globally for this endpoint identity group.

  If changes are made to the Endpoint Purge Policy based on other policy conditions, this setting is no longer available for use.

- **Display Language**
  - **Use Browser Locale**: Use the language specified in the client browser's locale setting as the display language of the portal. If browser locale's language is not supported by Cisco ISE, then the **Fallback Language** is used as the language portal.
  - **Fallback Language**: Choose the language to use when the language cannot be obtained from the browser locale, or if the browser locale language is not supported by Cisco ISE.
  - **Always Use**: Choose the display language to use for the portal. This setting overrides the **User Browser Locale** option.

Acceptable Use Policy (AUP) Page Settings for Hotspot Guest Portals

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Acceptable Use Policy (AUP) Page Settings**.

- **Include an AUP Page**: Display your company's network-usage terms and conditions on a separate page to the user.
- **Require an Access Code**: Assign an access code as the login credential that multiple guests should use to gain access to the network. An access code is primarily a locally known code that is given to physically present guests (either visually via a whiteboard or verbally by a lobby ambassador). It would not be known and used by someone outside the premises to access the network.

  You can use this option in addition to the usernames and passwords that are provided as the login credentials to individual guests.

- **Require scrolling to end of AUP**—Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP. Configure when the AUP appears to the user.

When configuring the Hotspot Guest Portals flow, the AUP access code is reliant on Endpoint Identity Group device registration.

The AUP access code page will appear only after the MAC address has been removed from the Endpoint Identity Group tied to the hotspot portal configuration. An endpoint is either manually deleted from the database through the Context Visibility page on Cisco ISE, or it is purged by way of the Endpoint Purge feature and configured endpoint purge policies.

Post-Access Banner Page Settings for Hotspot Portals

The navigation path for this page is **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Post-Access Banner Page Settings**.

Use this setting to inform guests of their access status and any other additional actions, if required.

Field	Usage Guidelines
Include a Post-Access Banner page	Display additional information after the guests are successfully authenticated and before they are granted network access.

Portal Settings for Credentialed Guest Portals

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Portal Settings**.

- **HTTPS Port**: Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blocked List Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you modify this window. If you modify this window, update the port setting to comply with this restriction.

  If you assign ports used by a non-guest (such as My Devices) portal to a guest portal, an error message appears.

  For posture assessments and remediation only, the Client Provisioning portal also uses ports 8905 and 8909. Otherwise, it uses the same ports assigned to the Guest portal.

  Portals assigned to the same HTTPS port can use the same Gigabit Ethernet interface or another interface. If they use the same port and interface combination, they must use the same certificate group tag. For example:

  - Valid combinations include, using the Sponsor portal as an example:
    - Sponsor portal: Port **8443**, Interface **0**, Certificate tag **A** and My Devices portal: Port **8443**, Interface **0**, Certificate group **A**.
    - Sponsor portal: Port **8443**, Interface **0**, Certificate group **A** and My Devices portal: Port **8445**, Interface **0**, Certificate group **B**.
    - Sponsor portal: Port **8444**, Interface **1**, Certificate group **A** and Blocked List portal: Port **8444**, Interface **0**, Certificate group **B**.
  - Invalid combinations include:
    - Sponsor portal: Port **8443**, Interface **0**, Certificate group **A** and My Devices portal: **8443**, Interface **0**, Certificate group **B**.
    - Sponsor portal: Port **8444**, Interface **0**, Certificate tag **A** and Blocked List portal: Port **8444**, Interface **0**, Certificate group **A**.

Note We recommend that you use interface 0 for Guest services for best performance. You can either configure only interface 0 in the **Portal Settings**, or you can use the CLI command **ip host** to map a hostname or FQDN to the IP address of interface 0.

- **Allowed Interfaces**: Select the PSN interfaces which a PAN can use to run a portal. When a request to open a portal is made on the PAN, the PAN looks for an available allowed port on the PSN. You must configure the Ethernet interfaces using IP addresses on different subnets.

  These interfaces must be available on all the PSNs, including VM-based ones, that have Policy Services turned on. This is a requirement because any of these PSNs can be used for the redirect at the start of the guest session.

  - The Ethernet interfaces must use IP addresses on different subnets.
  - The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
  - The portal certificate Subject Name or Alternate Subject Name must resolve to the interface IP address.
  - Configure **ip host x.x.x.x yyy.domain.com** in Cisco ISE CLI to map the secondary interface IP address to the FQDN, which is used to match the certificate Subject Name or Alternate Subject Name.
  - If only the bonded NIC is selected, when the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN logs an error and exits. The PSN will not try to start the portal on the physical interface.
  - NIC Teaming or bonding is a configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based in the **Portal Settings** configuration. If both physical NICs and the corresponding bonded NIC are configured, when the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.

- The portal certificate Subject Name or Alternate Subject Name must resolve to the interface IP address.

- **Authentication Method**: Choose which identity source sequence or Identity Provider (IdP) to use for user authentication. The identity source sequence is a list of identity stores that are searched in sequence to verify user credentials.

  Cisco ISE includes a default identity source sequence for sponsor portals, Sponsor_Portal_Sequence.

  To configure IdP, choose **Administration** > **Identity Management** > **External Identity Sources** > **SAML Id Providers**.

  To configure an identity source sequence, choose **Administration > Identity Management > Identity Source Sequences**.

- **Employees Using this Portal as Guests Inherit Login Options and Dynamic Endpoint Group Assignment from**: Choose the Guest Type that employees are assigned to when they log in to this portal. The employees' endpoint data is stored in the endpoint identity group configured in that guest type for the **Store device information in endpoint identity group** attribute. No other attributes from the associated guest type are inherited.
- **Display Language**
    - **Use Browser Locale**: Use the language specified in the client browser's locale setting as the display language of the portal. If browser locale's language is not supported by Cisco ISE, then the **Fallback Language** is used as the language portal.
    - **Fallback Language**: Choose the language to use when the language cannot be obtained from the browser locale, or if the browser locale language is not supported by Cisco ISE.
    - **Always Use**: Choose the display language to use for the portal. This setting overrides the **User Browser Locale** option.

Login Page Settings for Credentialed Guest Portals

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Login Page Settings**.

- **Require an Access Code**: Assign an access code as the login credential that multiple guests should use to gain access to the network. An access code is primarily a locally known code that is given to physically present guests (either visually via a whiteboard or verbally by a lobby ambassador). It would not be known and used by someone outside the premises to access the network.

  You can use this option in addition to the usernames and passwords that are provided as the login credentials to individual guests.
- **Maximum Failed Login Attempts Before Rate Limiting**: Specify the number of failed login attempts from a single browser session before Cisco ISE starts to throttle that account. This does not cause an account lockout. The throttled rate is configured in **Time between login attempts when rate limiting**.
- **Time Between Login Attempts when Rate Limiting**: Set the length of time in minutes that a user must wait before attempting to log in again (throttled rate), after failing to log in the number of times defined in **Maximum failed login attempts before rate limiting**.
- **Include an AUP**: Add a acceptable use policy window to the flow. You can add the AUP to the window, or link to another window.
- **Allow Guests to Create their Own Accounts**: Provide an option on this portal’s Login page for guests to register themselves. If this option is not selected, sponsors create guest accounts. Enabling this also enables tabs on this page for you to configure **Self-Registration Page Settings** and **Self-Registration Success Page Settings**.

  If guests choose this option, they are presented with the Self-Registration form where they can enter the requested information to create their own guest accounts.
- **Allow Guests to Recover the Password**: This option enables a Reset Password button on the Guest portal for self-registered guests. If a self-registered guest who still has a valid account connects to the

login portal, and forgot their password, they can click **Reset Password**. That brings them back to the self-registration window, where they can enter their phone or email (whichever they registered with) and enter a new password.

- **Allow Social Login**: Use a social media site to get login credentials for users of this portal. Checking this option displays the following settings:
  - **Show registration form after social login**: This allows the user to change the information provided by Facebook.
  - **Require guests to be approved**: This informs the user that a sponsor must approve their account, and will send them credentials for login.
- **Allow guests to change password after login**: Allow guests to change their password after successfully authenticating and accepting the AUP, if it is required. If guests change their passwords, sponsors cannot provide guests with their login credentials if lost. The sponsor can only reset the guest's password back to a random password.

Note Internal users logged in through the guest portal cannot reset their passwords.

- **Allow the following identity-provider guest portal to be used for login**: Checking this option and selecting a SAML Id identity provider adds a link for that SAML Id to this portal. This sub-portal can be configured to look like the SAML IDP that the user is providing credentials for.
- **Allow social login**: Allow this portal to use a social media type for user login. For more information about configuring social login, see Social Login for Self-Registered Guests, on page 493.

Self-Registration Page Settings

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portal & Components** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Self Registration Page Settings**. Use these settings to enable guests to register themselves and specify the information that they must provide on the Self-Registration form.

- **Assign self-registered guests to guest type**: Choose the guest type to which all the self-registered guests using this portal are assigned.
- **Account valid for**: Specify the duration for the account in days, hours, or minutes after which the account expires unless you or the sponsor extend the account duration in the Sponsor portal.
- **Require a registration code for self registration**: Assign a code that the self-registering guests must enter to successfully submit their Self-Registration form. Similar to the access code, the registration code is provided to the guest offline to prevent someone who is outside the premises from accessing the system.
- **Fields to include**: Check the fields that you want to display on the Self-Registration form. Then check which fields are mandatory for the guests to complete in order to submit the form and receive a guest account. You may want to require fields such as **SMS Service Provider** and **Person being Visited** to gather important information from self-registering guests.
  - **Location**: Enter locations that the self-registering guests can select at registration time using the list of locations that you have defined. This automatically assigns the related time zones as the valid

access times for these guests. Use clear location names to avoid ambiguity during selection (for example, Boston Office, 500 Park Ave New York, Singapore).

If you plan to restrict guest access by time of day, the time zone is used to determine that time. Unless all your time-access controlled guests are in the San Jose time zone, then create a time zone for your locale. If there is only one location, it is automatically assigned as the default location, and this field does not display in the portal for guests to view. Also, **Location** is disabled in the list of **Fields to include**.

    - **SMS Service Provider**: Select which SMS providers to display on the Self-Registration form to enable self-registering guests to choose their own SMS provider. You can then use the guest's SMS service to send them SMS notifications, which minimize expenses for your company. If you only selected one SMS provider for the guest to use, this field will not display on the Self-Registration form.
    - **Person being visited**: This is a text field, so if you want to use it, instruct your guests what kind of information to enter into this field.
    - **Custom Fields**: Select the custom fields that you previously created to collect more data from the self-registering guests. Then check which fields are mandatory for the guests to complete in order to submit the Self-Registration form and receive a guest account. These fields are listed in alphabetical order by name. You create these fields on **Work Centers** > **Guest Access** > **Settings** > **Custom Fields** to add more custom fields.
    - **Include an AUP**: Display your company's network-usage terms and conditions, either as text on the page currently being displayed for the user or as a link that opens a new tab or window with AUP text.
        - **Require acceptance**: Ensure that the user has read the AUP completely. This configures an **Accept** button on the self-registration page. If you configured AUP **as on page**, then you can also disable the Accept button until after the user has scrolled to the end of the AUP.

- **Only allow guests with an email address from**: Specify an allowed list of domains which the self-registering guests can use in **Email Address** to create email addresses, for example, cisco.com.

  If you leave this field blank, any email address is valid, except for domains listed in **Do not allow guests with email address from**.

- **Do not allow guests with an email address from**: Specify a blocked list of domains which the self-registering guests cannot use in **Email Address** to create email addresses, for example, czgtgj.com.
- **Require self-registered guests to be approved**: Specify that the self-registering guests using this portal require approval from a sponsor before receiving their guest credentials. Clicking this option displays more options for how sponsors approve a self-registered guest.
    - **Allow guests to login automatically from self-registration after sponsor's approval**: A self-registered guest will be logged in automatically after sponsor approval.
    - **Email approval request to**:
        - **Sponsor email addresses listed below**: Enter one or more email addresses of sponsors designated as approvers, or a mailer, to which all guest approval requests should be sent. If the email address is not valid, approval fails.
        - **Person being visited**: **Require sponsor to provide credentials for authentication** field is displayed, and the **Required** option in **Fields to include** is enabled (if it was previously

disabled). These fields are displayed on the Self-Registration form requesting this information from the self-registering guests. If the email address is not valid, approval fails.

  - **Approve/Deny Link Settings**:
    - **Links are valid for**: You can set an expiration period for the account approval links.
    - **Require sponsor to provide credentials for authentication**: Check this to force the sponsor to enter credentials to approve the account, even if it is not required by the configuration in this section. This field is only visible if **Require self-registered guests to be approved** is set to **person being visited**.
    - **Sponsor is matched to a Sponsor Portal to verify approval privileges**: Click **Details** to select the portals that are searched to verify that the sponsor is a valid system user, a member of a sponsor group, and that the members of that group have authority to approve the account. Each sponsor portal has an identity source sequence, which is used to identify the sponsor. Portals are used in the order they are listed. The first portal in the list determines the style and customization used in the sponsor portal.

- **After registration submission, direct guest to**: Choose where the self-registered guest is directed after successfully registering.
  - **Self-Registration Success page**: Direct successfully self-registered guests to the **Self-Registration Success** window, which displays the fields and messages you have specified on **Self Registration Success Page Settings**.

    It may not be desirable to display all the information, because the system may be awaiting account approval (if enabled on this window) or delivering the login credentials to an email address or phone number based on the allowed list and blocked list domains specified on this window.

    If you enabled **Allow guests to log in directly from the Self-Registration Success page** in **Self-Registration Success Page Settings**, successfully self-registered guests can log in directly from this window. If it is not enabled, they are directed to the portal's Login window after the **Self-Registration Success** window is displayed.

  - **Login page with instructions about how to obtain login credentials**: Direct successfully self-registered guests back to the portal’s Login window and display a message, such as “Please wait for your guest credentials to be delivered either via email, SMS, or print format and proceed with logging in.”

    To customize the default message, click the **Portal Page Customization** tab and select **Self-Registration Page Settings**.

    The system may be awaiting account approval (if enabled on this window) or delivering the login credentials to an email address or phone number based on the allowed list and blocked list domains specified on this window.

  - **URL**: Direct successfully self-registered guests to the specified URL while waiting for their account credentials to be delivered.

    The system may be awaiting account approval (if enabled on this window) or delivering the login credentials to an email address or phone number based on the allowed list and blocked list domains specified on this window.

- **Send credential notification automatically using:**

- **Email**: Choose email as the option by which successfully self-registered guests receive their login credential information. If you choose this option, **Email address** becomes a required field in the list of **Fields to include** and you can no longer disable this option.
- **SMS**: Choose SMS as the option by which successfully self-registered guests receive their login credential information. If you choose this option, **SMS Service Provider** becomes a required field in the list of **Fields to include** and you can no longer disable this option.

Self Registration Success Page Settings

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Self Registration Success Page Settings**. Use these settings to notify successfully self-registered guests of the credentials they need to gain access to the network.

Field	Usage Guidelines
Include this information on the Self-Registration Success page	Check the fields that you want to display for the successfully self-registered guests on the Self-Registration Success page. If sponsor approval of the guest is not required, check **Username** and **Password** to display these credentials for the guest. If sponsor approval is required, these fields are disabled, because the credentials can only be delivered to the guest after they have been approved.
Allow guest to send information to self using	Check the options by which the successfully self-registered guest can send credential information to themselves: **Print**, **Email**, or **SMS**.
Include an AUP (on page/as link)	Display your company's network-usage terms and conditions, either as text on the window currently being displayed for the user or as a link that opens a new tab or window with AUP text.
Require Acceptance	Require users to accept an AUP before their account is fully enabled. The **Login** button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not obtain network access.
Require scrolling to end of AUP	This field displays if you chose the **AUP on page** option. Ensure that the user has read the AUP completely. The **Accept** button is enabled only after the user has scrolled to the end of the AUP.

Field	Usage Guidelines
Allow guests to log in directly from the Self-Registration Success page	Display a **Login** button at the bottom of the Self-Registration Success page. This enables the guest to bypass the Login page and automatically deliver the login credentials to the portal and display the next page in the portal flow (for instance, the AUP page).

Acceptable Use Policy (AUP) Page Settings for Credentialed Guest Portals

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Acceptable Use Policy (AUP) Page Settings**.

- **Include an AUP Page**: Display your company's network-usage terms and conditions on a separate page to the user.
- **Use Different AUP for Employees**: Display a different AUP and network-usage terms and conditions for employees only. If you choose this option, you cannot also choose **Skip AUP for employees**.
- **Skip AUP for Employees**: Employees are not required to accept an AUP before accessing the network. If you choose this option, you cannot also choose **Use different AUP for employees**.
- **Require Scrolling to End of AUP**: This option displays only if **Include an AUP on page** is enabled.

  Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP. Configure when the AUP appears to the user.

  - **On First Login only**: Display an AUP the first time the user logs into the network or portal.
  - **On Every Login**: Display an AUP every time the user logs into the network or portal.
  - **Every __ Days (starting at first login)**: Display an AUP periodically after the user first logs into the network or portal.

Guest Change Password Settings for Credentialed Guest Portals

Guest Change Password Settings

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Guest Change Password Settings**

- **Allow guests to change password after login**: Allow guests to change their password after successfully authenticating and accepting the AUP, if it is required. If guests change their passwords, sponsors cannot provide guests with their login credentials if lost. The sponsor can only reset the guest's password back to a random password.

Note Internal users logged in through the guest portal cannot reset their passwords.

Guest Device Registration Settings for Credentialed Guest Portals

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Guest Device Registration Settings**.

Use these settings to either ensure that Cisco ISE automatically registers guest devices when they log in to or to allow guests to manually register their devices after they log in.

The maximum number of devices is specified for each guest type in **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Types**.

- **Automatically Register Guest Devices**: Automatically create an endpoint for the device from which the guest is accessing this portal. The endpoint is added to the endpoint identity group specified for this portal.

  An authorization rule can now be created to allow access to endpoints in that identity group, so that web authentication is no longer required.

  If the maximum number of registered devices is reached, the system automatically deletes the first registered device, registers the device the guest is trying to log in with, and notifies them. Choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Types** to change the maximum number of devices with which a guest can register.

- **Allow Guests to Register Devices**: Guests can register their devices manually by providing a name, description and MAC address. The MAC address is associated with an endpoint identity group.

  If the maximum number of registered devices is reached, the guest is required to delete at least one device before being allowed to register another device.

BYOD Settings for Credentialed Guest Portals

The navigation path for this page is **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **BYOD Settings**.

Use these settings to enable Bring Your Own Device (BYOD) functionality for non-guests, such as employees, using the Credentialed Guest portals to access your corporate network.

Field	Usage Guidelines
Allow Employees to use Personal Devices on the Network	Add the BYOD Registration window to this portal allowing employees to go through the employee device registration process, and possibly native supplicant and certificate provisioning, depending on the settings for Client Provisioning for the employee's personal device type (for example, iOS, Android, OSX).
Endpoint Identity Group	Choose an endpoint identity group to track guest devices. Cisco ISE provides the **GuestEndpoints** endpoint identity group to use as a default. You can also create more endpoint identity groups if you choose to not use the default.

Field	Usage Guidelines
Allow employees to choose to get guest access only	Let employees access your guest network and avoid additional provisioning and registration that may be required to access your corporate network.
Display Device ID Field During Registration	Display the device ID to the user during the registration process, even though the device ID is pre-configured and cannot be changed while using the BYOD portal.
Originating URL	After successfully authenticating to the network, redirect the user's browser to the original website that the user is trying to access, if available. If not available, the Authentication Success window appears. Make sure that the redirect URL is allowed to work on port 8443 of the PSN by the access-control list on the NAD and by authorization profiles configured in Cisco ISE for that NAD. For Windows, MAC, and Android devices, control is given to the Self-Provisioning Wizard app, which does provisioning. Therefore, these devices are not redirected to the originating URL. However, iOS (dot1X) and unsupported devices (that are allowed network access) are redirected to this URL.
Success page	Display a page indicating that the device registration was successful.
URL	After successfully authenticating to the network, redirect the user's browser to the specified URL, such as your company's website.

Post-Login Banner Page Settings for Credentialed Guest Portals

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals or Sponsor Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Post-Login Banner Page Settings**.

Use this setting to notify users (guests, sponsors or employees as applicable) of additional information after they log in successfully.

Field	Usage Guidelines
Include a Post-Login Banner page	Display additional information after the users successfully log in and before they are granted network access.

Guest Device Compliance Settings for Credentialed Guest Portals

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Guest Device Compliance Settings**. Use these settings to require guests, and employees using the guest portal, to undergo client provisioning of their devices in order to gain access to the network.

- **Require guest device compliance**—Redirect guests to the Client Provisioning page, which requires them to download a posture agent. This adds client provisioning to the Guest flow, where you configure posture policies for guests, such as checking for virus protection software.

  If the guest is an employee using the Credentialed Guest portals to access the network and:

    - If you enabled **Allow employees to use personal devices on the network** in the **BYOD Settings**, the employee is redirected to the BYOD flow and will not undergo client provisioning.
    - If you enabled both **Allow employees to use personal devices on the network** and **Allow employees to choose to get guest access only** in the **BYOD Settings**, and the employee chooses guest access, they are routed to the Client Provisioning page.

VLAN DHCP Release Page Settings for Guest Portals

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **VLAN DHCP Release Page Settings**.

- **Enable VLAN DHCP release**: Refresh a guest's IP address for Windows devices after a VLAN change in both wired and wireless environments.

  This affects the Central WebAuth (CWA) flow during final authorization, when the network access changes the guest VLAN to a new VLAN. The guest's old IP address must be released before the VLAN change, and a new guest IP address must be requested through DHCP when the guest connects to the new VLAN. The IP address release and renew operations are supported only on the Internet Explorer Browser which uses DirectX controls.

  The VLAN DHCP Release option does not work on mobile devices. Instead, guests are requested to manually reset the IP address. This method varies by devices. For example, on Apple iOS devices, guests can select the Wi-Fi network and click the **Renew Lease** button.

- **Delay to Release __ Seconds**: Enter the delay to release time. We recommend a short value, because the release must occur immediately after the applet is downloaded, and before the Cisco ISE server directs the NAD to re-authenticate with a CoA request.
- **Delay to CoA __ Seconds**: Enter the time to delay Cisco ISE from executing the CoA. Provide enough time (use the default value as a guideline) to allow the applet to download and perform the IP release on the client.
- **Delay to Renew __ Seconds**: Enter the delay to renew value. This time is added to the IP release value and does not begin timing until the control is downloaded. Provide enough time (use the default value as a guideline) so that the CoA is allowed to process and the new VLAN access granted.

Authentication Success Settings for Guest Portals

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Authentication Success Settings**.

These settings notify the users (guests, sponsors, or employees as applicable) of authentication success or display a URL. Under **Once authenticated, take guest to:**, configure the following fields:

- **Originating URL**: After successfully authenticating to the network, redirect the user's browser to the original website that the user is trying to access, if available. If not available, the Authentication Success window appears. Make sure that the redirect URL is allowed to work on port 8443 of the PSN by the access-control list on the NAD and by authorization profiles configured in ISE for that NAD.

  For Windows, MAC, and Android devices, control is given to the Self-Provisioning Wizard app, which does provisioning. Therefore, these devices are not redirected to the originating URL. However, iOS (dot1X) and unsupported devices (that are allowed network access) are redirected to this URL.

- **Authentication Success page**: Notification of successful authentication of the user.

- **URL**: After successfully authenticating to the network, redirect the user's browser to the specified URL, such as your company's website.

Note If you redirect a Guest to an external URL after authentication, there may be a delay while the URL address is resolved and the session is redirected. Make sure that the redirect URL is allowed to work on port 8443 of the PSN by the access-control list on the NAD and by authorization profiles configured in ISE for that NAD.

Support Information Page Settings for Guest Portals

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Support Information Page Settings**.

Use these settings to display the information that your Help Desk can use to troubleshoot access issues experienced by users (guests, sponsors or employees as applicable).

Field	Usage Guidelines
Include a Support Information Page	Display a link to an information window, such as **Contact Us**, on all enabled windows for the portal.
MAC Address	Include the MAC address of the device on the **Support Information** window.
IP Address	Include the IP address of the device on the **Support Information** window.
Browser User Agent	Include the browser details such as the product name and version, layout engine, and version of the user agent originating the request on the **Support Information** window.

Field	Usage Guidelines
Policy Server	Include the IP address of the ISE Policy Service Node (PSN) that is serving this portal on the **Support Information** window.
Failure Code	If available, include the corresponding number from the log message catalog. To view the message catalog, choose **Administration** > **System** > **Logging** > **Message Catalog**.
Hide Field	Do not display any field labels on the **Support Information** window if the information that they would contain is non-existent. For example, if the failure code is unknown, and therefore blank, do not display **Failure Code**, even if it is selected.
Display Label with no Value	Display all selected field labels on the **Support Information** window, even if the information that they would contain is non-existent. For example, if the failure code is unknown, display **Failure Code**, even if it is blank.
Display Label with Default Value	Display this text in any selected field on the **Support Information** window, if the information that they would contain is non-existent. For example, if you enter Not Available in this field, and the failure code is unknown, the **Failure Code** field displays **Not Available**.

Sponsor Portal Application Settings

Portal Identification Settings

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals or Sponsor Portals** > **Create, Edit or Duplicate** > **Guest Portals or Sponsor Portals Settings and Customization**.

- **Portal Name**: Enter a unique portal name to access this portal. Do not use this portal name for any other Sponsor, Guest, or nonguest portals, such as Blocked List, Bring Your Own Device (BYOD), Client Provisioning, Mobile Device Management (MDM), or My Devices portals.

  This name appears in the authorization profile portal selection for redirection choices. It is applied to the list of portals for easy identification among other portals.

- **Description**: Optional.

- **Portal Test URL**: A system-generated URL displays as a link after you click **Save**. Use it to test the portal.

Click the link to open a new browser tab that displays the URL for this portal. Policy Services Node (PSN) with Policy Services must be turned on. If Policy Services are disabled, the PSN only displays the Admin portal.

Note The test portal does not support RADIUS sessions, so you won't see the entire portal flow for all portals. BYOD and Client Provisioning are examples of portals that depend on RADIUS sessions. For example, a redirect to an external URL will not work. If you have more than one PSN, Cisco ISE chooses the first active PSN.

- **Language File**: Each portal type supports 15 languages by default, which are available as individual properties files bundled together in a single zipped language file. Export or import the zipped language file to use with the portal. The zipped language file contains all the individual language files that you can use to display text for the portal.

  The language file contains the mapping to the particular browser locale setting along with all of the string settings for the entire portal in that language. A single language file contains all the supported languages, so that it can easily be used for translation and localization purposes.

  If you change the browser locale setting for one language, the change is applied to all the other end-user web portals. For example, if you change the French.properties browser locale from fr,fr-fr,fr-ca to fr,fr-fr in the Hotspot Guest portal, the changes also apply to the My Devices portal.

  An alert icon displays when you customize any of the text on the **Portal Page Customizations** tab. The alert message reminds you that any changes made to one language while customizing the portal must also be added to all the supported languages properties files. You can manually dismiss the alert icon using the drop-down list option; or it is automatically dismissed after you import the updated zipped language file.

Portal Settings for Sponsor Portals

Configure these settings to identify the portal and select the language files to be used for all the portal pages.

- **HTTPS Port**: Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blocked List Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you modify this window. If you modify this window, update the port setting to comply with this restriction.

  If you assign ports used by a non-guest (such as My Devices) portal to a guest portal, an error message appears.

  For posture assessments and remediation only, the Client Provisioning portal also uses ports 8905 and 8909. Otherwise, it uses the same ports assigned to the Guest portal.

  Portals assigned to the same HTTPS port can use the same Gigabit Ethernet interface or another interface. If they use the same port and interface combination, they must use the same certificate group tag. For example:

  - Valid combinations include, using the Sponsor portal as an example:
    - Sponsor portal: Port **8443**, Interface **0**, Certificate tag **A** and My Devices portal: Port **8443**, Interface **0**, Certificate group **A**.

        - Sponsor portal: Port **8443**, Interface **0**, Certificate group **A** and My Devices portal: Port **8445**, Interface **0**, Certificate group **B**.
        - Sponsor portal: Port **8444**, Interface **1**, Certificate group **A** and Blocked List portal: Port **8444**, Interface **0**, Certificate group **B**.
    - Invalid combinations include:
        - Sponsor portal: Port **8443**, Interface **0**, Certificate group **A** and My Devices portal: **8443**, Interface **0**, Certificate group **B**.
        - Sponsor portal: Port **8444**, Interface **0**, Certificate tag **A** and Blocked List portal: Port **8444**, Interface **0**, Certificate group **A**.

Note We recommend that you use interface 0 for Guest services for best performance. You can either configure only interface 0 in the **Portal Settings**, or you can use the CLI command **ip host** to map a hostname or FQDN to the IP address of interface 0.

- **Allowed Interfaces**: Select the PSN interfaces which a PAN can use to run a portal. When a request to open a portal is made on the PAN, the PAN looks for an available allowed port on the PSN. You must configure the Ethernet interfaces using IP addresses on different subnets.

  These interfaces must be available on all the PSNs, including VM-based ones, that have Policy Services turned on. This is a requirement because any of these PSNs can be used for the redirect at the start of the guest session.

    - The Ethernet interfaces must use IP addresses on different subnets.
    - The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
    - The portal certificate Subject Name or Alternate Subject Name must resolve to the interface IP address.
    - Configure **ip host x.x.x.x yyy.domain.com** in Cisco ISE CLI to map the secondary interface IP address to the FQDN, which is used to match the certificate Subject Name or Alternate Subject Name.
    - If only the bonded NIC is selected, when the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN logs an error and exits. The PSN will not try to start the portal on the physical interface.
    - NIC Teaming or bonding is a configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based in the **Portal Settings** configuration. If both physical NICs and the corresponding bonded NIC are configured, when the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.

- **Certificate Group tag**: Pick a certificate group tag that specifies the certificate to be used for the portal's HTTPS traffic.
- **Fully Qualified Domain Name (FQDN)**: Enter at least one unique FQDN or hostname for the Sponsor or MyDevices portal. For example, you can enter `sponsorportal.yourcompany.com,sponsor`, so that when the user enters either of those into a browser, the sponsor portal displays. Separate names with commas, but do not include spaces between entries.

  If you change the default FQDN, then also do the following:

  - Update your DNS so that the FQDN of the new URL resolves to a valid Policy Services Node (PSN) IP address. Optionally, this address could point to a load balancer virtual IP address that serves a pool of PSNs.
  - To avoid certificate warning messages due to name mismatches, include the FQDN of the customized URL, or a wildcard, in the subject alternative name (SAN) attribute of the local server certificate of the Cisco ISE PSN. If the **Allow Kerberos SSO** option is enabled for the sponsor portal, you must include the FQDN of the Cisco ISE PSN, or a wildcard, in the SAN attribute of the local server certificate used by the portal.
- **Authentication Method**: Choose which identity source sequence or Identity Provider (IdP) to use for user authentication. The identity source sequence is a list of identity stores that are searched in sequence to verify user credentials.

  Cisco ISE includes a default identity source sequence for sponsor portals, Sponsor_Portal_Sequence.

  To configure IdP, choose **Administration** > **Identity Management** > **External Identity Sources** > **SAML Id Providers**.

  To configure an identity source sequence, choose **Administration > Identity Management > Identity Source Sequences**.
- **Idle Timeout**: Enter the time in minutes that you want Cisco ISE to wait before it logs out the user if there is no activity in the portal. The valid range is from 1 to 30 minutes.
- **Allow Kerberos**: Use Kerberos to authenticate a sponsor for access to the sponsor portal. Kerberos SSO is performed inside the secure tunnel after the browser establishes the SSL connection with ISE.

  Kerberos authentication requires the following items to be in the same domain:

  - Sponsor's PC
  - ISE PSN
  - FQDN configured for this sponsor portal

Note Kerberos authentication is NOT supported for the Guest portal.

- **Display Language**
  - **Use Browser Locale**: Use the language specified in the client browser's locale setting as the display language of the portal. If browser locale's language is not supported by Cisco ISE, then the **Fallback Language** is used as the language portal.

    - **Fallback Language**: Choose the language to use when the language cannot be obtained from the browser locale, or if the browser locale language is not supported by Cisco ISE.
    - **Always Use**: Choose the display language to use for the portal. This setting overrides the **User Browser Locale** option.
- **SSIDs Available to Sponsors**: Enter the names or the SSIDs (Session Service Identifiers) of the networks that a sponsor can notify guests as the correct networks to connect to for their visit.

Login Settings for Sponsor Portals

Login Page Settings for Sponsor Portals

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Login Page Settings**.

- **Maximum Failed Login Attempts Before Rate Limiting**: Specify the number of failed login attempts from a single browser session before Cisco ISE starts to throttle that account. This does not cause an account lockout. The throttled rate is configured in **Time between login attempts when rate limiting**.
- **Time Between Login Attempts when Rate Limiting**: Set the length of time in minutes that a user must wait before attempting to log in again (throttled rate), after failing to log in the number of times defined in **Maximum failed login attempts before rate limiting**.
- **Include an AUP**: Add a acceptable use policy window to the flow. You can add the AUP to the window, or link to another window.

Acceptable Use Policy (AUP) Settings for Sponsor Portals

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Acceptable Use Policy (AUP) Page Settings**.

Use these settings to define the AUP experience for the users (guests, sponsors or employees as applicable).

Field	Usage Guidelines
Include an AUP Page	Display your company's network-usage terms and conditions on a separate page to the user.
Require scrolling to end of AUP	Ensure that the user has read the AUP completely. The **Accept** button is enabled only after the user has scrolled to the end of the AUP.
On First Login only	Display an AUP when the user logs into the network or portal for the first time only.
On Every Login	Display an AUP each time the user logs into the network or portal.

Field	Usage Guidelines
Every __ Days (starting at first login)	Display an AUP periodically after the user first logs into the network or portal.

Sponsor Change Password Settings for Sponsor Portals

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Sponsor Change Password Settings**. These settings define the password requirements for sponsors using the Sponsor portal.

Field	Usage Guidelines
Allow sponsors to change their own passwords	Allow sponsors to change their passwords after they log into the Sponsor portal. This option displays a Change Password page only if the sponsors are part of the Internal Users database.

Post-Login Banner Settings for Sponsor Portals

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals or Sponsor Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Post-Login Banner Page Settings**.

Use this setting to notify users (guests, sponsors or employees as applicable) of additional information after they log in successfully.

Field	Usage Guidelines
Include a Post-Login Banner page	Display additional information after the users successfully log in and before they are granted network access.

Support Information Page Settings for Sponsor Portals

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Support Information Page Settings**.

Use these settings to display the information that your Help Desk can use to troubleshoot access issues experienced by users (guests, sponsors or employees as applicable).

Field	Usage Guidelines
Include a Support Information Page	Display a link to an information window, such as **Contact Us**, on all enabled windows for the portal.
MAC Address	Include the MAC address of the device on the **Support Information** window.

Field	Usage Guidelines
IP Address	Include the IP address of the device on the **Support Information** window.
Browser User Agent	Include the browser details such as the product name and version, layout engine, and version of the user agent originating the request on the **Support Information** window.
Policy Server	Include the IP address of the ISE Policy Service Node (PSN) that is serving this portal on the **Support Information** window.
Failure Code	If available, include the corresponding number from the log message catalog. To view the message catalog, choose **Administration** > **System** > **Logging** > **Message Catalog**.
Hide Field	Do not display any field labels on the **Support Information** window if the information that they would contain is non-existent. For example, if the failure code is unknown, and therefore blank, do not display **Failure Code**, even if it is selected.
Display Label with no Value	Display all selected field labels on the **Support Information** window, even if the information that they would contain is non-existent. For example, if the failure code is unknown, display **Failure Code**, even if it is blank.
Display Label with Default Value	Display this text in any selected field on the **Support Information** window, if the information that they would contain is non-existent. For example, if you enter Not Available in this field, and the failure code is unknown, the **Failure Code** field displays **Not Available**.

Notify Guests Customization for Sponsor Portals

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Create, Edit or Duplicate** > **Portal Page Customization** > **Notify Guests**.

Under **Page Customizations**, you can customize the messages, titles, content, instructions, and field and button labels that appear on the notifications that sponsors send to guests from the Sponsor portal.

Under **Settings**, you can specify whether sponsors can send usernames and passwords separately to guests using email or SMS. You can also specify whether sponsors can display a Support Information page for guests to provide information that a help desk can use to troubleshoot access issues.

Manage and Approve Customization for Sponsor Portals

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Create, Edit or Duplicate** > **Portal Page Customization** > **Manage and Approve**.

Under **Page Customizations**, you can customize the messages, titles, content, instructions, and field and button labels that appear on the Manage and Approve tabs of the Sponsor portal.

These include the accounts (registered and pending) summary and detailed views, the pop-up dialogs that display based on the operations the sponsor performs on guest accounts such as edit, extend, suspend and so on, and also general portal and account action messages.

Global Settings for Guest and Sponsor Portals

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Guest Access** > **Settings**. You can configure the following general settings that apply to Guest and Sponsor portals, guest types, and sponsor groups in Cisco ISE:

- Policies for purging guest accounts and generating usernames and passwords.
- SMTP servers and SMS gateways to use when sending email and SMS notifications to guests and sponsors.
- Locations, time zones, SSIDs, and custom fields to select from when creating guest accounts and when registering guests using Self-Registration Guest portals.

After configuring these global settings, you can use them as needed when configuring specific Guest and Sponsor portals, guest types, and sponsor groups.

The following tabs are on the Portal settings page:

- **Guest Account Purge Policy**: Schedule when to purge guest accounts that have expired. For more information, see Schedule When to Purge Expired Guest Accounts, on page 485.
- **Custom Fields**: Add custom fields to use in Guest portals, to retrieve additional information from users. For more information, see Add Custom Fields for Guest Account Creation, on page 485.
- **Guest Email Settings**: Decide whether to email notifications to guests about changes in their account. For more information, see Specify Email Addresses and SMTP Servers for Email Notifications, on page 486.
- **Guest Locations and SSIDs**: Configure the Locations and the Service Set Identifiers (SSIDs) of the networks that guests can use at these Locations. For more information, see Assign Guest Locations and SSIDs, on page 487.
- **Guest Username Policy**: Configure how guest user names are created. For more information, see Set the Guest Username Policy, on page 490 and Rules for Guest Password Policies, on page 488.
- **Guest Password Policy**: Define the guest password policies for all Guest and Sponsor portals. For more information, see Set the Guest Password Policy and Expiration, on page 488.
- **Logging**: Guest users are tracked by the MAC address of their device. When guest users are displayed in reports, the username is the MAC address. If you select this option, reports will show the portal user

ID as the username, instead of the MAC address. For more information about this option, see Guest Remember Me, on page 512.

Guest Type Settings

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Types**. Use these settings to create the types of Guests that can access your network and their access privileges. You can also specify which Sponsor Groups can create this type of Guest.

- **Guest type name**: Provide a name (from 1 to 256 characters) that distinguishes this Guest Type from the other Guest Types.
- **Description**: Provide additional information (maximum of 2000 characters) about the recommended use of this Guest Type, for example, Use for self-registering Guests.
- **Language File**: This field allows you to export and import the language file, which contains content for email subject, email message, and SMS messages in all supported languages. These languages and content are used in notifications about an expired account, and are sent to guests who are assigned to this guest type. If you are creating a new guest type, this feature is disabled until after you save the guest type. For more information about editing the lanaguage file, see Portal Language Customization, on page 589.
- **Collect Additional Data**: Click the **Custom Fields** option to select which custom fields to use to collect additional data from guests using this Guest Type.

  To manage custom fields, choose **Work Centers** > **Guest Access** > **Settings** > **Custom Fields**.
- **Maximum Access Time**
  - **Account duration starts**: If you select **From first login**, the account start time starts when the guest user first logs in to the guest portal, and the end time equals the configured duration time. If the guest user never logs in, the account remains in the `Awaiting first login` state until the guest account purge policy removes the account.

    Values are from 1 to 999 days, hours, or minutes.

    A self-registered user's account starts when they create and log on to their account.

    If you select **From sponsor-specified date**, enter the maximum number of days, hours, or minutes that Guests of this Guest Type can access and stay connected to the network.

    If you change these settings, your changes will not apply to existing Guest accounts that were created using this Guest Type.
  - **Maximum account duration**: Enter the number of days, hours, or minutes that guests assigned to this guest type can log on.

Note The account purge policy checks for expired guest accounts, and sends expiration notification. This policy runs every 20 minutes, so if you set the account duration to less than 20 mins, it is possible that expiration notices may not be sent out before the account is purged.

You can specify the duration time and the days of the week when access is provided to the guests of this Guest Type by using the **Allow access only on these days and times** option.

        - The days of the week that you select limits access to the dates that are selectable in the Sponsor's calendar.
        - Maximum account duration is enforced in the sponsor portal, when the Sponsor picks duration and dates.

    The settings you make here for access time affect the time settings that are available on the sponsor portal when creating a guest account. For more information, see Configuring the Time Settings Available to Sponsors , on page 523.

- **Logon Options**
    - **Maximum simultaneous logins**: Enter the maximum number of user sessions that users assigned to this Guest Type can have running concurrently.
    - **When guest exceeds limit**: When you select **Maximum simultaneous logins**, you must also select the action to take when a user connects after the maximum number of login is reached.
        - **Disconnect the oldest connection**
        - **Disconnect the newest connection**: If you select **Redirect user to a portal page showing an error message**, an error message is displayed for a configurable amount of time, then the session is disconnected, and the user is redirected to the Guest portal. The error page's content is configured on the Portal Page Customization dialog, on the **Messages** > **Error Messages** window.
    - **Maximum devices guests can register**: Enter the maximum number of devices that can be registered to each Guest. You can set the limit to a number lower than what is already registered for the Guests of this Guest Type. This only affects newly created Guest accounts. When a new device is added, and the maximum is reached, the oldest device is disconnected.
    - **Endpoint identity group for guest device registration**: Choose an endpoint identity group to assign to guest devices. Cisco ISE provides the **GuestEndpoints** endpoint identity group to use as a default. You can also create more endpoint identity groups if you choose to not use the default.
    - **Allow guest to bypass the Guest portal**: Allows users to bypass the credentialed guest-type captive portal (web authentication page), and access the network by providing credentials to wired and wireless (dot1x) supplicants or VPN clients. Guest accounts change to the `Active` state, bypassing the `Awaiting Initial Login` state and the AUP page, even if the AUP is required.

      If you do not enable this setting, users must first log in through the credentialed Guest captive portal before they are able to access other parts of the network.

- **Account Expiration Notification**
    - **Send account expiration notification __ days before account expires**: Send a notification to Guests before their account expires and specify how many days, hours, or minutes before the expiration.
    - **View messages in**: Specify the language to use when displaying email or SMS notifications as you set them up.
    - **Email**: Send account expiration notices by email.
    - **Use customization from**: Apply the same customizations that you configured for the selected portal to this Guest Type's account expiration emails.

    - **Copy text from**: Reuse email text that you created for another Guest Type's account expiration email.
    - **SMS**: Send account expiration notices by SMS.

      The settings that follow for SMS are the same as for email notifications, except that you choose an SMS gateway for **Send test SMS to me**.

- **Sponsor Groups**: Specify the sponsor groups whose members can create a guest account using this guest type. Delete the sponsor groups that you do not want to have access to this guest type.

Sponsor Group Settings

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Groups**. Use these settings to add members to the sponsor group, define guest types and location privileges, and set permissions related to creating and managing guest accounts.

- **Disable Sponsor Group**: Disable members of this sponsor group from accessing the Sponsor portal.

  For instance, you may want to temporarily prevent sponsors from logging in to the Sponsor portal while configuration changes are being made in the Admin portal. Or, you may want to disable a sponsor group that is involved in infrequent activity, such as sponsoring guests for an annual convention, until the time they need to be activated again.

- **Sponsor group name**: Enter a unique name (from 1 to 256 characters).
- **Description**: Include useful information (maximum of 2000 characters) such as the guest types used by this sponsor group.
- **Configure Guest Types**: If the guest type you need is not available, click **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Types** and create a new guest type or edit an existing one.
- **Match Criteria**
    - **Members**: Click to display the **Select Sponsor Group Members** box, where you can select available user identity groups (from internal and external identity stores) and add them as members of this sponsor group.
        - **Sponsor Group Members**: Search and filter the list of selected sponsor groups and delete any groups you do not want to include.

    - **Other conditions**: Click **Create New Condition** to build one or more conditions that a sponsor must match to be included in this sponsor group. You can use authentication attributes from Active Directory, LDAP, SAML, and ODBC identity stores, but not RADIUS Token or RSA SecurID stores. You can also use internal user attributes. Conditions have an attribute, and operator, and a value.
        - To create a condition using the internal dictionary attribute *Name*, prefix the identity group name with User Identity Groups. For example:

          InternalUser:Name EQUALS bsmith

          This means that only internal users with the Name "bsmith" can belong to this sponsor group.

- **This sponsor group can create accounts using these guest types**: Specify the guest types that the members in this sponsor group can use when creating guest accounts. For a sponsor group to be enabled, it must have at least one guest type that it can use.

  If you assign only one guest type to this sponsor group, you can choose not to display it in the Sponsor portal because it is the only valid guest type available for use. Choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portal** > **Page Customization** > **Create Accounts** > **Guest Types** > **Settings**. Check **Hide guest type if only one is available to sponsor** to enable this option.

- **Select the locations that guests will be visiting**: Select the locations that can be assigned to guests while creating their accounts. This helps define the valid time zones for these guest accounts and specifies all the time parameters that apply to the guest, such as valid access times. This does not prevent guests from connecting to the network from other locations.

  For a sponsor group to be enabled, it must have at least one location that it can use.

  If you assign only one location to this sponsor group, it will be the only valid time zone for the guest accounts created by its members. By default, it does not display in the Sponsor portal.

Sponsor Can Create

- **Multiple guest accounts assigned to specific guests (Import)**: Enable the sponsor to create multiple guest accounts by importing guest details such as first name and last name from a file.

  If this option is enabled, the **Import** option appears in the **Create Accounts** page of the Sponsor portal. The Import option is only available on desktop browsers (not mobile), such as Internet Explorer, Firefox, Safari, and so on.

- **Limit to batch of**: If this sponsor group is allowed to create multiple accounts simultaneously, specify the number of guest accounts that can be created in a single import operation.

  Although a sponsor can create a maximum of 10,000 accounts, we recommend that you limit the number of accounts you create, due to potential performance issues.

- **Multiple guest accounts to be assigned to any guests (Random)**: Enable the sponsor to create multiple random guest accounts as placeholders for guests who are not known as yet, or when they need to create many accounts quickly.

  If this option is enabled, the **Random** option appears in the **Create Accounts** window of the Sponsor portal.

- **Default username prefix**: Specify a username prefix that sponsors can use when creating multiple random guest accounts. If specified, this prefix appears in the Sponsor Portal when creating random guest accounts. In addition, if **Allow sponsor to specify a username prefix** is:

  - Enabled: The sponsor can edit the default prefix in the Sponsor portal.
  - Not enabled: The sponsor cannot edit the default prefix in the Sponsor portal.

  If you do not specify a username prefix or allow the sponsor to specify one, then the sponsor will not be able to assign username prefixes in the Sponsor portal.

- **Allow sponsor to specify a username prefix**: If this sponsor group is allowed to create multiple accounts simultaneously, specify the number of guest accounts that can be created in a single import operation.

  Although a sponsor can create a maximum of 10,000 accounts, we recommend that you limit the number of accounts you create, due to potential performance issues.

- **Start date can be no more than __ days into the future**: Specify the number of days within which sponsors have to set as the start date for the multiple guest accounts they have created.

Sponsor Can Manage

- **Only accounts sponsor has created**: Sponsors in this group can view and manage only the guest accounts that they have created, which is based on the Sponsor's email account.
- **Accounts created by members of this sponsor group**: Sponsors in this group can view and manage the guest accounts created by any sponsor in this sponsor group.
- **All guest accounts**: Sponsors view and manage all pending guest accounts.

Note Regardless of the group membership, all sponsors can see all pending accounts, unless you check **Approve and view requests from self-registering guests** with the option **Only pending accounts assigned to this sponsor** under **Sponsor Can**.

Sponsor Can

- **Update guests' contact information (email, Phone Number)**: For guest accounts that they can manage, allow the sponsor to change a guest's contact information
- **View/print guests' passwords**: When this option is enabled, the sponsor can print passwords for guests. The sponsor can see the passwords for guests on the **Manage Accounts**window and in the details for a guest. When this is not checked, the sponsor can't print the password, but the user can still get the password through email or SMS, if configured.
- **Send SMS notifications with guests' credentials**: For guest accounts that they can manage, allow the sponsor to send SMS (text) notifications to guests with their account details and login credentials.
- **Reset guest account passwords**: For guest accounts that they can manage, allow the sponsor to reset passwords for guests to a random password generated by Cisco ISE.
- **Extend guests' accounts**: For guest accounts that they can manage, allow the sponsor to extend them beyond their expiration date. The sponsor is automatically copied on email notifications sent to guests regarding their account expiration.
- **Delete guests' accounts**: For guest accounts that they can manage, allow the sponsor to delete the accounts, and prevent guests from accessing your company's network.
- **Suspend guests' accounts**: For guest accounts that they can manage, allow the sponsor to suspend their accounts to prevent guests from logging in temporarily.

  This action also issues a Change of Authorization (CoA) Terminate to remove the suspended guests from the network.

  - **Require sponsor to provide a reason**: Require the sponsor to provide an explanation for suspending the guest accounts.

- **Approve and view requests from self-registering guests**: Sponsors who are included in this Sponsor Group can either view all pending account requests from self-registering guests (that require approval), or only the requests where the user entered the Sponsor's email address as the person being visited. This feature requires that the portal used by the Self-registering guest has **Require self-registered guests to be approved** checked, and the Sponsor's email is listed as the person to contact. This feature also requires that the **Email** attribute be properly configured in the Sponsor's identity source.

  - Any pending accounts: A sponsor belonging to this group an approve and review accounts that were created by any sponsor.
  - Only pending accounts assigned to this sponsor: A sponsor belonging to this group can only view and approve accounts that they created.

Note The **Email** attribute is part of **User Info Attributes**. For more information on the **Email** attribute, see:

- Configure Custom Schema, on page 661
- **Schema** and **User Info** attributes in the LDAP General Settings table in LDAP Identity Source Settings, on page 615.
- Step 8 in Configure SAML ID Provider, on page 767.

- **Access Cisco ISE guest accounts using the programmatic interface (Guest REST API)**: For guest accounts that they can manage, allow the sponsor to access guest accounts using the Guest REST API programming interface.

End-User Portals

Cisco ISE provides web-based portals for three primary sets of end users:

- Guests who need to temporarily access your enterprise network using the Guest portals (Hotspot and credentialed Guest portals).
- Employees who are designated as sponsors who can create and manage guest accounts using the Sponsor portal.
- Employees who are using their personal devices on the enterprise network using the various non-guest portals such as the Bring Your Own Device (BYOD), Mobile Device Management (MDM), and My Devices portals.

Customization of End-User Web Portals

You can edit, duplicate, and create more portals. You can also fully customize the portal appearance and, therefore, the portal experience. You can customize each individual portal without affecting other portals.

You can customize various aspects of the portal interface that apply to the entire portal or to specific pages of the portal, such as:

- Themes, images, colors, banners, and footers
- Languages used for displaying portal text, error messages, and notifications

- Titles, content, instructions, and field and button labels
- Notifications sent to guests via email, SMS, and printer (applies only to the Self-Registered Guest and Sponsor portals)
- Error and informational messages displayed to users
- For the the Self-Registered Guest and Sponsor portals, you can create custom fields to gather guest information specific to your needs

ISE Community Resource

For more information about customizing web portals, see ISE Portal Builder and HowTo: ISE Web Portal Customization Options.

Customization Methods

There are several different ways to customize the end user portals pages, which require different levels of knowledge.

- **Basic**: You can modify the portal Customization page:
  - Upload banners and logos
  - Change some colors (except for buttons)
  - Change the text on the screens, and the language used on the entire portal
- **Intermediate**
  - Use the minieditor to add HTML and Javascript

Note Before you can enter HTML in a minieditor, click the HTML icon.

  - Use the jQuery mobile theme roller to change the color of all page elements
- **Advanced**
  - Manually modify properties and CSS files.

After you customize your portal, you can create multiple portals (of the same type) by duplicating it. For example, if you customized your Hotspot Guest portal for one business entity, you can duplicate it and make minor changes to create custom Hotspot Guest portals for other business entities.

Tips for Customizing Portals with the Mini Editors

- Long words in a minieditor box may scroll off the screen area of the portal. You can break the line with the HTML paragraph attribute style="word-wrap: break-word". For example:

```
 <p style="word-wrap:break-word">

thisisaverylonglineoftextthatwillexceedthewidthoftheplacethatyouwanttoputitsousethisstructure

 </p>
```

- When you use HTML or javascript to customize portal pages, make sure that you use valid syntax. Cisco ISE doesn't validate the tags and code that you enter into a minieditor. Invalid syntax may cause problems during the portal flow.

Portal Content Types

Cisco ISE provides a default set of portal themes that you can use "as is" or customize by using the existing CSS files as models to create new custom files. However, you can alter the appearance of the portals without using customized CSS files.

For instance, if you want to use unique corporate logos and banner images, you can simply upload and use these new image files. You can customize the default color scheme by changing the color of the different elements and areas of the portals. You can even choose the language in which you want to view the custom changes as you make them.

When you design images to replace the logos and banner, make the images as close to the following pixel size as you can:

Banner	1724 X 133
Desktop Logo	86 X 45
Mobile Logo	80 X 35

Note that ISE resizes the images to fit the portal, but images that are too small may not look right after resizing.

To perform advanced customization, such as changing the page layout or adding video clips or advertisements to your portal pages, you can use your own custom CSS files.

These types of changes within a specific portal are applied globally to all the pages of that portal. Changes to the page layout can be applied either globally or to just one specific page in the portal.

Portal Page Titles, Content, and Labels

You can customize the titles, text boxes, instructions, field and button labels, and other visual elements that the guest views on the end-user web portal pages. While you are customizing the page, you can even edit the page settings dynamically.

These changes are applied only to the specific page that you are customizing.

Basic Customization of Portals

Select a predefined theme that best suits your needs, and use most of its default settings. You can then do some basic customization, such as:

- Modify the Portal Theme Colors, on page 566
- Change the Portal Icons, Images, and Logos, on page 567
- Update the Portal Banner and Footer Elements, on page 567
- Change the Portal Display Language, on page 566
- Change the Titles, Instructions, Buttons, and Label Text, on page 568

- Format and Style Text Box Content, on page 568

Tip You can View Your Customization, on page 572 as you make the updates.

Modify the Portal Theme Colors

You can customize the default color scheme in the default portal themes and change the color of the different elements and areas of the portals. These changes apply to the entire portal that you are customizing.

If you plan to change the portal colors, be aware of the following:

- You cannot use this option to change the color scheme in any of the custom portal themes that you may have imported for use with this portal. You must edit the custom theme CSS file to change its color settings.
- After changing the colors in a portal theme, if you select another portal theme from the **Portal Theme** drop-down menu, the changes are lost in the original portal theme and it reverts to its default colors.
- If you tweak the colors of a portal theme with an already modified color scheme and then reset its colors before saving it, the color scheme reverts to its default colors and any previous modifications are lost.

Step 1 Navigate to these portals:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Configure** > **Guest Portals** > **Edit** > **Portal Page Customization**.
- For Sponsor portals, click the **Menu** icon (☰) and choose **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization**.
- For Device portals, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** > **Portal Page Customization**.

Step 2 Select one of the default themes from the **Portal Theme** drop-down list.

Step 3 Click **Tweaks** to override some of the color settings in the selected default portal theme.

a) Change the color settings for the banner and page backgrounds, text, and labels.
b) If you want to revert to the theme’s default color scheme, click **Reset Colors**.
c) Click **OK** if you want to view the color changes in **Preview**.

Step 4 Click **Save**.

Change the Portal Display Language

You can choose the language in which you want to view the custom changes as you make them. This change applies to the entire portal that you are customizing.

Step 1 Navigate to these portals:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Edit** > **Portal Page Customization** > **Global Customization**.
- For Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization** > **Global Customization**.
- For Device portals, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** > **Portal Page Customization** > **Global Customization**.

Step 2 From the **View In** drop-down list, choose the language in which you want to view the text while customizing the page.

The drop-down list includes all languages in the language file associated with the specific portal.

What to do next

Make sure that you update any changes made in the selected language while customizing the portal page into all the supported language properties files.

Change the Portal Icons, Images, and Logos

If you want to use unique corporate logos, icons, and banner images, you can simply replace the existing images by uploading your custom images. Supported image formats include .gif, .jpg, .jpeg, and .png. These changes apply to the entire portal that you are customizing.

Before you begin

To include images in the footer of the portal, for instance in an advertisement, you should be able to access an external server that has these images.

Step 1 Navigate to these portals:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Edit** > **Portal Page Customization**.
- For Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Configure** > **Sponsor Portals** > **Edit** > **Portal Page Customization**.
- For Device portals, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** > **Portal Page Customization**.

Step 2 Under **Images**, click any of the logos, icons, and image buttons and upload your custom images.

Step 3 Click **Save**.

Update the Portal Banner and Footer Elements

You can customize the information that appears in the banner and footer sections of every page in the portal. These changes apply to the entire portal that you are customizing.

Step 1 Navigate to these portals:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Edit** > **Portal Page Customization**.
- For Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization**.
- For Device portals, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** > **Portal Page Customization**.

Step 2 Change the **Banner title** that appears on every portal page.

Step 3 Include these links for the guests who use your portals:

- **Help**—Online help (provided for only the Sponsor and My Devices portals).
- **Contact**—Technical support (set up the Support Information page to enable this).

Step 4 Add a disclaimer or a copyright notice in the **Footer Elements** to appear on the bottom of every portal page.

Step 5 Click **Save**.

Change the Titles, Instructions, Buttons, and Label Text

You can update all the text that is displayed in the portal. Each UI element on the page that you are customizing has a minimum and maximum range for the number of characters that you can enter. When available in some of the text blocks, you can use a mini-editor to apply visual styling to the text. These changes apply only to the specific portal page you are customizing. These page elements are different for email, SMS, and print notifications.

Step 1 Navigate to these portals:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Configure** > **Guest Portals** > **Edit** > **Portal Page Customization**.
- For Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization**.
- For Device portals, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** > **Portal Page Customization**.

Step 2 Under **Pages**, choose the page that you want to change.

Step 3 Under **Page Customizations**, update any of the displayed UI elements. All pages contain **Browser Page Title**, **Content Title**, **Instructional Text**, **Content**, and two **Optional Content** text blocks. The fields in the **Content** area are specific to each page.

Format and Style Text Box Content

Use the mini-editor that is available in the **Instructional Text**, **Optional Content 1**, and **Optional Content 2** text boxes to do basic formatting of the text. These changes apply only to the specific portal pages that you are customizing.

Use the **Toggle Full Screen** button to increase and decrease the size of the text boxes as you work in them.

Step 1 Navigate to these portals:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Edit** > **Portal Page Customization**.
- For Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization**.
- For Device portals, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** > **Portal Page Customization**.

Step 2 Under **Pages**, choose the page that you want to change.

Step 3 Under **Page Customizations**, in the **Instructional Text** and **Optional Content** text blocks, you can:

- Change the font, size, and color of the text.
- Style the text as bold, italics, or underlined.
- Create bulleted and numbered lists.

Note You can use the **Toggle HTML Source** button to view the HTML tags that were applied to the text that you formatted using the mini-editor. If you edit the text in the **HTML Source** view, click the **Toggle HTML Source** button again, before saving your changes in the **Portal Page Customization** window.

Variables for Portal Pages Customization

The navigation paths for these portal page text boxes are:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Edit** > **Portal Page Customization** > **Pages**.
- For Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization** > **Pages**.
- For Device portals, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** > **Portal Page Customization** > **Pages**.

Use these variables when creating templates for portal content and guest notifications to enable consistency in the information presented to the portal users (guests, sponsors, and employees). Substitute text with the variable names listed here for each of the portals in the **Instructional Text** , **Optional Content 1**, and **Optional Content 2** text boxes.

Table 57: List of Variables for Guest Portals

Display Name	Substitute with Variable Name
Access code Use to provide an access code to guests using either email, text, or print notifications.	ui_access_code

Display Name	Substitute with Variable Name
BYOD IOS SSID Use to specify the network that a device should connect to after on-boarding in a dual SSID flow.	ui_byod_success_ios_ssid
Client Provisioning Agent Type Use to specify the currently configured agent in the client provisioning policy.	ui_client_provision_agent_type
Client Provisioning Agent URL Use to specify the download URL for the posture agent.	ui_client_provision_agent_url
Client Provisioning agent install minutes Use to notify guests the amount of time (set by the remediation timer) in which they must complete the installation instructions on the **Client Provisioning** window. If guests do not complete the installation instructions before the timer expires, they must refresh the browser page and go through the login process again.	ui_client_provision_install_agent_mins
Company	ui_company
Email address	ui_email_address
End date and time	ui_end_date_time
First name	ui_first_name
Last name	ui_last_name
Location name	ui_location_name
Maximum registered devices	ui_max_reg_devices
Maximum simultaneous logins	ui_max_siml_login
Password	ui_password
Person being visited (email)	ui_person_visited
Phone number	ui_phone_number
Reason for visit	ui_reason_visit
SMS Provider	ui_sms_provider
SSID Use to specify the wireless network that a guest can use to connect to the network.	ui_ssid

Display Name	Substitute with Variable Name
Start date and time	ui_start_date_time
Time left	ui_time_left
Username	ui_user_name

Table 58: List of Variables for Sponsor Portals

Display Name	Substitute with Variable Name
Guest - Company	ui_guest_company
Guest - Email address	ui_guest_email_address
Guest - End date and time	ui_guest_end_date_time
Guest - First name	ui_guest_first_name
Guest - Last name	ui_guest_last_name
Guest - Location name	ui_guest_location_name
Guest - Maximum registered devices	ui_guest_max_reg_devices
Guest - Maximum simultaneous logins	ui_guest_max_siml_login
Guest - Password	ui_guest_password
Guest - Person being visited (email)	ui_guest_person_visited
Guest - Phone number	ui_guest_phone_number
Guest - Reason for visit	ui_guest_reason_visit
Guest - SMS Provider	ui_guest_sms_provider
Guest - SSID Use to specify the wireless network that a guest can use to connect to the network.	ui_guest_ssid
Guest - Start date and time	ui_guest_start_date_time
Guest - Time left	ui_guest_time_left
Guest - Username	ui_guest_user_name
Username Use to specify the username of the user logged into the portal.	ui_sponsor_user_name
Use to display "From" in the **Guest Access Information** window.	ui_from_label

Display Name	Substitute with Variable Name
Use to display "First Login" in the **Guest Access Information** window.	ui_first_login_text
Use to display guest account notification message if the access time starts at First Login.	ui_notification_first_login_text
Dynamic variable that represents the account duration in email notifications.	ui_access_duration
Dynamic variable to display an account that is no longer available. For Start-End accounts, the date is the End date and for From-First-Login account, the date is the account creation date plus the purge duration days.	ui_account_purge_date
Use to restrict the sponsor from changing the guest type from From First Login to Start-End or vice versa, if the guest user has logged in at least once in the past. Displayed in the General Sponsor Portal Messages.	ui_guest_type_change_ffl_startend_not_allowed_error ui_guest_type_change_ startend_ffl_not_allowed_error

Table 59: List of Variables for MDM Portals

Display Name	Substitute with Variable Name
MDM - Vendor Name	ui_mdm_vendor_name

Table 60: List of Variables for My Devices Portals

Display Name	Substitute with Variable Name
MyDevices - Login Failure Rate Limit	$user_login_failure_rate_limit$
MyDevices - Max Devices to Register	ui_max_register_devices
MyDevices - User Name Use to specify the username of the user logged into the portal.	$session_username$

View Your Customization

You can view how your customization will display to the portal users (guests, sponsors, or employees).

Step 1 Click **Portal test URL** to view your changes.

Step 2 (Optional) Click **Preview** to dynamically view how your changes appear on various devices:

- Mobile devices: View your changes under **Preview**.
- Desktop devices: Click **Preview** and then click **Desktop Preview**.

If the changes are not displayed, click **Refresh Preview**. The portal displayed is only meant for viewing your changes; you cannot click buttons or enter data.

Note The test portal does not support RADIUS sessions, so you won't see the entire portal flow for all portals. BYOD and Client Provisioning are examples of portals that depend on RADIUS sessions. If you have more than one PSN, Cisco ISE chooses the first active PSN.

Custom Portal Files

The custom portal files menu lets you upload your own files to the ISE server, which you can use to customize all user facing portals (except for the Admin portal). The files you upload are stored on the PSN and synchronized to all PSNs.

Supported file types are:

- .png, .gif, .jpg, .jpeg, ico: For backgrounds, announcements, and advertisements
- .htm, .html, .js, .json, .css, .m4a, .m4v, .mp3, .mp4, .mpeg, .ogg, .wav: For advanced customization (for example,portal builder)

File sizes are limited to:

- 20 MB per file
- 200 MB total of all files

The path column in the list of files displays the URL to the file on this server, which you can use to reference it outside the mini-editor. If the file is an image, when you click the link, it opens a new window that displays the image.

Uploaded files can be referenced by all portal types, except the Admin portal, in the mini-editors under **Portal Page Customization**. To insert the file into a mini-editor, click **Insert File**. Toggle to the HTML Source view, and you will see the inserted file surrounded by the appropriate HTML tags.

You can also view the displayable uploaded files in your browser from outside of ISE, for testing. The URL is https://*ise_ip*:8443/portal/customFiles/*filename*.

Advanced Customization of Portals

If you do not want to use one of the default portal themes provided by Cisco ISE, you can customize the portal to suit your needs. To do so, you must have experience working with CSS and Javascript files and the jQuery Mobile ThemeRoller application.

You cannot alter the default portal themes, but you can:

- Export a Portal’s Default Theme CSS File, on page 578 and use it as a base for creating a custom portal theme.
- Create a Custom Portal Theme CSS File, on page 578 by editing the default portal theme and saving it as a new file.
- Import the Custom Portal Theme CSS File, on page 587 and apply it to the portal.

Depending on your expertise and requirements, you can perform various types of advanced customization. You can use predefined variables to enable consistency in displayed information, add advertisements to your portal pages, use HTML, CSS and Javascript code to customize your content, and modify the portal page layout.

You modify the portal by adding HMTL, CSS, and javascript into the content boxes on the **Portal Page Customization** tab of each portal. This document has examples of customization with HTML and CSS. Examples using javascript are on the ISE community here: http://cs.co/ise-community. More HTML, CSS, and Javascript examples are on the ISE community here: https://community.cisco.com/t5/security-documents/how-to-ise-web-portal-customization-options/ta-p/3619042.

Note TAC does not support Javascript customizations of Cisco ISE portals. If you are having problems with Javascript customizations, please post your questions to the ISE community https://community.cisco.com/t5/identity-services-engine-ise/bd-p/5301j-disc-ise.

Portal Theme and Structure CSS Files

If you have experience with working with CSS files, you can customize the default portal theme CSS files to alter the portal presentation and manipulate elements such as the page layout, colors, and fonts. Customizing the CSS files provides you with flexibility and control in specifying the presentation characteristics, it enables you to share formatting across multiple pages, and it reduces the complexity and repetition in the structural content.

Cisco ISE end-user portals use two distinct types of CSS files: structure.css and *theme*.css. Every portal theme has its own *theme*.css file, but there is only one structure.css file per portal type; for example guest.structure.css for Guest portals, sponsor.structure.css for Sponsor Portals, and mydevices.structure.css for My Devices portals.

The structure.css provides the styling for the page layout and structure. It defines the positioning of elements on each page and also includes jQuery Mobile structure styles. You can only view the structure.css file, but you cannot edit it. However, when you change the page layout within *theme*.css files, import these files into the portal, and apply them, the most recent changes take priority over the structure.css styles.

The *theme*.css files specify styles such as fonts, button colors, and header background. You can export the *theme*.css files, change the theme settings, and import them to use as custom themes for your portal. Any page layout style changes made to the *theme*.css files take priority over the styles that are defined in the structure.css file.

You cannot alter any of the Cisco provided default portal *theme*.css files. However, you can edit the settings in the files and save them to a new custom *theme*.css*theme*.css file. You can make further edits to the custom *theme*.css file, but when you import it back into Cisco ISE, remember to use the same theme name you originally used for it. You cannot use two different theme names for the same *theme*.css file.

For example, you can use a default *green theme.css* file to create a new custom *blue theme.css* file and name it as *Blue*. You can then edit the *blue theme.css* file, but when you import it again, you must reuse the same *Blue* theme name. You cannot call it *Red*, since Cisco ISE checks for the relationship between a filename and its name and the uniqueness of the theme's name. You can however edit the *blue theme.css* file, save it as *red theme.css*, import the new file, and name it as *Red*.

Changing Theme Colors with jQuery Mobile

The color scheme of Cisco's end-user portals is compatible with jQuery ThemeRoller. You can easily edit the colors for an entire portal using the ThemeRoller web site.

ThemeRoller color “swatches” contain a unique color scheme, which defines the colors, textures, and font settings for the primary UI elements, such as toolbars, content blocks, buttons, list items, and font text-shadow. A color scheme also defines the settings for various interaction states of the buttons: normal, hover, and pressed.

Cisco uses three swatches:

- Swatch A—The default swatch.
- Swatch B—Defines emphasized elements, such as an **Accept** button.
- Swatch C—Defines critical elements such as alerts, error messages, invalid input fields, and delete buttons.

You cannot apply additional swatches, unless you add HTML code (to the Optional Content, for example) with elements that use the newly added swatches.

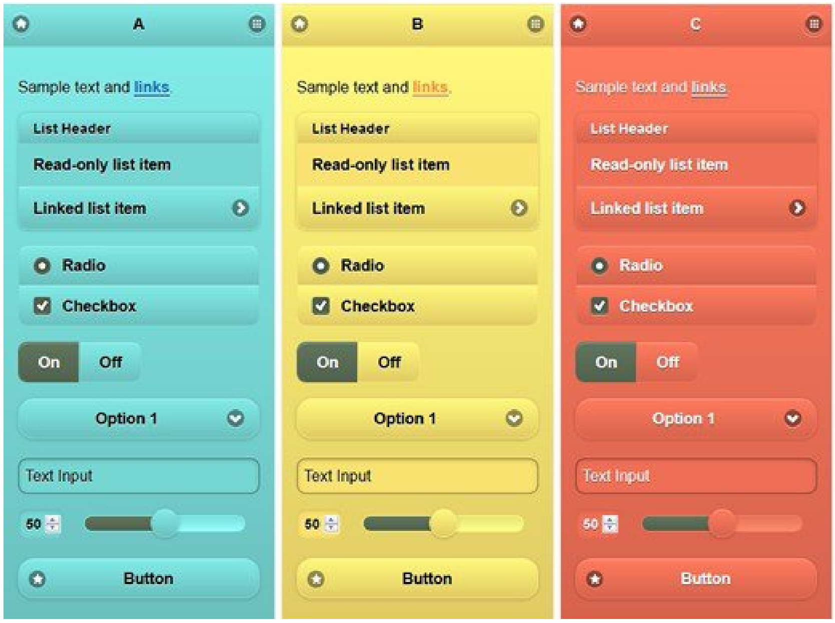
To edit the default Cisco-provided CSS files or create new files based on the CSS classes and structures defined in the default themes, use the required version of jQuery Mobile ThemeRoller (Release 1.3.2).

For additional information on swatches and themes in jQuery Mobile ThemeRoller, see "Theming Overview" in Creating a Custom Theme with ThemeRoller. Use the online help in jQuery Mobile ThemeRoller to learn how to download, import, and share your custom themes.

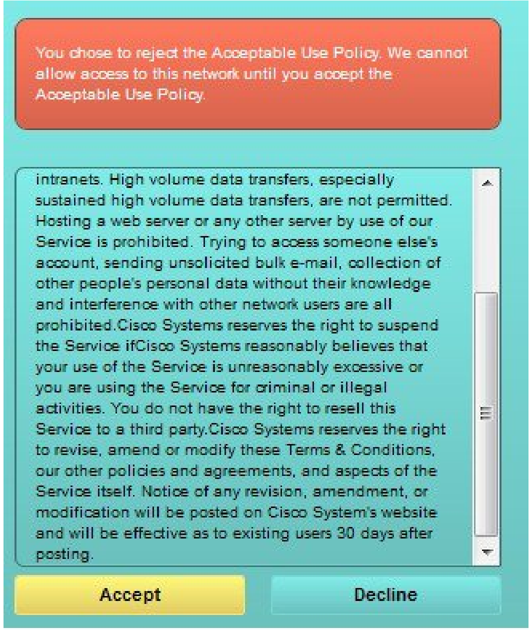
For tutorials on how to use HTML, CSS, and Javascript code to customize the text and content that appears on your portal pages, visit Codecademy.

Example of a Theme That Shows Cisco Swatches

To demonstrate how swatches are used, the default theme for the Guest Portal was edited in ThemeRoller to show the differences in color.


A
Sample text and links.
List Header
Read-only list item
Linked list item
Radio
Checkbox
On
Off
Option 1
Text Input
50
Button
B
Sample text and links.
List Header
Read-only list item
Linked list item
Radio
Checkbox
On
Off
Option 1
Text Input
50
Button
C
Sample text and links.
List Header
Read-only list item
Linked list item
Radio
Checkbox
On
Off
Option 1
Text Input
50
Button

The following screen shows a guest portal logon error (swatch C) along with a button that takes an action from the user (swatch B), and the rest of the screen is Swatch A.



You chose to reject the Acceptable Use Policy. We cannot allow access to this network until you accept the Acceptable Use Policy.

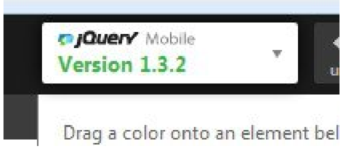
intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.Cisco Systems reserves the right to suspend the Service ifCisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party.Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

Accept
Decline

Change Theme Colors with jQuery Mobile

Before you begin

Make sure you are using version 1.3.2 of jQuery Mobile ThemeRoller. The version you are using is displayed in the top-left corner of the screen, as shown below.



Step 1 Export an existing theme from the portal you wish to change by clicking the **Configuration** tab on the portal.

Step 2 Choose **Advanced Customization** > **Export/Import Themes**.

Step 3 In the **Custom Theming** dialog, export the theme you want to update.

Step 4 Open that theme in a text editor, select all, and copy.

Step 5 Paste that text (CSS) into the jQuery web site's **Import Theme** field.

Step 6 Make your changes in the jQuery Mobil web-based application.

Step 7 Export the updated theme from the jQuery website (the export format is ZIP).

Step 8 Unzip the updated theme, and extract the updated theme in themes folder to your PC. The name of the theme is the one you provided on the jQuery website.

Step 9 Import the extracted CSS theme file into your portal in the portal configuration page's **Custom Theming** dialog.

You can switch back and forth between the old theme and the new theme by clicking the **Portal Theme** drop-down list on the **Portal Configuration** window.

Location Based Customization

When guest accounts are created, you can associate them with a location and specify a Service Set Identifier (SSID) attribute. Both the location and SSID are available as CSS classes that you can use to apply different CSS styles to portal pages, based on the guest's location and SSID.

For example:

- Guest location—When guests with accounts that have *San Jose* or *Boston* as their locations log into a credentialed Guest portal, one of these classes is available on every portal page: **guest-location-san-jose** or **guest-location-boston**.
- Guest SSID—For an SSID named *Coffee Shop Wireless*, the following CSS class is available on every portal page: **guest-ssid-coffee-shop-wireless**. This SSID is the one you specified on the guest account and not the SSID that the guests connected to when they logged in.

Note This information applies only to the credentialed Guest portals after the guests log in.

You can also specify locations when you add devices such as switches and Wireless LAN Controllers (WLCs) to a network. This location is also available as a CSS class that you can use to apply different CSS styles to portal pages depending on the network device's location.

For example, if a WLC is assigned to *Seattle* and guests are redirected to Cisco ISE from the Seattle-WLC, the following CSS class is available on every portal page: **device-location-my-locations-usa-seattle**.

Related Topics

Customize Greetings Based on Guest Location, on page 584

User Device Type Based Customization

Cisco ISE detects the type of client device (guest, sponsor, or employee) to access your company's network or end-user web portals (Guest, Sponsor, and Device). It is detected either as a mobile device (Android, iOS, and so on) or a desktop device (Windows, MacOS, and so on). The device type is available as a CSS class that you can use to apply different CSS styles to portal pages based on the user's device type.

When a user logs in to any of the Cisco ISE end-user web portals, the following class is available on their portal pages: **cisco-ise-mobile** or **cisco-ise-desktop**.

Related Topics

Customize Greetings Based on User Device Type, on page 585

Export a Portal's Default Theme CSS File

You can download a default portal theme provided by Cisco and customize it to suit your needs. You can use it as a base for performing advanced customization.

Step 1 Navigate to these portals:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Edit** > **Portal Page Customization** > **Pages**.
- For Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization** > **Pages**.
- For Device portals, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** > **Portal Page Customization** > **Pages**.

Step 2 From the **Advanced Customization** drop-down list, choose **Export/Import Themes**.

Step 3 In the **Custom Theming** dialog box, use the drop-down list to select the theme that you want to customize.

Step 4 Click **Export Theme CSS** to download a default *theme.css* file to customize.

Step 5 Click **Save** to save the file to your desktop.

Create a Custom Portal Theme CSS File

You can create a custom portal theme by customizing an existing default portal theme and saving the changes in a new portal *theme*.css file. You can modify the default theme settings and the swatches to make global changes to the selected portal.

Before you begin

- Download the *theme*.css file from the portal that you want to customize to your desktop .
- This task requires experience working with HTML, CSS, and Javascript code.
- Use Release 1.3.2 of jQuery Mobile ThemeRoller.

Step 1 Import the downloaded portal *theme*.css file contents into the jQuery Mobile ThemeRoller tool.

Tip You can View Your Customization, on page 588 as you make your changes.

Step 2 (Optional) Embed Links in Portal Content, on page 579

Step 3 (Optional) Insert Variables for Dynamic Text Updates, on page 580

Step 4 (Optional) Use Source Code to Format Text and Include Links, on page 581

Step 5 (Optional) Add an Image as an Advertisement, on page 581

Step 6 (Optional) Customize Greetings Based on Guest Location, on page 584

Step 7 (Optional) Customize Greetings Based on User Device Type, on page 585

Step 8 (Optional) Set Up Carousel Advertising, on page 582

Step 9 (Optional) Modify the Portal Page Layout, on page 586

Step 10 Save the customized file as a new *theme*.css file.

Note You cannot save the edits to the default CSS theme files. You can only create new custom files with any edits you have made.

Step 11 When your new *theme*.css file is ready, you can import it into Cisco ISE.

Embed Links in Portal Content

You can add links to enable guests to access various websites from the portal pages. These changes apply only to the specific portal page that you are customizing.

Use the **Toggle Full Screen** option to increase and decrease the size of the fields as you work in them.

Step 1 Navigate to these portals:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals and Components** > **Guest Portals** > **Edit** > **Portal Page Customization**.
- For Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals and Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization**.
- For Device portals, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** > **Portal Page Customization**.
- For Certificate Provisioning portal, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Certificate Provisioning** > **Edit** > **Portal Page Customization**.

Step 2 Under **Pages**, choose the page that you want to update.

Step 3 Under **Page Customizations**, use the mini-editor provided with the **Optional Content** text blocks to add links to portal pages.

Step 4 Click the **Create Link** button.
Link Properties dialog box appears.

Step 5 Enter the **URL** and the text you want to hyperlink in the **Description** window for the URL.

For the link to work correctly, include the protocol identifier in the URL. For example, use http://www.cisco.com instead of www.cisco.com.

Step 6 Click **Set** and then click **Save**.

You can use the **Toggle HTML Source** option to view the HTML tags that were applied to the text that you formatted using the mini-editor.

Insert Variables for Dynamic Text Updates

You can also create templates for text displayed on the portal by substituting predefined variables ($variable$) that dynamically update the content. This enables consistency in the text and information that you display to guests. These changes apply only to the specific portal pages that you are customizing.

Use the **Toggle Full Screen** option to increase and decrease the size of the fields as you work in them.

Step 1 Navigate to these portals:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals and Components** > **Guest Portals** > **Edit** > **Portal Page Customization**.
- For Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals and Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization**.
- For Device portals, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** > **Portal Page Customization**.

Step 2 Under **Pages**, choose the page you want to update.

Step 3 Under **Page Customizations**, use the mini-editor provided with the **Instructional Text**, **Optional Content 1**, and **Optional Content 2**fields to create text templates for the portal pages.

For example, you can create a single welcome message template for multiple guests, but personalize the message that displays to the guests after they successfully log in and connect to the network.

Step 4 Enter the information in the fields as you normally would.

For example, you could enter a welcome message for your portal:

```
Welcome to our company’s Guest portal,
```

Step 5 At the point where you want to substitute a variable for the text, click **Insert Variable**.
A list of variables appears in the pop-up menu.

Step 6 Select the variable that you want to substitute in your text.

For example, choose **First name** to display each guest’s first name in the welcome message. The variable **$ui_first_name$** is inserted at your cursor position:

```
Welcome to our company’s Guest portal,$ui_first_name$.
```

This is the welcome message that would appear on the portal welcome page for guests whose first name is John: **Welcome to our company’s Guest portal, John**.

Step 7 Continue to use the list of variables as needed until you have completed entering the information in the text boxes.

Step 8 Click **Save**.

You can use the **Toggle HTML Source** option to view the HTML tags that were applied to the text that you formatted using the mini-editor.

Use Source Code to Format Text and Include Links

Besides using the mini-editor's formatting and link icons with plain text, you can also use HTML, CSS, and Javascript code to customize text that displays on the portal pages. These changes apply only to the specific portal pages that you are customizing.

Use the **Toggle Full Screen** option to increase and decrease the size of the text boxes as you work in them.

Before you begin

Ensure that **Enable portal customization with HTML** is enabled by default in **Administration** > **System** > **Admin Access** > **Settings** > **Portal Customization**.

Step 1 Navigate to these portals:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Edit** > **Portal Page Customization**.
- For Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization**.
- For Device portals, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** > **Portal Page Customization**.

Step 2 Under **Pages**, choose the page that you want to update.

Step 3 Under **Page Customizations**, use the mini-editor provided with the **Instructional Text**, **Optional Content 1**, and **Optional Content 2** fields to enter and view source code.

Step 4 Click **Toggle HTML Source**.

Step 5 Enter your source code.

For example, to underline your text, enter:

```
<p style="text-decoration:underline;">Welcome to Cisco!</p>
```

For example, to include a link using HTML code, enter:

```
<a href="http://www.cisco.com">Cisco</a>
```

Important When inserting an external URL in the HTML code, make sure that you enter the absolute (entire) URL path, including "http" or "https".

Step 6 Click **Save**.

Add an Image as an Advertisement

You can include images and advertisements to appear in specific areas of the portal pages.

Use the **Toggle Full Screen** option to increase and decrease the size of the text boxes as you work in them.

Step 1 Navigate to these portals:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Edit** > **Portal Page Customization**.
- For Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization**.
- For Device portals, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** > **Portal Page Customization**.

Step 2 Under **Pages**, choose the page that you want to update.

Step 3 Under **Page Customizations**, use the mini-editor provided with the **Instructional Text**, **Optional Content 1**, and **Optional Content 2** fields to enter and view source code.

Step 4 Click **Toggle HTML Source**.

Step 5 Enter your source code.

For example, to include a product advertisement and its image using HTML code on the Hotspot Guest portal post-access banner, enter this code in the **Optional Content 1** text box on the **Post-Access Banner** page:

```
<p style="text-decoration:underline;">Optimized for 10/40/100 Campus Services!</p>
<img  src="http://www.static-cisco.com/assets/prod/root/catalyst_6800.jpg" width="100%" />
```

Note When inserting an external URL in the HTML code, make sure that you enter the absolute (entire) URL path, including “http” or “https”.

Step 6 Click **Save**.

Set Up Carousel Advertising

Carousel advertising is an advertisement format in which several product images or text descriptions are displayed and rotate in a repeating loop within a banner. Use carousel advertising on your guest portals to promote several related products or a variety of different products offered by your company.

Use the **Toggle Full Screen** option to increase and decrease the size of the text boxes as you work in them.

Before you begin

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Settings** > **Portal Customization** and check **Enable portal customization with HTML and Javascript**.

Step 1 Navigate to these portals:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Edit** > **Portal Page Customization**.
- For Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization**.
- For Device portals, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** > **Portal Page Customization**.

Step 2 Under **Pages**, choose the page that you want to update.

Step 3 Under **Page Customizations**, use the mini-editor provided with the **Instructional Text**, **Optional Content 1**, and **Optional Content 2** fields to enter and view source code.

Step 4 Click **Toggle HTML Source**.

Step 5 Enter your source code.

For example, to implement carousel advertising using product images on the Guest portals, enter the following HTML and Javascript code in the **Optional Content 1** field on the **Post-Access Banner** (for Hotspot portals) or **Post Login Banner** (for credentialed Guest portals) window:

```
<script>
var currentIndex = 0;
setInterval(changeBanner, 5000);

function changeBanner(){
var bannersArray = ["<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq/
n21v1DrawerContainer.img.jpg/1379452035953.jpg' width='100%'/>",
"<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq_0/
n21v1DrawerContainer.img.jpg/1400748629549.jpg' width='100%' />",
"<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq_1/
n21v1DrawerContainer.img.jpg/1376556883237.jpg' width='100%'/>"

];
  var div = document.getElementById("image-ads");
  if(div){
     currentIndex = (currentIndex<2) ? (currentIndex+1) : 0;
      div.innerHTML = bannersArray[currentIndex];
   }
}
</script>
<style>
.grey{
color: black;
background-color: lightgrey;
}
</style>
<div class="grey" id="image-ads">
<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout- overview/gd12v2/gd12v2-left/n21v1_cq/
n21v1DrawerContainer.img.jpg/1379452035953.jpg'/>
</div>
```

For example, to implement carousel advertising using text product descriptions on the Guest portals, enter the following HTML and Javascript code in the **Optional Content 2** field on the **Post-Access Banner** (for Hotspot portals) or **Post Login Banner** (for credentialed Guest portals) window:

```
<script>
var currentIndex = 0;
setInterval(changeBanner, 2000);

function changeBanner(){
var bannersArray = ["Optimize branch services on a single platform while delivering an optimal
application experience across branch and WAN infrastructure", "Transform your Network Edge to
deliver high-performance, highly secure, and reliable services to unite campus, data center,
and branch networks",  "Differentiate your service portfolio and increase revenues by delivering
end-to-end scalable solutions and subscriber-aware services"];

var colorsArray = ["grey", "blue",  "green"];
  var div = document.getElementById("text-ads");
  if(div){
     currentIndex = (currentIndex<2) ? (currentIndex+1) : 0;
      div.innerHTML = bannersArray[currentIndex];
               div.className = colorsArray[currentIndex];
   }
}
</script>
<style>
.grey{
color: black;
background-color: lightgrey;
}
.blue{
color: black;
background-color: lightblue;
}
.green{
color: black;
background-color: lightgreen;
}
</style>
<div class="grey" id="text-ads">
Optimize branch services on a single platform while delivering an optimal application
experience across branch and WAN infrastructure
</div>
```

Note When inserting an external URL in the HTML code, you must enter the absolute (entire) URL path, including “http” or “https”.

Step 6 Click **Save**.

Customize Greetings Based on Guest Location

This example shows how to customize the successful login message that your guests see after they log into a credentialed Guest portal (not Hotspot), based on the locations configured in their guest type.

Use the **Toggle Full Screen** option to increase and decrease the size of the fields as you work in them.

Step 1 Navigate to one of these portals:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Edit** > **Portal Page Customization**.
- For Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization**.

Step 2 Under **Pages**, click **Authentication Success**.

Step 3 Under **Page Customizations**, use the mini-editor provided with the **Optional Content 1** fields to enter and view HTML source code.

Step 4 Click **Toggle HTML Source**.

Step 5 Enter your source code.

For example, to include a location-based greeting, enter this code in **Optional Content 1**:

```
<style>
    .custom-greeting {
        display: none;
    }
    .guest-location-san-jose .custom-san-jose-greeting {
        display: block;
    }
    .guest-location-boston .custom-boston-greeting {
        display: block;
    }
</style>
<div class="custom-greeting custom-san-jose-greeting">
    Welcome to The Golden State!
</div>
<div class="custom-greeting custom-boston-greeting">
    Welcome to The Bay State!
</div>
```

Guests will see a different message after successful logon, depending on their specific location.

Customize Greetings Based on User Device Type

You can customize the greetings that you send to your users (guest, sponsor, or employee) after they log into any of the Cisco ISE end-user web portals (Guest, Sponsor and Device), based on their client device type (mobile or desktop).

Use the **Toggle Full Screen** option to increase and decrease the size of the fields as you work in them.

Step 1 Navigate to these portals:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Edit** > **Portal Page Customization**.
- For Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization**.
- For Device portals, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** > **Portal Page Customization**.

Step 2 Under **Pages**, choose the page that you want to update.

Step 3 Under **Page Customizations**, use the mini-editor provided with the **Optional Content 1** field to enter and view HTML source code.

Step 4 Click **Toggle HTML Source**.

Step 5 Enter your source code.

For example, to include a device type-based greeting on the AUP page, enter this code in the **Optional Content 1** field on the AUP window:

```
<style>
    .custom-greeting {
        display: none;
    }
    .cisco-ise-desktop .custom-desktop-greeting {
        display: block;
    }
    .cisco-ise-mobile .custom-mobile-greeting {
        display: block;
    }
</style>
```

```
<div class="custom-greeting custom-mobile-greeting">
    Try our New Dark French Roast! Perfect on the Go!
</div>
<div class="custom-greeting custom-desktop-greeting">
    We brough back our Triple Chocolate Muffin!
    Grab a seat and dig in!
</div>
```

Users will see a different greeting on the AUP page depending on the type of device they used to gain access to the network or portal.

Modify the Portal Page Layout

You can manipulate the overall layout of the pages; for example, you can add a sidebar to an AUP page that provides additional information or links to information.

Step 1 Add the following CSS code to the bottom of the custom *theme*.css file that you create and plan to apply to your portal. This changes the AUP page layout. The **Optional Content 1** field appears as a side bar in the desktop and mobile device mode.

```
#page-aup .cisco-ise-optional-content-1 {
        margin-bottom: 5px;
}
@media all and ( min-width: 60em ) {
        #page-aup .cisco-ise-optional-content-1 {
                float: left;
                margin-right: 5px;
                width: 150px;
        }
        #page-aup .cisco-ise-main-content {
                float: left;
                width: 800px;
        }
        #page-aup .cisco-ise-main-content h1,
        #page-aup .cisco-ise-main-content p {
                margin-right: auto;
                margin-left: -200px;
        }
}
```

You can then add links using HTML code in the **Optional Content 1** field for the AUP window for that portal.

Step 2 Navigate to these portals:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portal & Components** > **Guest Portals** > **Edit** > **Portal Page Customization**.
- For Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portal & Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization**.
- For Device portals, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** > **Portal Page Customization**.

Step 3 Under **Pages**, choose the page for which you want to include a side bar.

Step 4 Under **Page Customizations**, use the mini-editor provided with the **Optional Content 1** field to enter and view source code.

Step 5 Click **Toggle HTML Source**.

Step 6 Enter your source code.

For example, to include a side bar for the AUP window, enter this code in the **Optional Content 1** field on the AUP window:

```
<ul data-role="listview">
    <li>Rent a Car</li>
    <li>Top 10 Hotels</li>
    <li>Free Massage</li>
    <li>Zumba Classes</li>
</ul>
```

Step 7 Click **Save**.

What to do next

You can customize other pages by entering different text or HTML code in the **Optional Content** fields.

Import the Custom Portal Theme CSS File

You can upload any custom *theme*.css file that you have created and apply it to any of your end-user portals. These changes apply to the entire portal that you are customizing.

Any time you edit a custom *theme*.css file and import it back into Cisco ISE, remember to use the same theme name you originally used for it. You cannot use two different theme names for the same *theme*.css file.

Step 1 Navigate to these portals:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Configure** > **Guest Portals** > **Edit** > **Portal Page Customization**.
- For Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization**.
- For Device portals, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** > **Portal Page Customization**.

Step 2 From the **Advanced Customization** drop-down list, choose **Export/Import Themes**.

Step 3 In the **Custom Theming** dialog box, click **Browse** to find your new *theme*.css file.

Step 4 Enter a **Theme Name** for the new file.

Step 5 Click **Save**.

What to do next

You can apply this custom portal theme to the portal that you want to customize.

1. Choose the updated theme from the **Portal Themes** drop-down list to apply to the entire portal.
2. Click **Save**.

Delete a Custom Portal Theme

You can delete any custom portal theme that you have imported into Cisco ISE, unless it is being used by one of your portals. You cannot delete any of the default themes provided by Cisco ISE.

Before you begin

The portal theme that you want to delete should not be used by any of the portals.

Step 1 Navigate to these portals:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Edit** > **Portal Page Customization**.
- For Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization**.
- For Device portals, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** > **Portal Page Customization**.

Step 2 From the **Advanced Customization** drop-down list, choose **Delete Themes**.

Step 3 Select the portal theme that you want to delete from the **Theme Name** drop-down list.

Step 4 Click **Delete** and then **Save**.

View Your Customization

You can view how your customization will display to the portal users (guests, sponsors, or employees).

Step 1 Click **Portal test URL** to view your changes.

Step 2 (Optional) Click **Preview** to dynamically view how your changes appear on various devices:

- Mobile devices: View your changes under **Preview**.
- Desktop devices: Click **Preview** and then click **Desktop Preview**.

  If the changes are not displayed, click **Refresh Preview**. The portal displayed is only meant for viewing your changes; you cannot click buttons or enter data.

Note The test portal does not support RADIUS sessions, so you won't see the entire portal flow for all portals. BYOD and Client Provisioning are examples of portals that depend on RADIUS sessions. If you have more than one PSN, Cisco ISE chooses the first active PSN.

Portal Language Customization

The Guest, Sponsor, My Devices, and Client Provisioning portals are localized into all supported languages and locales. This includes text, labels, messages, field names, and button labels. If the client browser requests a locale that is not mapped to a template in Cisco ISE, the portals display content using the English template.

Using the Admin portal, you can modify the fields used for the Guest, Sponsor, and My Devices portals for each language individually, and you can add more languages. Currently, you cannot customize these fields for the Client Provisioning portal.

By default, each type of portal supports 15 languages. You select which language a portal uses, and optionally update page content for that language, on the **Portal Page Customization** window. Note, if you change fonts and content on the page for one language, those changes to not carry over into the other languages. The changes you make on the **Portal Page Customization** window are included when you export the Lanaguage File.

The supported languages are:

- Chinese Simplified
- Chinese Traditional
- Czech
- Dutch
- English
- French
- German
- Hungarian
- Italian
- Japanese
- Korean
- Polish
- Portuguese
- Russian
- Spanish

To Edit the Language Used by a Portal

1. Open the portal that you want to edit.
2. On the **Portal Page Customization** tab, select the language that you want to edit in the **view in** drop-down list.
3. Change content, headings, and fonts as desired.
4. Save that portal configuration, and repeat this flow for the other languages that you want to update.

To Edit the Language File

Each **Portal Page Customization** window also provides a Language File. The Language File is a ZIP of attribute files that you can use to customize headings and text that are part of the portal flow, but is not available to customize on the **Portal Page Customization** window.

The Language File also contains the mapping to the particular browser locale setting along with all of the string settings for the entire portal in that language. If you change the browser locale setting for one language, the change is applied to all the other end-user web portals. For example, if you change the French.properties browser locale from fr,fr-fr,fr-ca to fr,fr-fr in the Hotspot Guest portal, the change is applied to the My Devices portal also.

You can export the zipped language file and make updates to it, including adding new languages or deleting existing ones you do not need.

For instructions about how to update the Language File, see:

- Export the Language File, on page 590
- Add or Delete Languages from the Language File, on page 590
- Import the Updated Language File, on page 591

Export the Language File

You can export the language file available for each portal type to edit and customize the existing values specified in it, and add or delete a language.

Note Only some of the dictionary keys in the language properties files support HTML in their values (text).

Step 1 Navigate to these portals:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Edit** .
- For Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Configure** > **Portals & Components** > **Sponsor Portals** > **Edit** .
- For Device portals, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** .

Step 2 Click **Language File** and choose **Export** from the drop-down list.

Step 3 Save the zipped language file to your desktop.

Add or Delete Languages from the Language File

If a language you want to use for your portal type is missing from the language file, you can create a new language properties file and add it to the zipped language file. If there are languages you do not need, you can delete their language properties files.

Before you begin

Export the zipped language file available with each portal type in order to add or delete language properties files.

Step 1 Use any editor that displays UTF-8 (such as Notepad ++) to open the predefined language file for the portal type to which you want to add or delete languages.

If you want to add or delete languages for more than one portal type, use all the appropriate portal properties files.

Step 2 To add a new language, save an existing language properties file as the new language properties file using the same naming convention of the other files in the zipped language file. For example, to create a new Japanese language properties file, save the file as Japanese.properties (*LanguageName*.properties).

Step 3 Associate the new language with its browser locale by specifying the browser local value in the first line of the new language properties file. For example, LocaleKeys= ja,ja-jp (LocaleKeys=*browser locale value*) should be the first line in the Japanese.properties file.

Step 4 Update all the values (text) of the dictionary keys in the new language properties file.

You cannot change the dictionary keys. You can update only their values.

Note Only some of the dictionary keys support HTML in their values (text).

What to do next

1. Zip all the properties files (new and existing) and create a new zipped language file. Do not include any folders or directories.

Note When using a Mac, extracting the ZIP file produces a DS store. When you compress the language file after editing, do not include the DS store in the ZIP. To learn methods of extracting the DS store, see https://superuser.com/questions/198569/compressing-folders-on-a-mac-without-the-ds-store.

2. Use a new name or its original name for the zipped language file.
3. Import the zipped language file into the specific portal you exported it from.

Import the Updated Language File

You can import an edited language file that you have customized by adding or deleting language properties files or by updating text in existing properties files.

Note Ensure that you do not copy and paste customization content from Word files. Alternately, choose **File > Save As** and save the Word file in HTML format. You can then copy and paste customization content from the HTML file.

Step 1 Navigate to these portals:

- For Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Edit** .
- For Device portals, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** .

Step 2 Click **Language File** and choose **Import** from the drop-down list.

Step 3 Browse to find the new zipped language file on your desktop.

Step 4 Import it back for the portal type from where you exported it.

What to do next

To display the changed text or the new language you added, select the specific language from the **View In** drop-down list.

Customization of Guest Notifications, Approvals, and Error Messages

Within in each portal, you can customize how guests receive notifications via email, SMS text messages, and print. Use these notifications to email, text, or print the login credentials:

- When guests use the Self-Registration Guest portal and successfully register themselves.
- When sponsors create guest accounts and want to provide the details to guests. When you create sponsor groups, you can determine whether to authorize sponsors to use SMS notifications. They can always use email and print notifications, if these facilities are available.

You can also customize email notifications to sponsors requesting that they approve a self-registering guest trying to gain access to the network. Additionally, you can customize the default error messages that display to guests and sponsors.

Customize Email Notifications

You can customize the information that is sent via email to guests.

Before you begin

- Configure the SMTP server to enable email notifications. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **SMTP Server**.
- Configure support for email notifications to guests. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Settings** > **Guest Email Settings**. Check **Enable email notifications to guests**.
- Ensure that **Enable portal customization with HTML** is enabled by default in **Administration** > **System** > **Admin Access** > **Settings** > **Portal Customization**.

Step 1 For Self-Registered Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization** > **Notify Guests** > **Email Notification**.

Step 2 You can change the default **Logo (Email)** that was specified under **Global Page Customizations**.

Step 3 Specify the **Subject** and **Email body**. Use predefined variables to specify the guest account information to be included in the email message. Use the mini-editor and HTML tags to customize the text.

Step 4 Under **Settings**, you can:

- **Send username and password separately** in different emails. If you select this option, two separate tabs appear in **Page Customizations** for customizing the **Username Email** and **Password Email** notifications.
- **Send Test Email** to your email address to preview your customization on all devices to ensure that the information appears as it should.

Step 5 Click **Save** and then **Close**.

Customize SMS Text Message Notifications

You can customize the information that is sent via SMS text messages to guests.

Before you begin

- Configure the SMTP server, which is used to send emails to the SMS gateway to deliver the SMS text message. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **SMTP Server**.
- Configure the sponsor groups to support the SMS text notification.
- Set up an account with a third-party SMS gateway. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Systems** > **Settings** > **SMS Gateway**. Cisco ISE sends the text messages as email messages to the gateway, which forwards the messages via the SMS provider to the specified user.
- Ensure that **Enable portal customization with HTML** is enabled by default in **Administration** > **System** > **Admin Access** > **Settings** > **Portal Customization**.

Step 1 For Self-Registered Guest or Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest or Sponsor Portals** > **Edit** > **Portal Page Customization** > **SMS Receipt or SMS Notification**.

Step 2 Use the mini-editor and HTML tags to customize the **Message Text**. Use predefined variables to specify the guest account information to be included in the SMS text message.

Step 3 Under **Settings**, you can:

- **Send username and password separately** in different text messages. If you select this option, two separate tabs appear in **Page Customizations** for customizing the **Username Message** and **Password Message** notifications.
- **Send Test Message** to a cell phone to preview your customization to ensure that the information appears as it should.

Step 4 Click **Save** and then **Close**.

Customize Print Notifications

You can customize the information that is printed for guests.

Note Within each portal, the print notification logo is inherited from the email notification logo setting.

Before you begin

Ensure that **Enable portal customization with HTML** is enabled by default in **Administration** > **System** > **Admin Access** > **Settings** > **Portal Customization**.

Step 1 For Self-Registered Guest and Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest or Sponsor Portals** > **Edit** > **Portal Page Customization** > **Print Receipt or Print Notification**.

Step 2 Specify the **Print Introduction Text**. Use predefined variables to specify the guest account information to be included in the email message. Use the mini-editor and HTML tags to customize the text.

Step 3 Preview your customization in the thumbnail or click **Print Preview**. You cannot view any HTML customization in the thumbnail.
If you select the **Print Preview** option, a window appears from which you can print the account details to ensure that the information appears as it should.

Step 4 Click **Save** and then **Close**.

Customize Approval Request Email Notifications

You can require sponsors to approve self-registering guests before their accounts are created and before they can obtain their login credentials. You can customize the information that is sent via email to sponsors requesting their approval. This notification only displays if you have specified that self-registering guests using the Self-Registered Guest portals require approval before they are granted network access.

Before you begin

- Configure the SMTP server to enable email notifications. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Systems** > **Settings** > **SMTP Server**.
- Configure support for email notifications to guests. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Settings** > **Guest Email Settings**. Check **Enable email notifications to guests**.
- If you want a sponsor to approve self-registered account requests, check **Require self-registered guests to be approved** under **Self-Registration Page Settings** on the the **Portal Behavior and Flow Settings** tab. That enables the **Approval Request Email** tab under **Notifications** in **Portal Page Customization**, where you can customize the email that goes to the sponsor.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Configure** > **Self-Registered Guest Portals** > **Edit** > **Portal Page Customization** > **Approval Request Email**. Here you can:

Step 2 Do the following:

a) Change the default **Logo** that is specified under **Global Page Customizations**.

b) Specify the **Subject** and **Email body**. Use predefined variables to specify the guest account information to be included in the email message. Use the mini-editor and HTML tags to customize the text. For example, to include a link to the Sponsor portal in the request approval email, click **Create a Link** and add the FQDN to the Sponsor portal.

c) Preview your customization on all devices using **Send Test Email** to ensure that it appears as it should.

d) Click **Save** and then **Close**.

Step 3 Customize the content of the approval email sent by the sponsor:

a) Choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals**.

b) Click **Portal Page Customization**.

c) Click the **Email Notification** tab and enter the required details.

Edit Error Messages

You can fully customize the error messages that appear on the Failure pages displayed for guests, sponsors and employees. Failure pages are available with all end-user web portals, except the Blocked List portal.

Step 1 Do one of the following:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Edit** > **Portal Page Customizations** > **Messages** > **Error Messages**.
- For Sponsor Portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Edit** > **Portal Page Customizations** > **Messages** > **Error Messages**.
- For Device portals, click the **Menu** icon (☰) and choose **Adminsitration** > **Device Portals Management** > **(any portals)** > **Edit** > **Portal Page Customizations** > **Messages** > **Error Messages**.

Step 2 From the **View In** drop-down list, choose the language in which you want to view the text while customizing the messages.

The drop-down list includes all the languages in the language file associated with a specific portal. Make sure that you update any changes made while customizing the portal page into the supported languages properties files.

Step 3 Update the error message text. You can search for specific error messages by typing in keywords such as **aup** to find AUP related error messages.

Step 4 Click **Save** and **Close**.

Portal Pages Titles, Content and Labels Character Limits

There is a maximum and minimum range of characters you can enter in the titles, text boxes, instructions, field and button labels, and other visual elements on the **Portal Page Customization** tab.

Character Limits for Portal Pages Titles, Content and Labels

The navigation paths for these portal page UI elements are:

- For Guest portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Edit** > **Portal Page Customization** > **Pages**.
- For Sponsor portals, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization** > **Pages**.
- For Device portals, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** > **Portal Page Customization** > **Pages**.

Use this information when you enter content in the titles, text boxes, instructions, field and button labels, and other visual elements of the portal page the you are customizing. These updates are applied only to the specific page that you are customizing.

Note Whether you enter single-byte or multi-byte characters, you can only enter the maximum number of characters identified for a field. Multi-byte characters do not affect the character limit.

Field Category	Fields	Field Labels: Minimum Characters	Field Labels: Maximum Characters	Field Input Values: Minimum Characters	Field Input Values: Maximum Characters
Common page elements	Banner title				256
	Footer elements			0	2000
	Browser Page Title			0	256
	Instructional Text			0	2000
	Content Title			0	256
	Optional Content 1			0	2000
	Optional Content 2			0	2000
	Button labels	0	64		
	Check box labels	0	64		
	Tab labels	0	64		

Field Category	Fields	Field Labels: Minimum Characters	Field Labels: Maximum Characters	Field Input Values: Minimum Characters	Field Input Values: Maximum Characters
	Link labels	0	256		
AUP	AUP Text			0	50,000
Message text	Message text (displayed on page)			0	2000
	Message text (displayed in pop-up window)			0	256
Field labels	All fields labels	0	256		
Field input (general)	Field input in general (see special cases below)			0	256
Field input (special cases)	Access Code field			1	20
	Registration Code field			1	20
	Username fields			1	64
	Password fields			1	256
	Phone Number field			0	64
	Device ID field			12	17

Portal Customization

You can customize the appearance of the end-user web portals and the guest experience. If you have experience with the cascading style sheet (CSS) language and with Javascript, you can use the jQuery Mobile ThemeRoller application to customize portal themes by changing the portal page layout.

You can view all the fields by exporting the CSS theme or language properties from the required portal page. See Export a Portal’s Default Theme CSS File for more information.

CSS Classes and Descriptions for End-User Portals Page Layout

Use these CSS classes to define and modify the page layout of the Cisco ISE end-user web portals.

CSS Class Name	Description
cisco-ise-banner	Includes logos, banner image, and banner text. On the Sponsor and My Devices portals, this class also contains buttons that can activate a context menu. For example, the menu can bring up a pop-up window with options to **Log Out**, **Change Password**, and so on.
cisco-ise-body	Contains all page elements that are not part of the banner.
cisco-ise-optional-content-1	Empty by default. You can add text, links, and HTML and Javascript code.
cisco-ise-main-content	Includes the main contents of the portal page, such as instructional text, action buttons, and the cisco-ise-footer container.
cisco-ise-optional-content-2	Empty by default. You can add text, links, and HTML and Javascript code.
cisco-ise-footer	Part of the footer, it is a placeholder for links such as **Contact Support** and online **Help**.
cisco-ise-footer-text	Empty by default. It is a placeholder for anything that you want to display at the bottom of the portal page, such as a copyright notice or a disclaimer.

HTML Support for a Portal Language File

The zipped language file for each portal includes the default language properties files for that portal. Each properties file includes dictionary keys that define the content that displays on the portal.

You can customize the text that displays on a portal, including the content in the **Instructional Text**, **Content**, **Optional Content 1**, and **Optional Content 2** fields. Some of these fields have default content and some are empty.

Only some of these dictionary keys associated with these fields support HTML in their values (text).

HTML Support for the Blocked List Portal Language File

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Blocked List Portal** > **Edit** > **Portal Page Customization** > **Pages**. You can use the **View HTML Source** icon in the mini-editor and add HTML code in your content.

These dictionary keys in the portal's language properties files support HTML in their text.

Note This is not a complete list of the dictionary keys in the files.

- key.blacklist.ui_reject_message

HTML Support for Bring Your Own Device Portals Language Files

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **BYOD Portals** > **Edit** > **Portal Page Customization** > **Pages**. You can use the **View HTML Source** icon in the mini-editor and add HTML code in your content.

These dictionary keys in the portal's language properties files support HTML in their text.

Note This is not a complete list of the dictionary keys in the files.

- key.guest.ui_contact_instruction_message
- key.guest.ui_byod_welcome_optional_content_1
- key.guest.ui_byod_welcome_optional_content_2
- key.guest.ui_byod_reg_limit_message
- key.guest.ui_byod_reg_content_message
- key.guest.ui_byod_success_manual_reconnect_message
- key.guest.ui_byod_install_winmac_instruction_message
- key.guest.ui_byod_install_optional_content_1
- key.guest.ui_byod_reg_optional_content_2
- key.guest.ui_byod_install_optional_content_2
- key.guest.ui_byod_reg_optional_content_1
- key.guest.ui_byod_reg_instruction_message
- key.guest.ui_byod_welcome_aup_text
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_byod_install_ios_instruction_message

- key.guest.ui_byod_welcome_instruction_message
- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_byod_welcome_renew_cert_message
- key.guest.ui_byod_install_android_instruction_message
- key.guest.ui_byod_install_instruction_message
- key.guest.ui_byod_welcome_config_device_message
- key.guest.ui_byod_success_message
- key.guest.ui_byod_success_unsupported_device_message
- key.guest.ui_byod_success_optional_content_1
- key.guest.ui_byod_success_optional_content_2
- key.guest.ui_error_instruction_message

HTML Support for Certificate Provisioning Portal Language Files

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Certificate Provisioning Portal** > **Edit** > **Portal Page Customization** > **Pages**. You can use the **View HTML Source** icon in the mini-editor and add HTML code in your content.

These dictionary keys in the portal's language properties files support HTML in their text.

Note This is not a complete list of the dictionary keys in the files.

- key.manualcertprov.ui_login_instruction_message
- key.manualcertprov.ui_aup_instruction_message
- key.manualcertprov.ui_changepwd_instruction_message
- key.manualcertprov.ui_post_access_instruction_message
- key.manualcertprov.ui_status_csv_invalid_instruction_message
- key.manualcertprov.ui_login_optional_content_1
- key.manualcertprov.ui_login_optional_content_2
- key.manualcertprov.ui_aup_optional_content_1
- key.manualcertprov.ui_aup_optional_content_2
- key.manualcertprov.ui_changepwd_optional_content_1
- key.manualcertprov.ui_changepwd_optional_content_2
- key.manualcertprov.ui_post_access_optional_content_1

- key.manualcertprov.ui_post_access_optional_content_2
- key.manualcertprov.ui_landing_instruction_message
- key.manualcertprov.ui_status_page_single_generated_content
- key.manualcertprov.ui_status_generated_content

HTML Support for Client Provisioning Portal Language Files

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Client Provisioning Portals** > **Edit** > **Portal Page Customization** > **Pages**. You can use the **View HTML Source** icon in the mini-editor and add HTML code in your content.

These dictionary keys in the portal's language properties files support HTML in their text.

Note This is not a complete list of the dictionary keys in the files.

- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_client_provision_posture_agent_check_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_contact_optional_content_1
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_client_provision_optional_content_1
- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1

- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_client_provision_posture_agent_scan_message

HTML Support for Credential Guest Portals Language Files

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Edit** > **Portal Page Customization** > **Pages**. You can use the **View HTML Source** icon in the mini-editor and add HTML code in your content.

These dictionary keys in the portal's language properties files support HTML in their text.

Note This is not a complete list of the dictionary keys in the files.

- key.guest.ui_contact_instruction_message
- key.guest.ui_login_optional_content_1
- key.guest.ui_login_optional_content_2
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_device_reg_optional_content_2
- key.guest.ui_device_reg_optional_content_1
- key.guest.ui_byod_success_manual_reconnect_message
- key.guest.ui_byod_reg_optional_content_2
- key.guest.ui_byod_reg_optional_content_1
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message
- key.guest.ui_max_devices_instruction_message
- key.guest.ui_max_devices_optional_content_1
- key.guest.ui_self_reg_results_instruction_message
- key.guest.notification_credentials_email_body
- key.guest.ui_max_devices_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1

- key.guest.ui_byod_install_ios_instruction_message
- key.guest.ui_changepwd_instruction_message
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_aup_instruction_message
- key.guest.ui_changepwd_optional_content_2
- key.guest.ui_changepwd_optional_content_1
- key.guest.ui_self_reg_results_optional_content_2
- key.guest.ui_self_reg_results_optional_content_1
- key.guest.ui_device_reg_instruction_message
- key.guest.ui_byod_welcome_renew_cert_message
- key.guest.ui_vlan_execute_message
- key.guest.ui_byod_install_android_instruction_message
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_byod_install_instruction_message
- key.guest.ui_device_reg_max_reached_message
- key.guest.ui_byod_success_message
- key.guest.ui_byod_success_unsupported_device_message
- key.guest.ui_byod_success_optional_content_1
- key.guest.ui_byod_success_optional_content_2
- key.guest.ui_aup_employee_text
- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_success_message
- key.guest.ui_byod_welcome_optional_content_1
- key.guest.ui_byod_welcome_optional_content_2
- key.guest.ui_self_reg_optional_content_2
- key.guest.ui_self_reg_optional_content_1
- key.guest.ui_byod_reg_limit_message
- key.guest.notification_credentials_print_body
- key.guest.ui_byod_reg_content_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_post_access_message
- key.guest.ui_vlan_instruction_message

- key.guest.ui_byod_install_winmac_instruction_message
- key.guest.ui_aup_guest_text
- key.guest.ui_byod_install_optional_content_1
- key.guest.ui_byod_install_optional_content_2
- key.guest.ui_byod_reg_instruction_message
- key.guest.ui_aup_optional_content_1
- key.guest.ui_aup_optional_content_2
- key.guest.ui_self_reg_aup_text
- key.guest.ui_login_instruction_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_self_reg_results_aup_text
- key.guest.ui_device_reg_register_message
- key.guest.ui_byod_welcome_instruction_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_self_reg_instruction_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_post_access_instruction_message
- key.guest.ui_post_access_optional_content_2
- key.guest.ui_post_access_optional_content_1
- key.guest.ui_byod_welcome_config_device_message
- key.guest.ui_client_provision_posture_agent_scan_message

HTML Support for Hotspot Guest Portals Language Files

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Edit** > **Portal Page Customization** > **Pages**. You can use the **View HTML Source** icon in the mini-editor and add HTML code in your content.

These dictionary keys in the portal's language properties files support HTML in their text.

Note This is not a complete list of the dictionary keys in the files.

- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_post_access_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_success_instruction_message
- key.guest.ui_aup_optional_content_1
- key.guest.ui_aup_optional_content_2
- key.guest.ui_vlan_unsupported_error_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_aup_instruction_message
- key.guest.ui_aup_hotspot_text
- key.guest.ui_vlan_execute_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_post_access_instruction_message
- key.guest.ui_post_access_optional_content_2
- key.guest.ui_post_access_optional_content_1

HTML Support for Mobile Device Management Portals Language Files

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **MDM Portals** > **Edit** > **Portal Page Customization** > **Pages**. You can use the **View HTML Source** icon in the mini-editor and add HTML code in your content.

These dictionary keys in the portal's language properties files support HTML in their text.

- key.mdm.ui_contact_instruction_message
- key.mdm.ui_mdm_enrollment_after_message
- key.mdm.ui_error_optional_content_2
- key.mdm.ui_error_optional_content_1
- key.mdm.ui_mdm_enroll_optional_content_1

- key.mdm.ui_mdm_enroll_optional_content_1
- key.mdm.ui_mdm_enroll_optional_content_2
- key.mdm.ui_mdm_enroll_instruction_message
- key.mdm.ui_error_instruction_message
- key.mdm.ui_mdm_enrollment_link_message
- key.mdm.ui_mdm_not_reachable_message
- key.mdm.ui_contact_optional_content_2
- key.mdm.ui_mdm_continue_message
- key.mdm.ui_contact_optional_content_1

HTML Support for My Devices Portals Language Files

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **My Devices Portals** > **Edit** > **Portal Page Customization** > **Pages**. You can use the **View HTML Source** icon in the mini-editor and add HTML code in your content.

These dictionary keys in the portal's language properties files support HTML in their text.

Note This is not a complete list of the dictionary keys in the files.

- key.mydevices.ui_add_optional_content_1
- key.mydevices.ui_add_optional_content_2
- key.mydevices.ui_post_access_instruction_message
- key.mydevices.ui_edit_instruction_message
- key.mydevices.ui_contact_optional_content_2
- key.mydevices.ui_contact_optional_content_1
- key.mydevices.ui_changepwd_optional_content_1
- key.mydevices.ui_changepwd_optional_content_2
- key.mydevices.ui_post_access_message
- key.mydevices.ui_home_instruction_message
- key.mydevices.ui_edit_optional_content_1
- key.mydevices.ui_edit_optional_content_2
- key.mydevices.ui_add_instruction_message
- key.mydevices.ui_post_access_optional_content_2
- key.mydevices.ui_post_access_optional_content_1

- key.mydevices.ui_error_instruction_message
- key.mydevices.ui_actions_instruction_message
- key.mydevices.ui_home_optional_content_2
- key.mydevices.ui_aup_optional_content_1
- key.mydevices.ui_aup_optional_content_2
- key.mydevices.ui_home_optional_content_1
- key.mydevices.ui_changepwd_instruction_message
- key.mydevices.ui_contact_instruction_message
- key.mydevices.ui_aup_employee_text
- key.mydevices.ui_login_optional_content_2
- key.mydevices.ui_login_optional_content_1
- key.mydevices.ui_login_instruction_message
- key.mydevices.ui_error_optional_content_1
- key.mydevices.ui_error_optional_content_2
- key.mydevices.ui_aup_instruction_message

HTML Support for Sponsor Portals Language Files

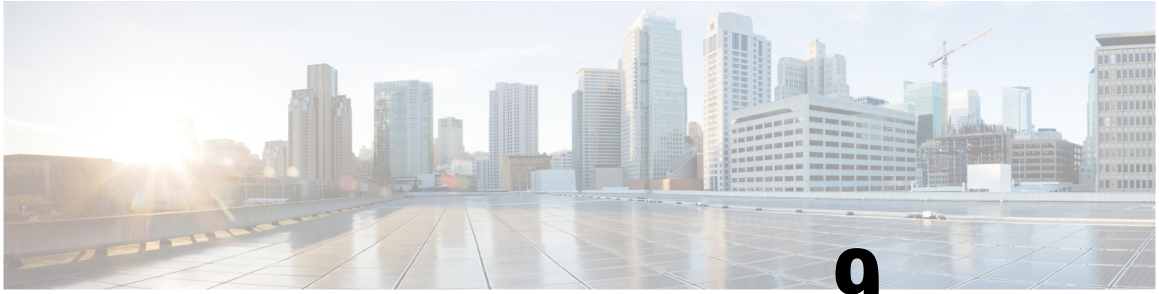
To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization** > **Pages**. You can use the **View HTML Source** icon in the mini-editor and add HTML code in your content.

These dictionary keys in the portal's language properties files support HTML in their text.

Note This is not a complete list of the dictionary keys in the files.

- key.sponsor.ui_aup_instruction_message
- key.sponsor.ui_create_random_instruction_message
- key.sponsor.ui_home_instruction_message
- key.sponsor.ui_post_access_instruction_message
- key.sponsor.notification_credentials_print_body
- key.sponsor.ui_aup_sponsor_text
- key.sponsor.ui_create_accounts_access_info_instruction_message
- key.sponsor.ui_login_instruction_message
- key.sponsor.notification_credentials_email_body

- key.sponsor.ui_create_known_instruction_message
- key.sponsor.ui_create_import_instruction_message
- key.sponsor.ui_suspend_account_instruction_message
- key.sponsor.ui_post_access_message
- key.sponsor.ui_login_optional_content_2
- key.sponsor.ui_login_optional_content_1
- key.sponsor.notification_credentials_email_password_body
- key.sponsor.ui_contact_optional_content_2
- key.sponsor.ui_contact_optional_content_1
- key.sponsor.ui_login_aup_text
- key.sponsor.ui_changepwd_instruction_message
- key.sponsor.ui_create_accounts_guest_type_instruction_message
- key.sponsor.ui_changepwd_optional_content_1
- key.sponsor.ui_changepwd_optional_content_2
- key.sponsor.notification_credentials_email_username_body
- key.sponsor.ui_aup_optional_content_1
- key.sponsor.ui_aup_optional_content_2
- key.sponsor.ui_post_access_optional_content_1
- key.sponsor.ui_post_access_optional_content_2
- key.sponsor.ui_contact_instruction_message



CHAPTER 9

Asset Visibility

- Administrative Access to Cisco ISE Using an External Identity Store, on page 610
- External Identity Sources, on page 615
- Cisco ISE Users, on page 624
- Internal and External Identity Sources, on page 637
- Certificate Authentication Profiles, on page 640
- Active Directory as an External Identity Source, on page 641
- Active Directory Requirements to Support Easy Connect and Passive Identity services, on page 672
- Easy Connect, on page 679
- PassiveID Work Center , on page 683
- LDAP, on page 730
- ODBC Identity Source, on page 744
- RADIUS Token Identity Sources, on page 752
- RSA Identity Sources, on page 758
- SAMLv2 Identity Provider as an External Identity Source, on page 764
- Identity Source Sequences, on page 772
- Identity Source Details in Reports, on page 773
- Profiled Endpoints on the Network, on page 773
- Profiler Condition Settings, on page 774
- Profiled Endpoints on the Network, on page 774
- Profiler Condition Settings, on page 775
- Cisco ISE Profiling Service, on page 775
- Profiler Forwarder Persistence Queue, on page 778
- Configure Profiling Service in Cisco ISE Nodes, on page 778
- Network Probes Used by Profiling Service, on page 778
- Configure Probes for Each Cisco ISE Node, on page 788
- Setup CoA, SNMP RO Community, and Endpoint Attribute Filter, on page 789
- Attribute Filters for ISE Database Persistence and Performance, on page 793
- Attributes Collection from Cisco IOS Sensor-Embedded Switches, on page 795
- Support for Cisco IND Controllers by ISE Profiler, on page 797
- Cisco ISE Support for MUD, on page 799
- Profiler Conditions, on page 800
- Profiling Network Scan Actions, on page 801
- Create a Profiler Condition, on page 815

- Endpoint Profiling Policy Rules, on page 815
- Endpoint Profiling Policies Settings, on page 816
- Create Endpoint Profiling Policies, on page 819
- Predefined Endpoint Profiling Policies, on page 822
- Wi-Fi Device Analytics Data from Cisco Catalyst 9800 Wireless LAN Controller, on page 825
- Endpoint Profiling Policies Grouped into Logical Profiles, on page 826
- Profiling Exception Actions, on page 827
- Create Endpoints with Static Assignments of Policies and Identity Groups, on page 828
- Identified Endpoints, on page 833
- Create Endpoint Identity Groups, on page 835
- Anycast and Profiler Services, on page 837
- Profiler Feed Service, on page 838
- Profiler Reports, on page 841
- Detect Anomalous Behavior of Endpoints , on page 842
- Agent Download Issues on Client Machine, on page 844
- Endpoints, on page 844
- Agent Download Issues on Client Machine, on page 854
- Endpoints, on page 854
- IF-MIB, on page 864
- SNMPv2-MIB, on page 864
- IP-MIB, on page 864
- CISCO-CDP-MIB, on page 865
- CISCO-VTP-MIB, on page 866
- CISCO-STACK-MIB, on page 866
- BRIDGE-MIB, on page 866
- OLD-CISCO-INTERFACE-MIB, on page 866
- CISCO-LWAPP-AP-MIB, on page 867
- CISCO-LWAPP-DOT11-CLIENT-MIB, on page 868
- CISCO-AUTH-FRAMEWORK-MIB, on page 869
- EEE8021-PAE-MIB: RFC IEEE 802.1X, on page 869
- HOST-RESOURCES-MIB, on page 869
- LLDP-MIB, on page 870
- Session Trace for an Endpoint, on page 870
- Global Search for Endpoints, on page 872
- Session Trace for an Endpoint, on page 873
- Global Search for Endpoints, on page 875

Administrative Access to Cisco ISE Using an External Identity Store

In Cisco ISE, you can authenticate administrators via an external identity store such as Active Directory, LDAP, or RSA SecureID. There are two models you can use to provide authentication via an external identity store:

- External Authentication and Authorization: There are no credentials that are specified in the local Cisco ISE database for the administrator, and authorization is based on external identity store group membership only. This model is used for Active Directory and LDAP authentication.
- External Authentication and Internal Authorization: The administrator's authentication credentials come from the external identity source, and authorization and administrator role assignment take place using the local Cisco ISE database. This model is used for RSA SecurID authentication. This method requires you to configure the same username in both the external identity store and the local Cisco ISE database.

During the authentication process, Cisco ISE is designed to "fall back" and attempt to perform authentication from the internal identity database, if communication with the external identity store has not been established or if it fails. In addition, whenever an administrator for whom you have set up external authentication launches a browser and initiates a login session, the administrator still has the option to request authentication via the Cisco ISE local database by choosing **Internal** from the **Identity Store** drop-down list in the login dialog box.

Administrators who belong to a Super Admin group, and are configured to authenticate and authorize using an external identity store, can also authenticate with the external identity store for Command Line Interface (CLI) access.

Note You can configure this method of providing external administrator authentication only via the Admin portal. Cisco ISE CLI does not feature these functions.

If your network does not already have one or more existing external identity stores, ensure that you have installed the necessary external identity stores and configured Cisco ISE to access those identity stores.

External Authentication and Authorization

By default, Cisco ISE provides internal administrator authentication. To set up external authentication, you must create a password policy for the external administrator accounts that you define in the external identity stores. You can then apply this policy to the external administrator groups that eventually become a part of the external administrator RBAC policy.

To configure external authentication, you must:

- Configure password-based authentication using an external identity store.
- Create an external administrator group.
- Configure menu access and data access permissions for the external administrator group.
- Create an RBAC policy for external administrator authentication.

In addition to providing authentication via an external identity store, your network may also require you to use a Common Access Card (CAC) authentication device.

Configure a Password-Based Authentication Using an External Identity Store

You must first configure password-based authentication for administrators who authenticate using an external identity store such as Active Directory or LDAP.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Authentication**.

Step 2 On the **Authentication Method** tab, click **Password Based** and choose one of the external identity sources you have already configured. For example, the Active Directory instance that you have created.

Step 3 Configure any other specific password policy settings that you want for administrators who authenticate using an external identity store.

Step 4 Click **Save**.

Create an External Administrator Group

You will need to create an external Active Directory or LDAP administrator group. This ensures that Cisco ISE uses the username that is defined in the external Active Directory or LDAP identity store to validate the administrator username and password that you entered upon login.

Cisco ISE imports the Active Directory or LDAP group information from the external resource and stores it as a dictionary attribute. You can then specify that attribute as one of the policy elements while configuring the RBAC policy for this external administrator authentication method.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Groups**.

The **External Groups Mapped** column displays the number of external groups that are mapped to internal RBAC roles. You can click the number corresponding to a admin role to view the external groups (for example, if you click 2 displayed against Super Admin, the names of two external groups are displayed).

Step 2 Click **Add**.

Step 3 Enter a name and optional description.

Step 4 Click **External**.

If you have connected and joined to an Active Directory domain, your Active Directory instance name appears in the **Name** field.

Step 5 From the **External Groups** drop-down list box, choose the Active Directory group that you want to map for this external administrator group.

Click the "+" sign to map additional Active Directory groups to this external administrator group.

Step 6 Click **Save**.

Create an Internal Read-Only Admin

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Users** .

Step 2 Click **Add** and select **Create An Admin User**.

Step 3 Check the **Read Only** check box to create a Read-Only administrator.

Map External Groups to the Read-Only Admin Group

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** to configure the external authentication source.

Step 2 Click the required external identity source, such as Active Directory or LDAP, and then retrieve the groups from the selected identity source.

Step 3 Choose **Administration** > **System** > **Admin Access** > **Authentication** to map the authentication method for the admin access with the identity source.

Step 4 Choose **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Groups** and select **Read Only Admin** group.

Step 5 Check the **External** check box and select the required external groups for whom you intend to provide read-only privileges.

Step 6 Click **Save**.

An external group that is mapped to a Read-Only Admin group cannot be assigned to any other admin group.

Configure Menu Access and Data Access Permissions for External Administrator Group

You must configure menu access and data access permissions that can be assigned to the external administrator group.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Permissions**.

Step 2 Click one of the following:

- **Menu Access**: All administrators who belong to the external administrator group can be granted permission at the menu or submenu level. The menu access permission determines the menus or submenus that they can access.
- **Data Access**: All administrators who belong to the external administrator group can be granted permission at the data level. The data access permission determines the data that they can access.

Step 3 Specify menu access or data access permissions for the external administrator group.

Step 4 Click **Save**.

Create an RBAC Policy for External Administrator Authentication

You must configure a new RBAC policy to authenticate an administrator using an external identity store and to specify custom menu and data access permissions. This policy must have the external administrator group for authentication and the Cisco ISE menu and data access permissions to manage the external authentication and authorization.

Note You cannot modify an existing (system-preset) RBAC policy to specify these new external attributes. If you have an existing policy that you would like to use as a template, you must duplicate that policy, rename it, and then assign the new attributes.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Authorization** > **RBAC Policy**.

Step 2 Specify the rule name, external administrator group, and permissions.

Remember that the appropriate external administrator group must be assigned to the correct administrator user IDs. Ensure that the administrator is associated with the correct external administrator group.

Step 3 Click **Save**.

If you log in as an administrator, and the Cisco ISE RBAC policy is not able to authenticate your administrator identity, Cisco ISE displays an "unauthenticated" message, and you cannot access the Admin portal.

Configure Admin Access Using an External Identity Store for Authentication with Internal Authorization

This method requires you to configure the same username in both the external identity store and the local Cisco ISE database. When you configure Cisco ISE to provide administrator authentication using an external RSA SecurID identity store, administrator credential authentication is performed by the RSA identity store. However, authorization (policy application) is still done according to the Cisco ISE internal database. In addition, there are two important factors to remember that are different from external authentication and authorization:

- You do not need to specify any particular external administrator groups for the administrator.
- You must configure the same username in both the external identity store and the local Cisco ISE database.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Users**.

Step 2 Ensure that the administrator username in the external RSA identity store is also present in Cisco ISE. Ensure that you click the **External** option under Password.

Note You do not need to specify a password for this external administrator user ID, nor are you required to apply any specially configured external administrator group to the associated RBAC policy.

Step 3 Click **Save**.

External Authentication Process Flow

When the administrator logs in, the login session passes through the following steps in the process:

1. The administrator sends an RSA SecurID challenge.
2. RSA SecurID returns a challenge response.
3. The administrator enters a user name and the RSA SecurID challenge response in the Cisco ISE login dialog, as if entering the user ID and password.

4. The administrator ensures that the specified Identity Store is the external RSA SecurID resource.
5. The administrator clicks **Login**.

Upon logging in, the administrator sees only the menu and data access items that are specified in the RBAC policy.

External Identity Sources

These windows enable you to configure and manage external identity sources that contain user data that Cisco ISE uses for authentication and authorization.

LDAP Identity Source Settings

The following table describes the fields on the LDAP Identity Sources window, which you can use to create an LDAP instance and connect to it. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **LDAP**.

LDAP General Settings

The following table describes the fields in the **General** tab.

Table 61: LDAP General Settings

Field Name	Usage Guidelines
Name	Enter a name for the LDAP instance. This value is used in searches to obtain the subject DN and attributes. The value is of type string and the maximum length is 64 characters.
Description	Enter a description for the LDAP instance. This value is of type string, and has a maximum length of 1024 characters.
Schema	You can choose any one of the following built-in schema types or create a custom schema: • Active Directory • Sun Directory Server • Novell eDirectory You can click the arrow next to Schema to view the schema details. If you edit the attributes of the predefined schema, Cisco ISE automatically creates a Custom schema.
Note	The following fields can be edited only when you choose the Custom schema.
Subject Objectclass	Enter a value to be used in searches to obtain the subject DN and attributes. The value is of type string and the maximum length is 256 characters.

Field Name	Usage Guidelines
Subject Name Attribute	Enter the name of the attribute containing the username in the request. The value is of type string and the maximum length is 256 characters. **Note** The subject name attributes that are configured should be an indexed one in the external ID store.
Group Name Attribute	• CN: To retrieve the LDAP Identity Store Groups based on Common Name. • DN: To retrieve the LDAP Identity Store Groups based on Distinguished Name.
Certificate Attribute	Enter the attribute that contains the certificate definitions. For certificate-based authentication, these definitions are used to validate certificates that are presented by clients.
Group Objectclass	Enter a value to be used in searches to specify the objects that are recognized as groups. The value is of type string and the maximum length is 256 characters.
Group Map Attribute	Specifies the attribute that contains the mapping information. This attribute can be a user or group attribute based on the reference direction that is chosen.
Subject Objects Contain Reference To Groups	Click this option if the subject objects contain an attribute that specifies the group to which they belong.
Group Objects Contain Reference To Subjects	Click this option if the group objects contain an attribute that specifies the subject. This value is the default value.
Subjects in Groups Are Stored in Member Attribute As	(Only available when you enable the **Group Objects Contain Reference To Subjects** option) Specifies how members are sourced in the group member attribute and defaults to the DN.
User Info Attributes	By default, predefined attributes are used to collect user information (such as, first name, last name, email, telephone, locality, and so on) for the following built-in schema types: • Active Directory • Sun Directory Server • Novell eDirectory If you edit the attributes of the predefined schema, Cisco ISE automatically creates a Custom schema. You can also select the Custom option from the Schema drop-down list to edit the user information attributes based on your requirements.

Note The subject name attributes that are configured should be an indexed one in the external ID store.

LDAP Connection Settings

The following table describes the fields in the **Connection Settings** tab.

Table 62: LDAP Connection Settings

Field Name	Usage Guidelines
Enable Secondary Server	Check this option to enable the secondary LDAP server to be used as a backup if the primary LDAP server fails. If you check this check box, you must enter configuration parameters for the secondary LDAP server.
Primary and Secondary Servers	
Hostname/IP	Enter the IP address or DNS name of the machine that is running the LDAP software. The hostname can contain from 1 to 256 characters or a valid IP address expressed as a string. The only valid characters for hostnames are alphanumeric characters (a to z, A to Z, 0 to 9), the dot (.), and the hyphen (-).
Port	Enter the TCP/IP port number on which the LDAP server is listening. Valid values are from 1 to 65,535. The default is 389, as stated in the LDAP specification. If you do not know the port number, you can find this information from the LDAP server administrator.
Specify server for each ISE node	Check this check box to configure primary and secondary LDAP server hostnames/IP and their ports for each PSN. When this option is enabled, a table listing all the nodes in the deployment is displayed. You need to select the node and configure the primary and secondary LDAP server hostname/IP and their ports for the selected node.
Access	**Anonymous Access**: Click to ensure that searches on the LDAP directory occur anonymously. The server does not distinguish who the client is and will allow the client read access to any data that is configured as accessible to any unauthenticated client. In the absence of a specific policy permitting authentication information to be sent to a server, a client should use an anonymous connection. **Authenticated Access**: Click to ensure that searches on the LDAP directory occur with administrative credentials. If so, enter information for the Admin DN and Password fields.
Admin DN	Enter the DN of the administrator. The Admin DN is the LDAP account that has permission to search all required users under the User Directory Subtree and to search groups. If the administrator specified does not have permission to see the group name attribute in searches, group mapping fails for users who are authenticated by that LDAP server.
Password	Enter the LDAP administrator account password.
Secure Authentication	Click to use SSL to encrypt communication between Cisco ISE and the primary LDAP server. Verify that the Port field contains the port number used for SSL on the LDAP server. If you enable this option, you must choose a root CA.
LDAP Server Root CA	Choose a trusted root certificate authority from the drop-down list to enable secure authentication with a certificate.

Field Name	Usage Guidelines
Server Timeout	Enter the number of seconds that Cisco ISE waits for a response from the primary LDAP server before determining that the connection or authentication with that server has failed. Valid values are 1 to 99. The default is 10.
Max. Admin Connections	Enter the maximum number of concurrent connections (greater than 0) with LDAP administrator account permissions that can run for a specific LDAP configuration. These connections are used to search the directory for users and groups under the User Directory Subtree and the Group Directory Subtree. Valid values are 1 to 99. The default is 20.
Force reconnect every N seconds	Check this check box and enter the desired value in the **Seconds** field to force the server to renew LDAP connection at the specified time interval. The valid range is from 1 to 60 minutes.
Test Bind to Server	Click to test and ensure that the LDAP server details and credentials can successfully bind. If the test fails, edit your LDAP server details and retest.
Failover	
Always Access Primary Server First	Click this option if you want Cisco ISE to always access the primary LDAP server first for authentications and authorizations.
Failback to Primary Server After	If the primary LDAP server that Cisco ISE attempts to contact cannot be reached, Cisco ISE attempts to contact the secondary LDAP server. If you want Cisco ISE to use the primary LDAP server again, click this option and enter a value in the text box.

LDAP Directory Organization Settings

The following table describes the fields in the **Directory Organization** tab.

Table 63: LDAP Directory Organization Settings

Field Name	Usage Guidelines
Subject Search Base	Enter the DN for the subtree that contains all subjects. For example: o=corporation.com If the tree containing subjects is the base DN, enter: o=corporation.com or dc=corporation,dc=com as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.

Field Name	Usage Guidelines
Group Search Base	Enter the DN for the subtree that contains all groups. For example: ou=organizational unit, ou=next organizational unit, o=corporation.com If the tree containing groups is the base DN, type: o=corporation.com or dc=corporation,dc=com as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.
Search for MAC Address in Format	Enter a MAC Address format for Cisco ISE to use for search in the LDAP database. MAC addresses in internal identity sources are sourced in the format xx-xx-xx-xx-xx-xx. MAC addresses in LDAP databases can be sourced in different formats. However, when Cisco ISE receives a host lookup request, Cisco ISE converts the MAC address from the internal format to the format that is specified in this field. Use the drop-down list to enable searching for MAC addresses in a specific format, where <*format*> can be any one of the following: • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx The format you choose must match the format of the MAC address sourced in the LDAP server.
Strip Start of Subject Name Up To the Last Occurrence of the Separator	Enter the appropriate text to remove domain prefixes from usernames. If Cisco ISE finds the delimiter character that is specified in this field in the username, it strips all characters from the beginning of the username through the delimiter character. If the username contains more than one of the characters that are specified in the <start_string> box, Cisco ISE strips characters through the last occurrence of the delimiter character. For example, if the delimiter character is the backslash (\) and the username is DOMAIN\user1, Cisco ISE submits user1 to an LDAP server. **Note** The <start_string> cannot contain the following special characters: the pound sign (#), the question mark (?), the quotation mark (“), the asterisk (*), the right angle bracket (>), and the left angle bracket (<). Cisco ISE does not allow these characters in usernames.

Field Name	Usage Guidelines
Strip End of Subject Name from the First Occurrence of the Separator	Enter the appropriate text to remove domain suffixes from usernames. If Cisco ISE finds the delimiter character that is specified in this field in the username, it strips all characters from the delimiter character through the end of the username. If the username contains more than one of the characters that are specified in this field, Cisco ISE strips characters starting with the first occurrence of the delimiter character. For example, if the delimiter character is @ and the username is *user1@domain*, then Cisco ISE submits *user1* to the LDAP server. **Note** The *<end_string>* box cannot contain the following special characters: the pound sign (#), the question mark (?), the quotation mark ("), the asterisk (*), the right angle bracket (>), and the left angle bracket (<). Cisco ISE does not allow these characters in usernames.

LDAP Group Settings

Table 64: LDAP Group Settings

Field Name	Usage Guidelines
Add	Choose **Add > Add Group** to add a new group or choose **Add > Select Groups From Directory** to select the groups from the LDAP directory. If you choose to add a group, enter a name for the new group. If you are selecting from the directory, enter the filter criteria, and click **Retrieve Groups**. Check the check boxes next to the groups that you want to select and click **OK**. The groups that you have selected will appear in the **Groups** window.

LDAP Attribute Settings

Table 65: LDAP Attribute Settings

Field Name	Usage Guidelines
Add	Choose **Add > Add Attribute** to add a new attribute or choose **Add > Select Attributes From Directory** to select attributes from the LDAP server. If you choose to add an attribute, enter a name for the new attribute. If you are selecting from the directory, enter the username and click **Retrieve Attributes** to retrieve the attributes. Check the check boxes next to the attributes that you want to select, and then click OK.

LDAP Advanced Settings

The following table describes the field in the Advanced Settings tab.

Table 66: LDAP Advanced Settings

Field Name	Usage Guidelines
Enable Password Change	Check this check box to enable the user to change the password in case of password expiry or password reset while using PAP protocol for device admin and RADIUS EAP-GTC protocol for network access. User authentication fails for the unsupported protocols. This option also enables the user to change the password on their next login.

Related Topics

- LDAP Directory Service, on page 730
- LDAP User Authentication, on page 732
- LDAP User Lookup, on page 735
- Add LDAP Identity Sources, on page 735

RADIUS Token Identity Sources Settings

The following table describes the fields on the RADIUS Token Identity Sources window, which you can use to configure and connect to an external RADIUS identity source. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **RADIUS Token**.

Table 67: RADIUS Token Identity Source Settings

Field Name	Usage Guidelines
Name	Enter a name for the RADIUS token server. The maximum number of characters allowed is 64.
Description	Enter a description for the RADIUS token server. The maximum number of characters is 1024.
SafeWord Server	Check this check box if your RADIUS identity source is a SafeWord server.
Enable Secondary Server	Check this check box to enable the secondary RADIUS token server for Cisco ISE to use as a backup in case the primary fails. If you check this check box, you must configure a secondary RADIUS token server.
Always Access Primary Server First	Click this option if you want Cisco ISE to always access the primary server first.
Fallback to Primary Server after	Click this option to specify the amount of time in minutes that Cisco ISE can authenticate using the secondary RADIUS token server if the primary server cannot be reached. After this time elapses, Cisco ISE reattempts to authenticate against the primary server.
Primary Server	
Host IP	Enter the IP address of the primary RADIUS token server. This field can take as input a valid IP address that is expressed as a string. Valid characters that are allowed in this field are numbers and dot (.).

Field Name	Usage Guidelines
Shared Secret	Enter the shared secret that is configured on the primary RADIUS token server for this connection.
Authentication Port	Enter the port number on which the primary RADIUS token server is listening.
Server Timeout	Specify the time in seconds that Cisco ISE should wait for a response from the primary RADIUS token server before it determines that the primary server is down.
Connection Attempts	Specify the number of attempts that Cisco ISE should make to reconnect to the primary server before moving on to the secondary server (if defined) or dropping the request if a secondary server is not defined.
Secondary Server	
Host IP	Enter the IP address of the secondary RADIUS token server. This field can take as input a valid IP address that is expressed as a string. Valid characters that are allowed in this field are numbers and dot (.).
Shared Secret	Enter the shared secret configured on the secondary RADIUS token server for this connection.
Authentication Port	Enter the port number on which the secondary RADIUS token server is listening. Valid values are from 1 to 65,535. The default is 1812.
Server Timeout	Specify the time in seconds that Cisco ISE should wait for a response from the secondary RADIUS token server before it determines that the secondary server is down.
Connection Attempts	Specify the number of attempts that Cisco ISE should make to reconnect to the secondary server before dropping the request.

Related Topics

RADIUS Token Identity Sources, on page 752
Add a RADIUS Token Server, on page 756

RSA SecurID Identity Source Settings

The following table describes the fields on the RSA SecurID Identity Sources window, which you can use to create and connect to an RSA SecurID identity source. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **RSA SecurID**.

RSA Prompt Settings

The following table describes the fields in the **RSA Prompts** tab.

Table 68: RSA Prompt Settings

Field Name	Usage Guidelines
Enter Passcode Prompt	Enter a text string to obtain the passcode.
Enter Next Token Code	Enter a text string to request the next token.
Choose PIN Type	Enter a text string to request the PIN type.
Accept System PIN	Enter a text string to accept the system-generated PIN.
Enter Alphanumeric PIN	Enter a text string to request an alphanumeric PIN.
Enter Numeric PIN	Enter a text string to request a numeric PIN.
Re-enter PIN	Enter a text string to request the user to re-enter the PIN.

RSA Message Settings

The following table describes the fields in the **RSA Messages** tab.

Table 69: RSA Messages Settings

Field Name	Usage Guidelines
Display System PIN Message	Enter a text string to label the system PIN message.
Display System PIN Reminder	Enter a text string to inform the user to remember the new PIN.
Must Enter Numeric Error	Enter a message that instructs users to enter only numbers for the PIN.
Must Enter Alpha Error	Enter a message that instructs users to enter only alphanumeric characters for PINs.
PIN Accepted Message	Enter a message that the users see when their PIN is accepted by the system.
PIN Rejected Message	Enter a message that the users see when the system rejects their PIN.
User Pins Differ Error	Enter a message that the users see when they enter an incorrect PIN.
System PIN Accepted Message	Enter a message that the users see when the system accepts their PIN.
Bad Password Length Error	Enter a message that the users see when the PIN that they specify does not fall within the range specified in the PIN length policy.

Related Topics

RSA Identity Sources, on page 758
Cisco ISE and RSA SecurID Server Integration, on page 759
Add RSA Identity Sources, on page 761

Cisco ISE Users

In this topic, the term *user* refers to employees and contractors who access a network regularly, as well as to sponsor users and guest users. A sponsor user is an employee or contractor of an organization who creates and manages guest user accounts through the sponsor portal. A guest user is an external visitor who needs access to an organization's network resources for a limited period of time.

You must create an account for all the users to gain access to resources and services on the Cisco ISE network. Employees, contractors, and sponsor users should be created from the Admin portal.

From Cisco ISE Release 3.2, you can choose to add the **Date Enabled** column (**Settings** > **Columns** > **Date Enabled**) and the **Days Until Password Expires** column (**Settings** > **Columns** > **Days Until Password Expires**) to the **Network Access User** table in the **Network Access Users** window (**Administration** > **Identity Management** > **Identities** > **Users**) to help you sort network access users by using their password expiry information. The **Date Enabled** and **Days Until Password Expires** fields are not added by default. You can add them to the **Network Access User** table using the customization option in the window.

User Identity

User identity is like a container that holds information about a user and forms their network access credentials. Each user's identity is defined by data and includes: a username, e-mail address, password, account description, associated administrative group, user group, and role.

User Groups

User groups are a collection of individual users who share a common set of privileges that allow them to access a specific set of Cisco ISE services and functions.

User Identity Groups

A user's group identity is composed of elements that identify and describe a specific group of users that belong to the same group. A group name is a description of the functional role that the members of this group have. A group is a listing of the users that belong to this group.

Default User Identity Groups

Cisco ISE comes with the following predefined user identity groups:

- All_Accounts
- Employee
- Group_Accounts
- GuestType_Contractor

- GuestType_Daily
- GuestType_SocialLogin
- GuestType_Weekly
- Own_Accounts

User Role

A user role is a set of permissions that determine what tasks a user can perform and what services they can access on the Cisco ISE network. A user role is associated with a user group. For example, a network access user.

User Account Custom Attributes

Cisco ISE allows you to restrict network access based on user attributes for both network access users and administrators. Cisco ISE comes with a set of predefined user attributes and also allows you to create custom attributes. Both types of attributes can be used in conditions that define the authentication policy. You can also define a password policy for user accounts so that passwords meet specified criteria.

Custom User Attributes

You can configure more user-account attributes on the **User Custom Attributes** window (**Administration > Identity Management > Settings > User Custom Attributes**). You can also view the list of predefined user attributes in this window. You cannot edit the predefined user attributes.

Enter the required details in the **User Custom Attributes** pane to add a new custom attribute. The custom attributes and the default values that you add on the **User Custom Attributes** window are displayed while adding or editing a Network Access user (**Administration > Identity Management > Identities > Users > Add/Edit**) or Admin user (**Administration > System > Admin Access > Administrators > Admin Users > Add/Edit**). You can change the default values while adding or editing a Network Access or Admin user.

Note PAP and PAP_ASCII (for VPN connections) authentication flows do not support the **Change password on next login** setting.

You can select the following data types for the custom attributes on the **User Custom Attributes** window:

- String: You can specify the maximum string length (maximum allowed length for a string attribute value).
- Integer: You can configure the minimum and maximum value (specifies the lowest and the highest acceptable integer value).
- Enum: You can specify the following values for each parameter:
  - Internal value
  - Display value

  You can also specify the default parameter. The values that you add in the Display field are displayed while adding or editing a Network Access or Admin user.

- Float
- Password: You can specify the maximum string length.
- Long: You can configure the minimum and maximum value.
- IP: You can specify a default IPv4 or IPv6 address.
- Boolean: You can set either True or False as the default value.
- Date: You can select a date from the calendar and set it as the default value. The date is displayed in yyyy-mm-dd format.

Check the **Mandatory** check box if you want to make an attribute mandatory while adding or editing a Network Access or Admin user. You can also set default values for the custom attributes.

The custom attributes can be used in the authentication policies. The data type and the allowable range that you set for the custom attributes are applied to the custom attribute values in the policy conditions.

Remember Some characters are considered invalid for Attribute Names and Attribute Values. Using the following characters for Attribute Names and Attribute Values is restricted.

- Attribute Value: @, =, +, or - (do not use these characters at the beginning of an attribute name or value)
- Attribute Name: ^, =, , \, ", `, |, : (do not use these characters anywhere in the string)

User Authentication Settings

Not all external identity stores allow network access users to change their passwords. See the section for each identity source for more information.

Network-use password rules should be configured in **Administration** > **Identity Management** > **Settings** > **User Authentication Settings**.

The following section has additional information about some of the fields in the **Password Policy** tab.

- **Required Characters**: If you configure a user-password policy that requires upper or lowercase characters, and the user’s language does not support these characters, the user cannot set a password. To support UTF-8 characters, uncheck the following check boxes:
  - **Lowercase Alphabetic Characters**
  - **Uppercase Alphabetic Characters**
- **Password Change Delta**: Specifies the minimum number of characters that must change when changing the current password to a new password. Cisco ISE does not consider changing the position of a character as a change. For Example, if the password delta is 3, and the current password is "?Aa1234?", then "?Aa1567?" ("5","6" and "7" are the three new characters) is a valid new password. "?Aa1562?" fails, because "?","2", and "?" characters are in the current password. "Aa1234??" fails, because even though the character positions changed, the same characters are in the current password.

  Password change delta also considers the previous X passwords, where X is the value of **Password must be different from the previous versions**. If your password delta is 3, and your password history is 2, then you must change the four characters that are not a part of the past two passwords.

- **Dictionary words**: Check this check box to restrict the use of any dictionary word, its characters in reverse order, or its letters replaced with other characters.

  Substitution of "$" for "s", "@" for "a", "0" for "o", "1" for "l", "!" for "i", "3" for "e", is not permitted. For example, "Pa$$w0rd".

  - **Default Dictionary**: Choose this option to use the default Linux dictionary in Cisco ISE. The default dictionary contains approximately 480,000 English words.
  - **Custom Dictionary**: Choose this option to use your customized dictionary. Click **Choose File** to select a custom dictionary file. The text file must be of newline-delimited words, .dic extension, and size less than 20 MB.

- You can use the **Password Lifetime** section to update the password reset interval and reminder. To set the lifetime of a password, check the **Change password every __ days (valid range 1 to 3650)** check box, and enter the number of days in the input field. A user account can be disabled if a user does not change the password in the specified time by selecting the **Disable User Account** option. Choose the **Require password change on next login** to prompt the user to change their password the next time they login to Cisco ISE.

  To send a reminder email for password reset, check the **Display Reminder __ Days Prior to Password Expiration** check box and enter the number of days before which a reminder email should be sent to the email address configured for the network access user. While creating a network access user, you can add the email address in the **Administration > Identity Management > Identities > Users > Add Network Access User** window to send an email notification for password reset.

Note

- The reminder email is sent from the following email address: iseadminportal@<ISE-Primary-FQDN>. You must explicitly permit access for this sender.
- By default, the reminder email has the following content: Your network access password will expire on <*password expiry date and time*>. Please contact your system administrator for assistance.

  From Cisco ISE Release 3.2, you can customize the email content after the *Please contact your system administrator for assistance* portion of the email notification.

- **Lock/Suspend Account with Incorrect Login Attempts**: Use this option to suspend or lock an account if the login attempt failed for the specified number of times. The valid range is from 3 to 20.
- **Account Disable Policy**: Configure the rules about when to disable an existing user account. See Disable User Accounts Globally for more information.

Related Topics

User Account Custom Attributes, on page 625

To Add Users, on page 628

Generate Automatic Password for Users and Administrators

You can use the **Generate Password** option on the user and administrator creation window to generate instant password adhering to Cisco ISE password policies. This helps the users or administrators to use the password generated by Cisco ISE than spending time in thinking of a safe password to be configured.

The **Generate Password** option is available in the following windows:

- **Administration > Identity Management > Identities > Users**.
- **Administration > System > Admin Access > Administrators > Admin Users**.
- **Settings > Account Settings > Change Password**.

Internal User Operations

To Add Users

Cisco ISE allows you to view, create, modify, duplicate, delete, change the status, import, export, or search for attributes of Cisco ISE users.

If you are using a Cisco ISE internal database, you must create an account for any new user who needs access to the resources or services on a Cisco ISE network.

Step 1 Choose **Administration** > **Identity Management** > **Identities** > **Users**.

You can also create users by accessing the **Work Centers** > **Device Administration** > **Identities** > **Users** window.

Step 2 Click **Add (+)** to create a new user.

Step 3 Enter values in all the fields the fields**.**

Note Do not include !, %, :, ;, [, {, |, },], `, ?, =, <, >, \ and control characters in the username. Username with only spaces is also not allowed. If you use the Cisco ISE Internal Certificate Authority (CA) for BYOD, the username that you provide here is used as the Common Name for the endpoint certificate. Cisco ISE Internal CA does not support "+" or "*" characters in the Common Name field.

Step 4 Click **Submit** to create a new user in the Cisco ISE internal database.

Export Cisco ISE User Data

You can export user data from the Cisco ISE internal database. Cisco ISE allows you to export user data in the form of a password-protected CSV file.

Step 1 Choose **Administration** > **Identity Management** > **Identities** > **Users**.

Step 2 Check the check box that corresponds to the user(s) whose data you want to export.

Step 3 Click **Export Selected**.

Step 4 In the **Key** field, enter a key for encrypting the password.

Step 5 Click **Start Export** to create a users.csv file.

Step 6 Click **OK** to export the users.csv file.

Import Cisco ISE Internal Users

You can import new user data into Cisco ISE with a CSV file, to create new internal accounts. A template CSV file is available for download while you import user accounts. Sponsors can import users in the Sponsor portal. See Configure Account Content for Sponsor Account Creation, on page 518 for information about configuring the information types that the sponsor guest accounts use.

Note If the CSV file contains custom attributes, the data type and the allowable range that you set for the custom attributes will be applied to the custom attribute values during import.

Step 1 Choose **Administration** > **Identity Management** > **Identities** > **Users**.

Step 2 Click **Import** to import users from a comma-delimited text file.

If you do not have a comma-delimited text file, click **Generate a Template** to create a CSV file with the heading rows filled in.

Step 3 In the **File** field, enter the filename containing the usernames to import, or click **Browse** and navigate to the location where the file is present.

Step 4 Check the **Create new user(s) and update existing user(s) with new data** check box to create new users and update existing user details.

Step 5 Click **Save**.

We recommend that you do not delete all the network access users at a time, because this may lead to CPU spike and the services to crash, especially if you are using a very large database.

Endpoint Settings

The following table describes the fields on the **Endpoints** window, which you can use to create endpoints and assign policies for endpoints. To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Identities** > **Endpoints**.

Table 70: Endpoint Settings

Field Name	Usage Guidelines
MAC Address	Enter the MAC address in hexadecimal format to create an endpoint statically. The MAC address is the device identifier for the interface that is connected to the Cisco ISE enabled network.
Static Assignment	Check this check box when you want to create an endpoint statically in the Endpoints window and the status of static assignment is set to static. You can toggle the status of static assignment of an endpoint from static to dynamic or from dynamic to static.

Field Name	Usage Guidelines
Policy Assignment	(Disabled by default unless the **Static Assignment** is checked) Choose a matching endpoint policy from the **Policy Assignment** drop-down list. You can do one of the following: • If you do not choose a matching endpoint policy, but use the default endpoint policy Unknown, then the static assignment status is set to dynamic for the endpoint that allows dynamic profiling of an endpoint. • If you choose a matching endpoint policy other than Unknown, then the static assignment status is set to static for that endpoint and the **Static Assignment** check box is automatically checked.
Static Group Assignment	Check this check box when you want to assign an endpoint to an identity group statically. In you check this check box, the profiling service does not change the endpoint identity group the next time during evaluation of the endpoint policy for these endpoints, which were previously assigned dynamically to other endpoint identity groups. If you uncheck this check box, then the endpoint identity group is dynamic as assigned by the ISE profiler based on policy configuration. If you do not choose the Static Group Assignment option, then the endpoint is automatically assigned to the matching identity group the next time during evaluation of the endpoint policy.

Identity Group Assignment	Choose an endpoint identity group to which you want to assign the endpoint.
	You can assign an endpoint to an identity group when you create an endpoint statically, or when you do not want to use the **Create Matching Identity Group** option during evaluation of the endpoint policy for an endpoint.
	Cisco ISE includes the following system created endpoint identity groups:
	• Blocked List
	• GuestEndpoints
	• Profiled
	  • Cisco IP-Phone
	  • Workstation
	• RegisteredDevices
	• Unknown

Active Directory user endpoints that repeatedly fail RADIUS authentication for the same reason will be automatically rejected for a certain period, to avoid unnecessary processing by Cisco ISE and to protect against potential denial of service attacks.

To view a list of rejected endpoints, choose **Operations** > **Reports** > **Rejected Endpoints**. The data for this report will be available and displayed only when Advantage License is installed.

Note AD user endpoints that fail RADIUS authentication with the following two error messages are not rejected:

22063 - WRONG_PASSWORD

24408 - ACTIVE_DIRECTORY_USER_WRONG_PASSWORD

Related Topics

Identified Endpoints, on page 833

Create Endpoints with Static Assignments of Policies and Identity Groups, on page 828

Endpoint Import from LDAP Settings

The following table describes the fields on the Import from LDAP window, which you can use to import endpoints from an LDAP server. To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Identities** > **Endpoints**.

Table 71: Endpoint Import from LDAP Settings

Field Name	Usage Guidelines
Connection Settings	
Host	Enter the hostname, or the IP address of the LDAP server.
Port	Enter the port number of the LDAP server. You can use the default port 389 to import from an LDAP server, and the default port 636 to import from an LDAP server over SSL. **Note** Cisco ISE supports any configured port number. The configured value should match the LDAP server connection details.
Enable Secure Connection	Check the **Enable Secure Connection** check box to import from an LDAP server over SSL.
Root CA Certificate Name	Click the drop-down arrow to view the trusted CA certificates. The Root CA Certificate Name refers to the trusted CA certificate that is required to connect to an LDAP server. You can add (import), edit, delete, and export trusted CA certificates in Cisco ISE.
Anonymous Bind	You must enable either the **Anonymous Bind** check box, or enter the LDAP administrator credentials from the slapd.conf configuration file.
Admin DN	Enter the distinguished name (DN) configured for the LDAP administrator in the slapd.conf configuration file. Admin DN format example: cn=Admin, dc=cisco.com, dc=com
Password	Enter the password configured for the LDAP administrator in the slapd.conf configuration file.

Field Name	Usage Guidelines
Base DN	Enter the distinguished name of the parent entry. Base DN format example: dc=cisco.com, dc=com.
Query Settings	
MAC Address objectClass	Enter the query filter, which is used for importing the MAC address, for example, ieee802Device.
MAC Address Attribute Name	Enter the returned attribute name for import, for example, macAddress.
Profile Attribute Name	Enter the name of the LDAP attribute. This attribute holds the policy name for each endpoint entry that is defined in the LDAP server. When you configure the **Profile Attribute Name** field, consider the following: • If you do not specify this LDAP attribute in the **Profile Attribute Name** field or configure this attribute incorrectly, then endpoints are marked "Unknown" during an import operation, and these endpoints are profiled separately to the matching endpoint profiling policies. • If you configure this LDAP attribute in the **Profile Attribute Name** field, the attribute values are validated to ensure that the endpoint policy matches with an existing policy in Cisco ISE, and endpoints are imported. If the endpoint policy does not match with an existing policy, then those endpoints will not be imported.
Time Out	Enter the time in seconds. The valid range is from 1 to 60 seconds.

Related Topics

Identified Endpoints, on page 833

Import Endpoints from LDAP Server, on page 831

Identity Group Operations

Create a User Identity Group

You must create a user identity group before you can assign a user to it.

Step 1 Choose **Administration** > **Identity Management** > **Groups** > **Identity Groups** > **User Identity Groups** > **Add**.

You can also create a user identity group by accessing the **Work Centers** > **Device Administration** > **User Identity Groups** > **Identity Groups** > **User Identity Groups** > **Add** page.

Step 2 Enter values in the Name and Description fields. Supported characters for the Name field are space # $ & ‘ ( ) * + - . / @ _ .

Step 3 Click **Submit**.

Related Topics

User Identity Groups, on page 624

Export User Identity Groups

Cisco ISE allows you to export locally configured user identity groups in the form of a csv file.

Step 1 Choose **Administration** > **Identity Management** > **Groups** > **Identity Groups** > **User Identity Groups**.

Step 2 Check the check box that corresponds to the user identity group that you want to export, and click **Export**.

Step 3 Click **OK**.

Import User Identity Groups

Cisco ISE allows you to import user identity groups in the form of a csv file.

Step 1 Choose **Administration** > **Identity Management** > **Groups** > **Identity Groups** > **User Identity Groups**.

Step 2 Click **Generate a Template** to get a template to use for the import file.

Step 3 Click Import to import network access users from a comma-delimited text file.

Step 4 Check the **Overwrite existing data with new data** check box if you want to both add a new user identity group and update existing user identity groups.

Step 5 Click **Import**.

Step 6 Click **Save** to save your changes to the Cisco ISE database.

Endpoint Identity Group Settings

The following table describes the fields on the Endpoint Identity Groups window, which you can use to create an endpoint group. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **Groups** > **Endpoint Identity Groups**.

Table 72: Endpoint Identity Group Settings

Field Name	Usage Guidelines
Name	Enter the name of the endpoint identity group that you want to create.
Description	Enter a description for the endpoint identity group that you want to create.
Parent Group	Choose an endpoint identity group from the **Parent Group** drop-down list to which you want to associate the newly created endpoint identity group.

Related Topics

Identified Endpoints Grouped in Endpoint Identity Groups, on page 835

Create Endpoint Identity Groups, on page 835

Configure Maximum Concurrent Sessions

For optimal performance, you can limit the number of concurrent user sessions. You can set the limits at the user level or at the group level. Depending upon the maximum user session configurations, the session count is applied to the user.

You can configure the maximum number of concurrent sessions for each user per ISE node. Sessions above this limit are rejected.

Step 1 Choose **Administration** > **System** > **Settings** > **Max Sessions** > **User**.

Step 2 Do one of the following:

- Enter the maximum number of concurrent sessions that are allowed for each user in the **Maximum Sessions per User** field.
- Check the **Unlimited Sessions** check box if you want the users to have unlimited sessions. This option is selected by default.

Step 3 Click **Save**.

If the maximum number of sessions is configured at both the user and group level, the smaller value will have precedence. For example, if the maximum session value for a user is set as 10 and the maximum session value of the group to which the user belongs is set as 5, the user can have a maximum of 5 sessions only.

Note The maximum concurrent session count is managed by the PSN in which it is configured. This count is not synchronized among the PSNs. If the authentication is done in Cisco ISE, where the maximum concurrent sessions per user or group is configured, and authorization is done in a different proxy server, then the maximum concurrent session limit is applicable only in the Cisco ISE and is not applied to the proxy server.

Maximum concurrent session count is implemented in the runtime process and the data is stored only in the memory. If the PSN is restarted, the maximum concurrent session counters are reset.

Maximum concurrent session count is case insensitive with respect to usernames irrespective of the Network Access Device used (when the same PSN node is used)

Maximum Concurrent Sessions for a Group

You can configure the maximum number of concurrent sessions for the identity groups.

Sometimes all the sessions can be used by a few users in the group. Requests from other users to create a new session are rejected because the number of sessions has already reached the maximum configured value. Cisco ISE allows you to configure a maximum session limit for each user in the group; each user belonging to a specific identity group cannot open sessions more than the session limit, irrespective of the number of sessions other users from the same group have opened. When calculating the session limit for a particular user, the lowest configuration value takes the precedence—whether the global session limit per user, the session limit per identity group that the user belongs to, or the session limit per user in the group.

To configure maximum number of concurrent sessions for an identity group:

Step 1 Choose **Administration** > **System** > **Settings** > **Max Sessions** > **Group**.

All the configured identity groups are listed.

Step 2 Click the Edit icon next to the group that you want to edit and enter the values for the following:

- Maximum number of concurrent sessions permitted for that group. If the maximum number of sessions for a group is set as 100, the total count of all sessions established by all members of that group cannot exceed 100.

  Note Group-level session limits are applied based on the group hierarchy.

- Maximum number of concurrent sessions permitted for each user in that group. This option overrides the maximum number of sessions for a group.

If you want to set the maximum number of concurrent sessions for a group or maximum concurrent sessions for the users in a group as Unlimited, leave the **Max Sessions for Group/Max Sessions for User in Group** field blank, click the Tick icon, and then click Save. By default, both these values are set as Unlimited.

Step 3 Click **Save**.

Configure Counter Time Limit

You can configure the timeout value for concurrent user sessions.

Step 1 Choose **Administration** > **System** > **Settings** > **Max Sessions** > **Counter Time Limit**.

Step 2 Select one of the following options:

- **Unlimited**: Check this check box if you do not want to set any timeout or time limit for the sessions.
- **Delete sessions after**: You can enter the timeout value for concurrent sessions in minutes, hours, or days. When a session exceeds the time limit, Cisco ISE deletes the session from the counter and updates the session count, thereby allowing new sessions. Users will not be logged out if their sessions exceed the time limit.

Step 3 Click **Save**.

You can reset the session count from the RADIUS Live Logs window. Click the Actions icon displayed on the Identity, Identity Group, or Server column to reset the session count. When you reset a session, the session is deleted from the counter (thereby allowing new sessions). Users will not be disconnected if their sessions are deleted from the counter.

Disable Account Policy

While authenticating or querying a user or administrator, Cisco ISE checks the global account disable policy settings at **Administration** > **Identity Management** > **Settings** > **User Authentication Settings** and authenticates or returns a result based on the configuration.

Cisco ISE verifies the following three policies:

- Disable user accounts that exceed a specified date (yyyy-mm-dd): Disables the user account on the specified date. However, the account disable policy settings for an individual network access user configured at **Administration > Identity Management > Identities > Users > Account Disable Policy** takes precedence over the global settings.
- Disable user account after *n* days of account creation or last enable: Disables user accounts after specific number of days of account creation or the last date when the account was active. You can check the user status at **Administration > Identity Management > Identities > Users > Status**.
- Disable accounts after *n* days of inactivity: Disables administrator and user accounts that have not been authenticated for the configured consecutive number of days. The disable accounts after *n* days of inactivity option is only applicable for Cisco ISE Internal Users using internal passwords.

When you migrate from Cisco Secure ACS to Cisco ISE, the account disable policy settings specified for a network access user in Cisco Secure ACS is migrated to Cisco ISE.

Note A collection filter configured for any **Filter Type** filters out the authentication syslog messages that are sent to the monitoring node. For more information, see the topic "Collection Filters" in the chapter "Maintain and Monitor" in the *Cisco ISE Administrator Guide*.

If you configure a collection filter (**Administration** > **System** > **Logging** > **Collection Filter**) for any **Attribute** and **Filter Type**; and you have also selected the **Disable account after n days of inactivity** check box (**Administration** > **Identity Management** > **User Authentication Settings** > **Disable Account Policy**), your account might be disabled as a result of the syslog messages of successful authentication not being relayed to the monitoring node.

Disable Individual User Accounts

Cisco ISE allows you to disable the user account for each individual user if the disable account date exceeds the date specified by the admin user.

Step 1 Choose **Administration > Identity Management > Identities > Users**.

Step 2 Click **Add** to create a new user or check the check box next to an existing user and click **Edit** to edit the existing user details.

Step 3 Check the **Disable account if the date exceeds** check box and select the date.

This option allows you to disable the user account when the configured date exceeds at user level. You can configure different expiry dates for different users as required. This option overrules the global configuration for each individual user. The configured date can either be the current system date or a future date.

Note You are not allowed to enter a date earlier than the current system date.

Step 4 Click **Submit** to configure the account disable policy for an individual user.

Disable User Accounts Globally

You can disable user accounts on a certain date, several days after account creation or last access date, and after several days of account inactivity.

Step 1 Choose **Administration** > **Identity Management** > **Settings** > **User Authentication Settings** > **Account Disable Policy**.

Step 2 Perform one of the following actions:

- Check the **Disable account if date exceeds** check box and select the appropriate date in yyyy-mm-dd format. This option allows you to disable the user account after the configured date. The **Disable account if date exceeds** setting at user level takes precedence over this global configuration.
- Check the **Disable account after n days of account creation or last enable** check box and enter the number of days. This option disables the user account when the account creation date or last access date exceeds the specified number of days. Administrators can manually enable the disabled user accounts, which reset the number of days count.
- Check the **Disable account after n days of inactivity** check box and enter the number of days. This option disables the user account when the account is inactive for the specified number of days.

Step 3 Click **Submit** to configure the global account disable policy.

Note When you are using the **Disable account after n days of inactivity** option to disable inactive users of Cisco ISE, the endpoints logged to My Devices portal will not have the number of active days reset. This is because My Devices portal doesn't send any profiling updates or accounting information.

Internal and External Identity Sources

Identity sources are databases that store user information. Cisco ISE uses user information from the identity source to validate user credentials during authentication. User information includes group information and other attributes that are associated with the user. You can add, edit, and delete user information from identity sources.

Cisco ISE supports internal and external identity sources. You can use both sources to authenticate sponsor and guest users.

Internal Identity Sources

Cisco ISE has an internal user database whree you can store user information. Users in the internal user database are called internal users. Cisco ISE also has an internal endpoint database that stores information about all the devices and endpoints that connect to it.

External Identity Sources

Cisco ISE allows you to configure the external identity source that contains user information. Cisco ISE connects to an external identity source to obtain user information for authentication. External identity sources also include certificate information for the Cisco ISE server and certificate authentication profiles. Cisco ISE uses authentication protocols to communicate with external identity sources.

Note the following points while configuring policies for internal users:

- Configure an authentication policy to authenticate internal users against an internal identity store.
- Configure an authorization policy for internal user groups by selecting the following option:

  `Identitygroup.Name EQUALS User Identity Groups:` **`Group_Name`**

The following table lists authentication protocols and the external identity sources that they support.

Table 73: Authentication Protocols and Supported External Identity Sources

Protocol (Authentication Type)	Internal Database	Active Directory	LDAP	RADIUS Token Server or RSA	REST	ODBC
EAP-GTC, PAP (plain text password)	Yes	Yes	Yes	Yes	Yes	Yes
MS-CHAP password hash: MSCHAPv1/v2 EAP-MSCHAPv2 (as inner method of PEAP, EAP-FAST, EAP-TTLS or TEAP) LEAP	Yes	Yes	No	No	No	Yes
EAP-MD5 CHAP	Yes	No	No	No	No	Yes

Protocol (Authentication Type)	**Internal Database**	**Active Directory**	**LDAP**	**RADIUS Token Server or RSA**	**REST**	**ODBC**
EAP-TLS PEAP-TLS (certificate retrieval) **Note** For TLS authentications (EAP-TLS and PEAP-TLS), identity sources are not required but can optionally be added for authorization policy conditions.	No	Yes	Yes	No	No	No

Credentials are stored differently, depending on the external data source connection type, and the features used.

- When joining an Active Directory Domain (but not for Passive ID), the credentials that are used to join are not saved. Cisco ISE creates an AD computer account, if it does not exist, and uses that account to authenticate users.
- For LDAP and Passive ID, the credentials that are used to connect to the external data source are also used to authenticate users.

Create an External Identity Source

Cisco ISE can connect with external identity sources such as Active Directory, LDAP, RADIUS Token, and RSA SecurID servers to obtain user information for authentication and authorization. External identity sources also include certificate authentication profiles that you need for certificate-based authentications.

Note To work with passive identity services, which enable you to receive and share authenticated user identities, see Additional Passive Identity Service Providers, on page 690.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources**.

Step 2 Choose one of these options:

- **Certificate Authentication Profile** for certificate-based authentications.

- **Active Directory** to connect to an Active Directory as an external identity source. See Active Directory as an External Identity Source, on page 641 for more details.
- **LDAP** to add an LDAP identity source. See LDAP, on page 730 for more details.
- **RADIUS Token** to add a RADIUS Token server. See RADIUS Token Identity Sources, on page 752 for more details.
- **RSA SecurID** to add an RSA SecurID server. See RSA Identity Sources, on page 758 for more details.
- **SAML Id Providers** to add an identity provider (IdP), such as Oracle Access Manager. See SAMLv2 Identity Provider as an External Identity Source, on page 764 for more details.
- **Social Login** to add a Social Login, such as Facebook, as an external identity source. See Social Login for Self-Registered Guests, on page 493 for more details.

Authenticate Internal Users Against External Identity Store Password

Cisco ISE allows you to authenticate internal users against external identity store passwords. Cisco ISE provides an option to select the password identity store for internal users from the **Administration** > **Identity Management** > **Identities** > **Users** window. Administrators can select the identity store from the list of Cisco ISE External Identity Sources while adding or editing users in the **Users** window. The default password identity store for an internal user is the internal identity store. Cisco Secure ACS users will retain the same password identity store during and after migration from Cisco Secure ACS to Cisco ISE.

Cisco ISE supports the following external identity stores for password types:

- Active Directory
- LDAP
- ODBC
- RADIUS Token server
- RSA SecurID server

Note As per the current design, if authentication is done against an external ID store, then the internal user identity group name cannot be configured in authorization policy. In order to use internal user identity group for authorization, authentication policy must be configured to authenticate against Internal Users ID store and password type, which can be either internal or external, must be selected in user configuration.

Certificate Authentication Profiles

For each profile, you must specify the certificate field that should be used as the principal username and whether you want a binary comparison of the certificates.

Add a Certificate Authentication Profile

You must create a certificate authentication profile if you want to use the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) certificate-based authentication method. Instead of authenticating via the traditional username and password method, Cisco ISE compares a certificate received from a client with one in the server to verify the authenticity of a user.

Before you begin

You must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **Certificate Authentication Profile** > **Add**.

Step 2 Enter the name and an optional description for the certificate authentication profile.

Step 3 Select an identity store from the drop-down list.

Basic certificate checking does not require an identity source. If you want binary comparison checking for the certificates, you must select an identity source. If you select Active Directory as an identity source, subject and common name and subject alternative name (all values) can be used to look up a user.

Step 4 Select the use of identity from **Certificate Attribute** or **Any Subject or Alternative Name Attributes in the Certificate**. This will be used in logs and for lookups.

If you choose **Any Subject or Alternative Name Attributes in the Certificate**, Active Directory UPN will be used as the username for logs and all subject names and alternative names in a certificate will be tried to look up a user. This option is available only if you choose Active Directory as the identity source.

Step 5 Choose when you want to **Match Client Certificate Against Certificate In Identity Store**. For this you must select an identity source (LDAP or Active Directory.) If you select Active Directory, you can choose to match certificates only to resolve identity ambiguity.

- **Never**: This option never performs a binary comparison.
- **Only to resolve identity ambiguity**: This option performs the binary comparison of client certificate to certificate on account in Active Directory only if ambiguity is encountered. For example, several Active Directory accounts matching to identity names from certificate are found.
- **Always perform binary comparison**: This option always performs the binary comparison of client certificate to certificate on account in identity store (Active Directory or LDAP).

Step 6 Click **Submit** to add the certificate authentication profile or save the changes.

Active Directory as an External Identity Source

Cisco ISE uses Microsoft Active Directory as an external identity source to access resources such as users, machines, groups, and attributes. User and machine authentication in Active Directory allows network access only to users and devices that are listed in Active Directory.

After a Cisco ISE node joins Active Directory, in Active Directory, it is a member of the Authenticated Users group. The Authenticated Users group is a member of the Pre-Windows 2000 group by default. If you disable the Pre-Windows 2000 group or remove Authenticated Users from the Pre-Windows 2000 group, authentication failures occur.

We recommend that you do not disable the Pre-windows 2000 group. However, if you must disable this group for any reason, grant the Read Remote Access Information permission to Cisco ISE in AD for the relevant users or users' folders.

ISE Community Resource

ISE Administrative Portal Access with AD Credentials Configuration Example

Active Directory-Supported Authentication Protocols and Features

Active Directory supports features such as user and machine authentications, changing Active Directory user passwords with some protocols. The following table lists the authentication protocols and the respective features that are supported by Active Directory.

Table 74: Authentication Protocols Supported by Active Directory

Authentication Protocols	Features
EAP-FAST and password based Protected Extensible Authentication Protocol (PEAP)	User and machine authentication with the ability to change passwords using EAP-FAST and PEAP with an inner method of MS-CHAPv2 and EAP-GTC
Password Authentication Protocol (PAP)	User and machine authentication
Microsoft Challenge Handshake Authentication Protocol Version 1 (MS-CHAPv1)	User and machine authentication
Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2)	User and machine authentication
Extensible Authentication Protocol-Generic Token Card (EAP-GTC)	User and machine authentication
Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)	• User and machine authentication • Groups and attributes retrieval • Binary certificate comparison

Authentication Protocols	**Features**
Extensible Authentication Protocol- Flexible Authentication via Secure Tunneling-Transport Layer Security (EAP-FAST-TLS)	• User and machine authentication • Groups and attributes retrieval • Binary certificate comparison
Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)	• User and machine authentication • Groups and attributes retrieval • Binary certificate comparison
Lightweight Extensible Authentication Protocol (LEAP)	User authentication

Active Directory Attribute and Group Retrieval for Use in Authorization Policies

Cisco ISE retrieves user or machine attributes and groups from Active Directory for use in authorization policy rules. These attributes can be used in Cisco ISE policies and determine the authorization level for a user or machine. Cisco ISE retrieves user and machine Active Directory attributes after successful authentication and can also retrieve attributes for an authorization that is independent of authentication.

Cisco ISE may use groups in external identity stores to assign permissions to users or computers; for example, to map users to sponsor groups. You should note the following restrictions on group memberships in Active Directory:

- Policy rule conditions may reference any of the following: a user's or computer's primary group, the groups of which a user or computer is a direct member, or indirect (nested) groups.
- Domain local groups outside a user's or computer's account domain are not supported.

Note You can use the value of the Active Directory attribute, msRadiusFramedIPAddress, as an IP address. This IP address can be sent to a network access server (NAS) in an authorization profile. The msRADIUSFramedIPAddress attribute supports only IPv4 addresses. Upon user authentication, the msRadiusFramedIPAddress attribute value fetched for the user will be converted to IP address format.

Attributes and groups are retrieved and managed per join point. They are used in authorization policy (by selecting first the join point and then the attribute). You cannot define attributes or groups per scope for authorization, but you can use scopes for authentication policy. When you use a scope in authentication policy, it is possible that a user is authenticated via one join point, but attributes and/or groups are retrieved via another join point that has a trust path to the user's account domain. You can use authentication domains to ensure that no two join points in one scope have any overlap in authentication domains.

During the authorization process in a multi join point configuration, Cisco ISE will search for join points in the order in which they listed in the authorization policy, only until a particular user has been found. Once a user has been found the attributes and groups assigned to the user in the join point, will be used to evaluate the authorization policy.

In a multi join point configuration, if authentication is successful for the same identity from each of the join points individually, then this authentication fails if it is done against the identity source sequence "All_AD_Join_Points".

In a multi join point configuration, if Active Directory group retrieval is successful for the same identity from each of the join points individually, then Active Directory group retrieval fails if:

- different join points are used for authentication and authorization.
- authentication uses EAP-TLS without Binary Comparison (**Match Client Certificate Against Certificate In Identity Store** is set to **Never** in the **Certificate Authentication Profile**) and there is an unmatched authorization rule with a different join point ahead of the matched authorization rule.
- authentication uses EAP-TLS without Binary Comparison (**Match Client Certificate Against Certificate In Identity Store** is set to **Never** in **Certificate Authentication Profile**) and Machine Access Restriction (MAR) is enabled with the endpoint using a different join point within the MAR period, from the join point in the current matched authorization rule.

Note See Microsoft-imposed limits on the maximum number of usable Active Directory groups: http://technet.microsoft.com/en-us/library/active-directory-maximum-limits-scalability(v=WS.10).aspx

An authorization policy fails if the rule contains an Active Directory group name with special characters such as /, !, @, \, #, $, %, ^, &, *, (,), _, +, or ~.

Admin user login through Active Directory might fail if the admin username contains $ character.

Use Explicit UPN

To reduce ambiguity when matching user information against Active Directory's User-Principal-Name (UPN) attributes, you must configure Active Directory to use Explicit UPN. Using Implicit UPN can produce ambiguous results if two users have the same value for *sAMAccountName*.

To set Explicit UPN in Active Directory, open the **Advanced Tuning** page, and set the attribute *REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\UseExplicitUPN* to 1.

Support for Boolean Attributes

Cisco ISE supports retrieving Boolean attributes from Active Directory and LDAP identity stores.

You can configure the Boolean attributes while configuring the directory attributes for Active Directory or LDAP. These attributes are retrieved upon authentication with Active Directory or LDAP.

The Boolean attributes can be used for configuring policy rule conditions.

The Boolean attribute values are fetched from Active Directory or LDAP server as String type. Cisco ISE supports the following values for the Boolean attributes:

Boolean attribute	Supported values
True	t, T, true, TRUE, True, 1
False	f, F, false, FALSE, False, 0

Note Attribute substitution is not supported for the Boolean attributes.

If you configure a Boolean attribute (for example, msTSAllowLogon) as String type, the Boolean value of the attribute in the Active Directory or LDAP server will be set for the String attribute in Cisco ISE. You can change the attribute type to Boolean or add the attribute manually as Boolean type.

Active Directory Certificate Retrieval for Certificate-Based Authentication

Cisco ISE supports certificate retrieval for user and machine authentication that uses the EAP-TLS protocol. The user or machine record on Active Directory includes a certificate attribute of the binary data type. This certificate attribute can contain one or more certificates. Cisco ISE identifies this attribute as userCertificate and does not allow you to configure any other name for this attribute. Cisco ISE retrieves this certificate and uses it to perform binary comparison.

The certificate authentication profile determines the field where the username is taken from in order to lookup the user in Active Directory to be used for retrieving certificates, for example, Subject Alternative Name (SAN) or Common Name. After Cisco ISE retrieves the certificate, it performs a binary comparison of this certificate with the client certificate. When multiple certificates are received, Cisco ISE compares the certificates to check for one that matches. When a match is found, the user or machine authentication is passed.

Active Directory User Authentication Process Flow

When authenticating or querying a user, Cisco ISE checks the following:

- MS-CHAP and PAP authentications check if the user is disabled, locked out, expired or out of logon hours and the authentication fails if any of these conditions are true.
- EAP-TLS authentications checks if the user is disabled or locked out and the authentication fails if any of these conditions are met.

Configure Resource Owner Password Credentials Flow to Authenticate Users with Microsoft Entra ID

Caution The Resource Owner Password Credentials (ROPC) flow in Cisco ISE is a controlled introduction feature. We recommend that you thoroughly test this feature in a test environment before using it in a production environment.

Resource Owner Password Credentials (ROPC) is an OAuth 2.0 grant type that allows Cisco ISE to carry out authorization and authentication in a network with cloud-based identity providers.

Using the ROPC flow, Cisco ISE validates a user's credentials with a cloud-based identity source. The ROPC flow supports plaintext authentication protocols.

Cisco ISE currently supports Microsoft Entra ID through the ROPC flow.

Configure an Application for Resource Owner Password Credentials Flow in Microsoft Entra ID

Step 1 Log in to the Azure portal.

Step 2 Click the **Directory+Application** filter icon in the top navigation bar. Choose the Microsoft Entra ID tenant to which an ROPC-enabled application must be added.

Step 3 Use the search bar to find and choose **App Registrations**.

Step 4 Click **+ New Registration**.

Step 5 In the **Register an Application** window displayed, enter a meaningful name for this app in the **Name** field.

Step 6 In the **Supported account types** area, click **Accounts in this organizational directory only**.

Step 7 Click **Register**.

Step 8 In the new window displayed, click **Certificates & Secrets** from the left menu pane.

Step 9 In the **Client Secrets** area, click **+ New Client Secret**.

Step 10 In the **Add a Client Secret** dialog box displayed, enter a description in the **Description** field.

Step 11 In the **Expiry** area, click **Never**.

Step 12 Click **Add**.

Step 13 Click the copy to clipboard icon to copy the shared secret. You will need this value when configuring the ROPC flow in Cisco ISE.

Step 14 Click **Overview** in the left menu pane, and copy the following values to use in Cisco ISE when configuring the ROPC flow.

- Application (client) ID.
- Directory (tenant) ID.

Step 15 To enable the ROPC flow for this application, click **Authentication** in the left menu pane. In the **Advanced Settings** area, ensure that the toggle button is set to **Yes**.

Step 16 To add a groups claim to the app, click **Token Configuration** in the left menu pane.

Step 17 Click **+ Add Groups Claim**.

Step 18 In the **Edit Groups Claim** dialog box, check the **Security groups** check box.

Step 19 Click **Save**.

Step 20 To enable the use of APIs, click **API Permissions** in the left menu pane.

Step 21 Click **+ Add A Permission**.

Step 22 In the **Microsoft APIs** area, click **Microsoft Graph**.

Step 23 Click **Application Permissions**.

Step 24 In the **Group** drop-down area, check the **Group.Read.All** check box.

Step 25 Click **Add Permissions**.

Step 26 Click **Grant Admin Consent for <user>**, and then click **Yes**.

Configure Resource Owner Password Credentials Flow in Cisco ISE

Before you begin

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **System** > **Certificates** > **Certificate Management** > **Trusted Certificates**. Check if **DigiCert Global Root G2** is displayed in the list trusted certificates.

If this certificate is not available in the Trusted Certificates store, import the public root certificate DigiCert Global Root G2 in PEM format into the Cisco ISE Trusted Certificates store.

See https://www.digicert.com/kb/digicert-root-certificates.htm.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **Settings** > **REST ID Store Settings**.

Step 2 Click **Enabled**, and then click **Submit**.

The message "**The service is starting. This may take a few minutes.**" is displayed on the window while the service is being enabled. The message "**The service is enabled**" is displayed on the window to indicate that the service is active.

Step 3 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **REST (ROPC)**.

Step 4 Click **Add**.

Step 5 In the new window displayed, in the **General** tab, enter a value in the **Name** field.

Step 6 From the **REST Identity Provider** drop-down list, choose the identity source to be configured.

Step 7 Enter the required values for the fields **Client ID**, **Client Secret**, and **Tenant ID**, from the information saved when configuring Microsoft Entra ID in the preceding task.

Step 8 Click **Test Connection** to check if Cisco ISE is able to connect to the chosen identity source.

Step 9 Click **Submit**.

Step 10 To add a REST identity store group, choose the **Groups** tab and click **Load Groups** to import user groups from the connected identity source. You can then choose a specific group from the **Groups** drop-down list.

Step 11 (Optional) Enter a value in the **Username Suffix** field to authenticate the users of a Microsoft Entra ID tenant by their user names.

For example, if the Azure Active Directory User Private Name (UPN) of a user is *example@myTest.onMicrosoft.com*, the suffix is the separator and the domain name is *@myTest.onMicrosoft.com*.

Step 12 Click **Submit**.

Support for Active Directory Multidomain Forests

Cisco ISE supports Active Directory with multidomain forests. Within each forest, Cisco ISE connects to a single domain, but can access resources from the other domains in the Active Directory forest if trust relationships are established between the domain to which Cisco ISE is connected and the other domains.

Refer to Release Notes for Cisco Identity Services Engine for a list of Windows Server Operating Systems that support Active Directory services.

Note Cisco ISE does not support Microsoft Active Directory servers that reside behind a network address translator and have a Network Address Translation (NAT) address.

Prerequisites for Integrating Active Directory and Cisco ISE

This section describes the manual steps required to configure Active Directory for integration with Cisco ISE. However, in most cases, you can enable Cisco ISE to automatically configure Active Directory. The following are the prerequisites to integrate Active Directory with Cisco ISE.

- Ensure you have Active Directory Domain Admin credentials, required to make changes to any of the AD domain configurations.
- Ensure you have the privileges of a Super Admin or System Admin in Cisco ISE.
- Use the Network Time Protocol (NTP) server settings to synchronize the time between the Cisco ISE server and Active Directory. You can configure NTP settings from Cisco ISE CLI.
- Cisco ISE can connect with multiple Active Directory domains that do not have a two-way trust or have zero trust between them. If you want to query other domains from a specific join point, ensure that trust relationships exist between the join point and the other domains that have user and machine information to which you need access. If trust relationships does not exist, you must create another join point to the untrusted domain. For more information on establishing trust relationships, refer to Microsoft Active Directory documentation.
- You must have at least one global catalog server operational and accessible by Cisco ISE, in the domain to which you are joining Cisco ISE.

Active Directory Account Permissions Required to Perform Various Operations

Join Operations	Leave Operations	Cisco ISE Machine Accounts
The join operation requires the following account permissions: • Search Active Directory (to see if a Cisco ISE machine account exists) • Create Cisco ISE machine account to domain (if the machine account does not already exist) • Set attributes on the new machine account (for example, Cisco ISE machine account password, SPN, dnsHostname)	The leave operation requires the following account permissions: • Search Active Directory (to see if a Cisco ISE machine account exists) • Remove the Cisco ISE machine account from the domain If you perform a force leave (leave without the password), it will not remove the machine account from the domain.	The ISE machine account that communicates to the Active Directory connection requires the following permissions: • Change password • Read the user and machine objects corresponding to users and machines that are authenticated • Query Active Directory to get information (for example, trusted domains, alternative UPN suffixes, and so on) • Read the tokenGroups attribute You can precreate the machine account in Active Directory. If the SAM name matches the Cisco ISE appliance hostname, it is located during the join operation and re-used. If there are multiple join operations, multiple machine accounts are maintained inside Cisco ISE, one for each join.

Note The credentials that are used for the join or leave operation are not stored in Cisco ISE. Only the newly created Cisco ISE machine account credentials are stored.

The **Network access: Restrict clients allowed to make remote calls to SAM** security policy in Microsoft Active Directory has been revised. Hence, Cisco ISE might not able to update its machine account password every 15 days. If the machine account password is not updated, Cisco ISE will no longer authenticate users through Microsoft Active Directory. You will receive the **AD: ISE password update failed** alarm on your Cisco ISE dashboard to notify you of this event.

Note This issue happens in Windows Server 2016 Active Directory or later and Windows 10 version 1607 due to the restriction in them. To overcome this restriction, when you are integrating Windows Server 2016 Active Directory or later or Windows 10 version 1607 with Cisco ISE, you much set the registry value in the following registry from non-zero to blank to give access to all: Registry:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictremotesam This allows Cisco ISE to update its machine account password.

The security policy allows users to enumerate users and groups in the local Security Accounts Manager (SAM) database and in Microsoft Active Directory. To ensure Cisco ISE can update its machine account password, check that your configurations in Microsoft Active Directory are accurate. For more information on the Windows operating systems and Windows Server versions affected, what this means for your network, and what changes may be needed, see:

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls

Network Ports that Must Be Open for Communication

Protocol	Port (remote-local)	Target	Authenticated	Notes
DNS (TCP/UDP)	Random number greater than or equal to 49152	DNS Servers/AD Domain Controllers	No	—
MSRPC	445	Domain Controllers	Yes	—
Kerberos (TCP/UDP)	88	Domain Controllers	Yes (Kerberos)	MS AD/KDC
LDAP (TCP/UDP)	389	Domain Controllers	Yes	—
LDAP (GC)	3268	Global Catalog Servers	Yes	—
NTP	123	NTP Servers/Domain Controllers	No	—
IPC	80	Other ISE Nodes in the Deployment	Yes (Using RBAC credentials)	—

DNS Server

While configuring your DNS server, make sure that you take care of the following:

- The DNS servers that you configure in Cisco ISE must be able to resolve all forward and reverse DNS queries for the domains that you want to use.
- The Authoritative DNS server is recommended to resolve Active Directory records, as DNS recursion can cause delays and have significant negative impact on performance.
- All DNS servers must be able to answer SRV queries for DCs, GCs, and KDCs with or without additional Site information.
- Cisco recommends that you add the server IP addresses to SRV responses to improve performance.
- Avoid using DNS servers that query the public Internet. They can leak information about your network when an unknown name has to be resolved.

Configure Active Directory as an External Identity Source

Configure Active Directory as an external identity source as part of the configuration for features such as Easy Connect and the PassiveID Work Center. For more information about these features, see Easy Connect, on page 679 and PassiveID Work Center , on page 683.

Before you configure Active Directory as an External Identity Source, make sure that:

- The Microsoft Active Directory server does not reside behind a network address translator and does not have a Network Address Translation (NAT) address.
- The Microsoft Active Directory account intended for the join operation is valid and is not configured with the Change Password on Next Login.
- You have the privileges of a Super Admin or System Admin in ISE.

Note If you see operational issues when Cisco ISE is connected to Active Directory, see the AD Connector Operations Report under **Operations** > **Reports**.

You must perform the following tasks to configure Active Directory as an external identity source.

1. Add an Active Directory Join Point and Join Cisco ISE Node to the Join Point, on page 651
2. Configure Authentication Domains, on page 656
3. Configure Active Directory User Groups, on page 657
4. Configure Active Directory User and Machine Attributes, on page 658
5. (Optional) Modify Password Changes, Machine Authentications, and Machine Access Restriction Settings, on page 658

Add an Active Directory Join Point and Join Cisco ISE Node to the Join Point

Before you begin

Ensure that the Cisco ISE node can communicate with the networks where the NTP servers, DNS servers, domain controllers, and global catalog servers are located. You can check these parameters by running the Domain Diagnostic tool.

Join points must be created in order to work with Active Directory as well as with the Agent, Syslog, SPAN and Endpoint probes of the Passive ID Work Center.

If you want to use IPv6 when integrating with Active Directory, then you must ensure that you have configured an IPv6 address for the relevant ISE nodes.

If you use the Google Chrome browser and have ad blocking software enabled, you must disable the ad blocker. This task contains Cisco ISE GUI elements that are affected by ad blockers. Alternatively, you can carry out this task in a Google Chrome Incognito browser.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

Step 2 Click **Add** and enter the domain name and identity store name from the **Active Directory Join Point Name** settings.

Step 3 Click **Submit**.

A pop-up appears asking if you want to join the newly created join point to the domain. Click **Yes** if you want to join immediately.

If you clicked **No**, then saving the configuration saves the Active Directory domain configuration globally (in the primary and secondary policy service nodes), but none of the Cisco ISE nodes are joined to the domain yet.

Step 4 Check the check box next to the new Active Directory join point that you created and click **Edit**, or click on the new Active Directory join point from the navigation pane on the left. The deployment join/leave table is displayed with all the Cisco ISE nodes, the node roles, and their status.

Step 5 In case the join point was not joined to the domain during Step 3, check the check box next to the relevant Cisco ISE nodes and click **Join** to join the Cisco ISE node to the Active Directory domain.

You must do this explicitly even though you saved the configuration. To join multiple Cisco ISE nodes to a domain in a single operation, the username and password of the account to be used must be the same for all join operations. If different username and passwords are required to join each Cisco ISE node, the join operation should be performed individually for each Cisco ISE node.

Step 6 Enter the Active Directory username and password in the **Join Domain** dialog box.

It is strongly recommended that you choose **Store credentials**, in which case your administrator's user name and password will be saved in order to be used for all Domain Controllers (DC) that are configured for monitoring.

The user used for the join operation should exist in the domain itself. If it exists in a different domain or subdomain, the username should be noted in a UPN notation, such as jdoe@acme.com.

Step 7 (Optional) Check the **Specify Organizational Unit** check box.

You should check this check box in case the Cisco ISE node machine account is to be located in a specific Organizational Unit other than CN=Computers,DC=someDomain,DC=someTLD. Cisco ISE creates the machine account under the specified organizational unit or moves it to this location if the machine account already exists. If the organizational unit is not specified, Cisco ISE uses the default location. The value should be specified in full distinguished name (DN) format. The syntax must conform to the Microsoft guidelines. Special reserved characters, such as /'+,;=<> line feed, space, and carriage return must be escaped by a backslash (\). For example, OU=Cisco ISE\,US,OU=IT Servers,OU=Servers\, and Workstations,DC=someDomain,DC=someTLD. If the machine account is already created, you need not check this check box. You can also change the location of the machine account after you join to the Active Directory domain.

Step 8 Click **OK**.

You can select more than one node to join to the Active Directory domain.

If the join operation is not successful, a failure message appears. Click the failure message for each node to view detailed logs for that node.

Note the following points while configuring the join points:

- When using multiple join points, if alternate UPN suffix is configured only for a single join point or domain, identity lookup is performed only in that join point or domain. Authentication might fail in such cases. As a workaround, you can configure the alternate UPN suffix for all the joint points or domains.
- You can only add up to 200 Domain Controllers on ISE. On exceeding the limit, you will receive the error "Error creating <*DC FQDN*> - Number of DCs Exceeds allowed maximum of 200". For more

information on the tested scale limit of domain controllers for deployment, see Performance and Scalability Guide for Cisco Identity Services Engine.

- When the join is complete, Cisco ISE updates its AD groups and corresponding security identifiers (SIDs). Cisco ISE automatically starts the SID update process. You must ensure that this process is allowed to complete.
- You might not be able to join Cisco ISE with an Active Directory domain if the DNS service (SRV) records are missing (the domain controllers do not advertise their SRV records for the domain that you are trying to join to).
- The AD machine account name that is created will not match the Cisco ISE hostname if the hostname contains more than 15 characters. In this case, the machine account name will be created in the following format:

  first_8_characters_of(hostname) + "-" + 6 random characters + "$"

  For the machine account name and the hostname to match, the hostname must have 15 characters or less.
- Even if the AD credentials used to join Cisco ISE and AD are no longer valid, the join point between Cisco ISE and AD remains unchanged.

Add Domain Controllers

Step 1 Choose **Work Centers** > **PassiveID** > **Providers** and then from the left panel choose **Active Directory**.

Step 2 Check the check box next to the Active Directory join point that you created and click **Edit**. The deployment join/leave table is displayed with all the Cisco ISE nodes, the node roles, and their statuses.

Step 3 **Note** To add a new Domain Controller (DC) for Passive Identity services, you need the login credentials of that DC.

Go to the PassiveID tab and click **Add DCs**.

Step 4 Check the check box next to the domain controllers that you would like to add to the join point for monitoring and click **OK**.
The domain controllers appear in the Domain Controllers list of the PassiveID tab.

Step 5 Configure the domain controller:

a) Checkmark the domain controller and click **Edit**. The **Edit Item** screen appears.
b) Optionally, edit the different domain controller fields.

The DC failover mechanism is managed based on the DC priority list, which determines the order in which the DCs are selected in case of failover. If a DC is offline or not reachable due to some error, its priority is decreased in the priority list. When the DC comes back online, its priority is adjusted accordingly (increased) in the priority list.

MSRPC Protocol for Passive ID

From Cisco ISE Release 3.0 onwards, you can use MS-Eventing API or Microsoft Remote Procedure Call (MSRPC) protocol for Passive Identity. MSRPC protocol is used to establish node communication and monitor heartbeats between nodes in Cisco ISE.

MSRPC protocol promotes a reliable mechanism when Cisco ISE or Cisco ISE-PIC collects or monitors the events from several domain controllers. It also reduces latency on the domain controller user logon events.

For Cisco ISE 3.0 and later, MSRPC is the default protocol. We recommend that you enable the primary and secondary agent for high availability functionalities of the MSPRC, so that if there is a failure in the primary agent installed server, the secondary agent becomes active and monitors the domain controller.

You can also choose to use the standalone option for MSPRC while creating an agent. However, the standalone agent will not be backed up by a secondary agent, in case of agent failure and the domain controller events cannot be monitored.

While upgrading from Cisco ISE 2.x to 3.0 version, if the member server is updated with existing agents, the agent version is displayed as 2.0.0.1 in the **Version** column in the **Agents** window. To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Passive ID** > **Providers > Agents** .

When the agent is installed on the domain controller directly, ensure that the monitoring user is a member of the Event Log Readers group.

When the agent is installed on the AD domain member server, you must do the following:

- Ensure that the monitoring user is a member of the Event Log Readers group.
- If you have configured high availability, open UDP port 9095 in the firewall between the server pair.
- Ensure that the DNS servers configured in Cisco ISE are able to resolve the forward (A) and reverse (PTR) records of the Windows member servers. You must add the required details, if missing.

Irrespective of whether the agent is installed directly on the server or a member server, enable the following firewall rules for Remote Event Log Management group on the domain controller, to allow the server to access the event logs of the domain controller.

- Remote Event Log Management (NP-in)
- Remote Event Log Management (RPC)
- Remote Event Log Management (RPC-EPMAP)

If this is done after the agent is installed, you must restart the agent service on the server.

Deploy Agents for MSRPC

Before you begin

You must enable the Passive Identity Service. To do this:

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment** and check the check box adjacent to the deployment node. Click **Edit**. In the **Edit Node** window, check the **Enable Passive Identity Service** check box and click **Save**.

In the Cisco ISE-PIC GUI, choose **Administration** > **System** > **Deployment** and check the check box adjacent to the deployment node. Click **Edit**. In the **Edit Node** window, check the **Enable Passive Identity Service** check box and click **Save**.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Passive ID** > **Providers** > **Agents**.

Step 2 Click **Add**.

Step 3 In the **Agents** window, click **Deploy New Agent**, if you want to deploy new agents or click **Register Existing Agents**, if you want to register an existing agent.

If you choose the **Register Existing Agent** option, a request from a supported registered client may be dropped due to the unsupported protocol. In such events, you need to configure the Cisco ISE client with a supported protocol.

Step 4 Enter the agent name in the **Name** field.

Step 5 Enter the Host FQDN URL in the **Host FQDN** field.

Step 6 Enter the **User Name** and **Password**.

The user account must have the permission to connect remotely to install the PIC agent.

Step 7 Choose **MSRPC** from the **Protocol** dropdown list.

Step 8 Click **Primary** in the **High Availability Settings** section.

After the primary agent is successfully deployed, the above steps should be repeated to deploy the secondary agents by selecting the **Secondary** option in the **High Availability Settings** section. While deploying the secondary agent, select the configured primary agent from the **Primary Agent** drop-down list.

Step 9 Click **Deploy**.

Map Domain Controller with Primary Agent

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **PassiveID** > **Providers** > **Active Directory**.

Step 2 In the **Active Directory** window, click **Add**.

Step 3 In the **Connection** section, enter the **Join Point Name** and **Active Directory Domain** for the domain controller.

Step 4 Click **Submit**.

The following message is displayed:

```
Would you like to Join all ISE Nodes to this Active Directory Domain?
```

Step 5 Click **Yes** to join all the ISE nodes.

Step 6 In the **Join Domain** pop-up window, enter the **AD User name** and **Password**.

Step 7 Click **Ok**.

Step 8 Click the **PassiveID** tab.

Step 9 In the **PassiveID Domain Controllers** window, click the check box adjacent to the ISE domain you want to map.

For multiple DC mapping, you can choose the existing agent from the **Use Existing Agent** option.

Step 10 Click **Edit**

Step 11 Enter the Host FQDN URL in the **Host FQDN** field.

Step 12 Enter the AD credentials in the **AD User Name** and **Password** fields. The user account must have the permission to read the security events on the domain controller.

Step 13 Choose **Agent** from the **Protocol** drop-down list.

Step 14 Select the corresponding agent (**Primary** for high availability or **Standalone**) from the **Agent** drop-down list.

Step 15 Click **Save**.

You can review the agent mapping status, the agent monitoring the domain controller and the agent role in the **Dashboard**. To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **PassiveID** > **Overview**.

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **RADIUS** > **Live Sessions** to view the domain controller event logs.

Leave the Active Directory Domain

If you no longer need to authenticate users or machines from this Active Directory domain or from this join point, you can leave the Active Directory domain.

When you reset the Cisco ISE application configuration from the command-line interface or restore configuration after a backup or upgrade, it performs a leave operation, disconnecting the Cisco ISE node from the Active Directory domain, if it is already joined. However, the Cisco ISE node account is not removed from the Active Directory domain. We recommend that you perform a leave operation from the Admin portal with the Active Directory credentials because it also removes the node account from the Active Directory domain. This is also recommended when you change the Cisco ISE hostname.

Before you begin

If you leave the Active Directory domain, but still use Active Directory as an identity source for authentication (either directly or as part of an identity source sequence), authentications may fail.

Step 1 Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

Step 2 Check the checkbox next to the Active Directory join point that you created and click **Edit**. The deployment join/leave table is displayed with all the Cisco ISE nodes, the node roles, and their statuses.

Step 3 Check the checkbox next to the Cisco ISE node and click **Leave**.

Step 4 Enter the Active Directory username and password, and click **OK** to leave the domain and remove the machine account from the Cisco ISE database.

If you enter the Active Directory credentials, the Cisco ISE node leaves the Active Directory domain and deletes the Cisco ISE machine account from the Active Directory database.

Note To delete the Cisco ISE machine account from the Active Directory database, the Active Directory credentials that you provide here must have the permission to remove machine account from domain.

Step 5 If you do not have the Active Directory credentials, check the **No Credentials Available** checkbox, and click **OK**.

If you check the **Leave domain without credentials** checkbox, the primary Cisco ISE node leaves the Active Directory domain. The Active Directory administrator must manually remove the machine account that was created in Active Directory during the time of the join.

Configure Authentication Domains

The domain to which Cisco ISE is joined to has visibility to other domains with which it has a trust relationship. By default, Cisco ISE is set to permit authentication against all those trusted domains. You can restrict interaction with the Active Directory deployment to a subset of authentication domains. Configuring authentication domains enables you to select specific domains for each join point so that the authentications are performed against the selected domains only. Authentication domains improves security because they instruct Cisco ISE to authenticate users only from selected domains and not from all domains trusted from join point. Authentication domains also improve performance and latency of authentication request processing because authentication domains limit the search area (that is, where accounts matching to incoming username or identity will be searched). It is especially important when incoming username or identity does not contain domain markup (prefix or suffix). Due to these reasons, configuring authentication domains is a best practice, and we highly recommended it.

Step 1 Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

Step 2 Click **Active Directory** join point.

Step 3 Click the **Authentication Domains** tab.

A table appears with a list of your trusted domains. By default, Cisco ISE permits authentication against all trusted domains.

Step 4 To allow only specified domains, uncheck **Use all Active Directory domains for authentication** check box.

Step 5 Check the check box next to the domains for which you want to allow authentication, and click **Enable Selected**. In the **Authenticate** column, the status of this domain changes to Yes.

You can also disable selected domains.

Step 6 Click **Show Unusable Domains** to view a list of domains that cannot be used. Unusable domains are domains that Cisco ISE cannot use for authentication due to reasons such as one-way trust, selective authentication and so on.

What to do next

Configure Active Directory user groups.

Configure Active Directory User Groups

You must configure Active Directory user groups for them to be available for use in authorization policies. Internally, Cisco ISE uses security identifiers (SIDs) to help resolve group name ambiguity issues and to enhance group mappings. SID provides accurate group assignment matching.

Step 1 Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

Step 2 Click the **Groups** tab.

Step 3 Do one of the following:

a) Choose **Add** > **Select Groups From Directory** to choose an existing group.

b) Choose **Add** > **Add Group** to manually add a group. You can either provide both group name and SID or provide only the group name and press **Fetch SID**.

Do not use double quotes (”) in the group name for the user interface login.

Step 4 If you are manually selecting a group, you can search for them using a filter. For example, enter **admin*** as the filter criteria and click **Retrieve Groups** to view user groups that begin with admin. You can also enter the asterisk (*) wildcard character to filter the results. You can retrieve only 500 groups at a time.

Step 5 Check the check boxes next to the groups that you want to be available for use in authorization policies and click **OK**.

Step 6 If you choose to manually add a group, enter a name and SID for the new group.

Step 7 Click **OK**.

Step 8 Click **Save**.

Note If you delete a group and create a new group with the same name as original, you must click **Update SID Values** to assign new SID to the newly created group. After an upgrade, the SIDs are automatically updated after the first join.

What to do next

Configure Active Directory user attributes.

Configure Active Directory User and Machine Attributes

You must configure Active Directory user and machine attributes to be able to use them in conditions in authorization policies.

Step 1 Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

Step 2 Click the **Attributes** tab.

Step 3 Choose **Add** > **Add Attribute** to manually add a attribute, or choose **Add** > **Select Attributes From Directory** to choose a list of attributes from the directory.

Cisco ISE allows you to configure the AD with IPv4 or IPv6 address for user authentication when you manually add the attribute type IP.

Step 4 If you choose to add attributes from the directory, enter the name of a user in the **Sample User or Machine Account** field, and click **Retrieve Attributes** to obtain a list of attributes for users. For example, enter **administrator** to obtain a list of administrator attributes. You can also enter the asterisk (*) wildcard character to filter the results.

Note When you enter an example username, ensure that you choose a user from the Active Directory domain to which the Cisco ISE is connected. When you choose an example machine to obtain machine attributes, be sure to prefix the machine name with "host/" or use the SAM$ format. For example, you might use host/myhost. The example value displayed when you retrieve attributes are provided for illustration only and are not stored.

Step 5 Check the check boxes next to the attributes from Active Directory that you want to select, and click **OK**.

Step 6 If you choose to manually add an attribute, enter a name for the new attribute.

Step 7 Click **Save**.

Modify Password Changes, Machine Authentications, and Machine Access Restriction Settings

Before you begin

You must join Cisco ISE to the Active Directory domain. For more information, see Add an Active Directory Join Point and Join Cisco ISE Node to the Join Point, on page 651.

Step 1 Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

Step 2 Check the check box next to the relevant Cisco ISE node and click **Edit** .

Step 3 Click the **Advanced Settings** tab.

Step 4 Modify as required, the Password Change, Machine Authentication, and Machine Access Restrictions (MARs) settings.

Step 5 Check the **Enable dial-in check** check box to check the dial-in permissions of the user during authentication or query. The result of the check can cause a reject of the authentication in case the dial-in permission is denied.

Step 6 Check the **Enable callback check for dial-in clients** check box if you want the server to call back the user during authentication or query. The IP address or phone number used by the server can be set either by the caller or the network administrator. The result of the check is returned to the device on the RADIUS response.

Step 7 Check the **Use Kerberos for Plain Text Authentications** check box if you want to use Kerberos for plain-text authentications. The default and recommended option is MS-RPC.

Configure Maximum Password Attempts for Active Directory Account

A Cisco ISE admin needs a mechanism to prevent Active Directory account lockout because of too many bad password attempts. You can configure the Bad Password Count attribute to prevent a lockout. Before sending the authentication to Active Directory, Cisco ISE should check if there are enough attempts left.

Before authenticating a user, Cisco ISE compares the maximum bad password attempts configured in Cisco ISE with the current value of the badPwdCount attribute on the Active Directory. When the maximum bad password attempts configured in Cisco ISE is equal to the value of the badPwdCount attribute, the authentication is dropped and not sent to the Active Directory.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

Step 2 Check the check box next to the relevant Cisco ISE node and click **Edit** .

Step 3 Click the **Advanced Settings** tab.

Step 4 In the **Prevent Active Directory User Lockout** section, check the **Enable Failed Authentication Protection** check box.

Step 5 Enter the number of maximum bad password attempts.

Note The maximum password attempts here should be less than the maximum bad password attempts configured as the value of the badPwdCount attribute in the Active Directory.

Step 6 Check the **Wired** and **Wireless** check boxes as per the connection requests, for authentication.

Note The connection type (Wired or Wireless) is derived from the RADIUS NAS-port-type attribute. The NAD must include the correct value for this Radius attribute in the Access-request message for this feature to function.

Step 7 Click **Save**.

Step 8 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Sets** > **Default** > **Authentication Policy**.

Step 9 For the required **Rule Name**, **Use** the Active Directory configured as the Identity Source.

Note Identity Sequence Scope or Active Directory Scope will not work. Make sure you use the specific Active Directory join point.

Step 10 Click **Save**.

Step 11 The same can be configured for Guest Portals as well.

Step 12 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Identities** > **Identity Source Sequences** > **Add**.

Step 13 Enter the **Name** of the Identity Source Sequence.

Step 14 In the **Authentication Search List** section, use the > button to move the identity sources from the **Available** pane to the **Selected** pane.

Note Identity Sequence Scope or Active Directory Scope will not work. Make sure that you use the specific Active Directory join point. It uses only the first Active Directory join point that has this capability enabled. If this capability is enabled on more than one join point, only the first join point in the list is checked.

Step 15 Click **Submit**.

Troubleshooting

Issue 1: User is locked in Active Directory.

Solution: Ask the network administrator to reset the badPwdCount attribute for that user on the Active Directory.

Issue 2: User fails authentication in Active Directory while lockout prevention is enabled for that Active Directory.

Solution: Check or perform the following:

- Ensure that the User account exists in the Active Directory.
- The badPwdCount attribute value for the user account in the Active Directory must be less than the maximum bad password attempts configured in Cisco ISE.
- Authenticate using the unselected connection type. If lockout prevention is set to Wireless, try to authenticate using Wired connection and vice versa. Successful authentication resets the badPwdCount attribute in the Active Directory .
- Ask the network administrator to reset the badPwdCount attribute for the user in the Active Directory.

Issue 3: User gets locked out even when the lockout prevention for Active Directory is enabled.

Solution: Ensure that the maximum bad password attempts configured in Cisco ISE is less than the value of the badPwdCount attribute set in the Active Directory.

Issue 4: User fails authentication in Active Directory in a portal flow while lockout prevention is enabled for that Active Directory.

Solution: Check or perform the following:

- Make sure that the relevant Active Directory instance is part of the identity store (not sequence) used for that portal flow.
- Ensure that the user account exists in the Active Directory.
- The badPwdCount attribute value for the user account in the Active Directory must be less than the maximum bad password attempts configured in Cisco ISE.
- Try authenticating using the unselected connection type. If lockout prevention is set to Wireless, try to authenticate using Wired connection and vice versa. Successful authentication resets the badPwdCount attribute in the Active Directory.
- Ask the network administrator to reset the badPwdCount attribute for the user in the Active Directory.

Machine Access Restriction Cache

Cisco ISE stores the Machine Access Restriction (MAR) cache content, calling-station-ID list, and the corresponding time stamps to a file on its local disk when you manually stop the the application services. Cisco ISE does not store the MAR cache entries of an instance when there is an accidental restart of the application services. Cisco ISE reads the MAR cache entries from the file on its local disk based on the cache entry time to live when the application services restart. When the application services come up after a restart, Cisco ISE compares the current time of that instance with the MAR cache entry time. If the difference between the current time and the MAR entry time is greater than the MAR cache entry time to live, then Cisco ISE does not retrieve that entry from disk. Otherwise, Cisco ISE retrieves that MAR cache entry and updates its MAR cache entry time to live.

To Configure MAR Cache

On **Advanced Settings** tab of the Active Directory defined in External Identity Sources, verify that the following options are checked:

- **Enable Machine Authentication**: To enable machine authentication.
- **Enable Machine Access Restriction**: To combine user and machine authentication before authorization.

To Use MAR Cache in Authorization

Use `WasMachineAuthenticated is True` in an authorization policy. You can use this rule plus a credentials rule to do dual-authentication. Machine authentication must be done before AD credentials.

If you created a Node Group on the **System > Deployment** page, enable MAR Cache Distribution. MAR cache distribution replicates the MAR cache to all the PSNs in the same node group.

For more information, see the following Cisco ISE Community pages:

- https://community.cisco.com/t5/policy-and-access/mar-why-is-it-useful/td-p/3213527
- https://community.cisco.com/t5/policy-and-access/ise-2-1-mar-aging-time-eap-tls/td-p/3209628

Related Topics

Configure Active Directory as an External Identity Source, on page 651

Configure Custom Schema

Before you begin

You must join Cisco ISE to the Active Directory domain.

Step 1 Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

Step 2 Select the Join point.

Step 3 Click the **Advanced Settings** tab.

Step 4 Under the **Schema** section, select the **Custom** option from the **Schema** drop-down list. You can update the user information attributes based on your requirements. These attributes are used to collect user information, such as, first name, last name, email, telephone, locality, and so on.

Predefined attributes are used for the Active Directory schema (built-in schema). If you edit the attributes of the predefined schema, Cisco ISE automatically creates a custom schema.

Support for Active Directory Multijoin Configuration

Cisco ISE supports multiple joins to Active Directory domains. Cisco ISE supports up to 50 Active Directory joins. Cisco ISE can connect with multiple Active Directory domains that do not have a two-way trust or have zero trust between them. Active Directory multi-domain join comprises a set of distinct Active Directory domains with their own groups, attributes, and authorization policies for each join.

You can join the same forest more than once, that is, you can join more than one domain in the same forest, if necessary.

Cisco ISE now allows to join domains with one-way trust. This option helps bypass the permission issues caused by a one-way trust. You can join either of the trusted domains and hence be able to see both domains.

- Join Point: In Cisco ISE, each independent join to an Active Directory domain is called a join point. The Active Directory join point is an Cisco ISE identity store and can be used in authentication policy. It has an associated dictionary for attributes and groups, which can be used in authorization conditions.
- Scope: A subset of Active Directory join points grouped together is called a scope. You can use scopes in authentication policy in place of a single join point and as authentication results. Scopes are used to authenticate users against multiple join points. Instead of having multiple rules for each join point, if you use a scope, you can create the same policy with a single rule and save the time that Cisco ISE takes to process a request and help improve performance. A join point can be present in multiple scopes. A scope can be included in an identity source sequence. You cannot use scopes in an authorization policy condition because scopes do not have any associated dictionaries.

  When you perform a fresh Cisco ISE install, by default no scopes exist. This is called the no scope mode. When you add a scope, Cisco ISE enters multi-scope mode. If you want, you can return to no scope mode. All the join points will be moved to the Active Directory folder.

  - Initial_Scope is an implicit scope that is used to store the Active Directory join points that were added in no scope mode. When multi-scope mode is enabled, all the Active Directory join points move into the automatically created Initial_Scope. You can rename the Initial_Scope.
  - All_AD_Instances is a built-in pseudo scope that is not shown in the Active Directory configuration. It is only visible as an authentication result in policy and identity sequences. You can select this scope if you want to select all Active Directory join points configured in Cisco ISE.

Create a New Scope to Add Active Directory Join Points

Step 1 Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

Step 2 Click **Scope Mode**.
A default scope called Initial_Scope is created, and all the current join points are placed under this scope.

Step 3 To create more scopes, click **Add**.

Step 4 Enter a name and a description for the new scope.

Step 5 Click **Submit**.

Identity Rewrite

Identity rewrite is an advanced feature that directs Cisco ISE to manipulate the identity before it is passed to the external Active Directory system. You can create rules to change the identity to a desired format that includes or excludes a domain prefix and/or suffix or other additional markup of your choice.

Identity rewrite rules are applied on the username or hostname received from the client, before being passed to Active Directory, for operations such as subject searches, authentication, and authorization queries. Cisco ISE will match the condition tokens and when the first one matches, Cisco ISE stops processing the policy and rewrites the identity string according to the result.

During the rewrite, everything enclosed in square bracket [ ] (such as [IDENTITY]) is a variable that is not evaluated on the evaluation side but instead added with the string that matches that location in the string. Everything without the brackets is evaluated as a fixed string on both the evaluation side and the rewrite side of the rule.

The following are some examples of identity rewrite, considering that the identity entered by the user is ACME\jdoe:

- If identity matches **ACME\[IDENTITY]**, rewrite as **[IDENTITY]**.

  The result would be jdoe. This rule instructs Cisco ISE to strip all usernames with the ACME prefix.

- If the identity matches **ACME\[IDENTITY]**, rewrite as **[IDENTITY]@ACME.com**.

  The result would be jdoe@ACME.com. This rule instructs Cisco ISE to change the format from prefix for suffix notation or from NetBIOS format to UPN formats.

- If the identity matches **ACME\[IDENTITY]**, rewrite as **ACME2\[IDENTITY]**.

  The result would be ACME2\jdoe. This rule instructs Cisco ISE to change all usernames with a certain prefix to an alternate prefix.

- If the identity matches **[ACME]\jdoe.USA**, rewrite as **[IDENTITY]@[ACME].com**.

  The result would be jdoe\ACME.com. This rule instructs Cisco ISE to strip the realm after the dot, in this case the country and replace it with the correct domain.

- If the identity matches **E=[IDENTITY]**, rewrite as **[IDENTITY]**.

  The result would be jdoe. This is an example rule that can be created when an identity is from a certificate, the field is an email address, and Active Directory is configured to search by Subject. This rule instructs Cisco ISE to remove ‘E=’.

- If the identity matches **E=[EMAIL],[DN]**, rewrite as **[DN]**.

  This rule will convert certificate subject from E=jdoe@acme.com, CN=jdoe, DC=acme, DC=com to pure DN, CN=jdoe, DC=acme, DC=com. This is an example rule that can be created when identity is taken from a certificate subject and Active Directory is configured to search user by DN . This rule instructs Cisco ISE to strip email prefix and generate DN.

The following are some common mistakes while writing the identity rewrite rules:

- If the identity matches **[DOMAIN]\[IDENTITY]**, rewrite as **[IDENTITY]@DOMAIN.com**.

The result would be jdoe@DOMAIN.com. This rule does not have [DOMAIN] in square brackets [ ] on the rewrite side of the rule.

- If the identity matches **DOMAIN\[IDENTITY]**, rewrite as **[IDENTITY]@[DOMAIN].com**.

  Here again, the result would be jdoe@DOMAIN.com. This rule does not have [DOMAIN] in square brackets [ ] on the evaluation side of the rule.

Identity rewrite rules are always applied within the context of an Active Directory join point. Even if a scope is selected as the result of an authentication policy, the rewrite rules are applied for each Active Directory join point. These rewrite rules also applies for identities taken from certificates if EAP-TLS is being used.

Enable Identity Rewrite

Note This configuration task is optional. You can perform it to reduce authentication failures that can arise because of various reasons such as ambiguous identity errors.

Before you begin

You must join Cisco ISE to the Active Directory domain.

Step 1 Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

Step 2 Click the **Advanced Settings** tab.

Step 3 Under the **Identity Rewrite** section, choose whether you want to apply the rewrite rules to modify usernames.

Step 4 Enter the match conditions and the rewrite results. You can remove the default rule that appears and enter the rule according to your requirement. Cisco ISE processes the policy in order, and the first condition that matches the request username is applied. You can use the matching tokens (text contained in square brackets) to transfer elements of the original username to the result. If none of the rules match, the identity name remains unchanged. You can click the **Launch Test** button to preview the rewrite processing.

Identity Resolution Settings

Some type of identities include a domain markup, such as a prefix or a suffix. For example, in a NetBIOS identity such as ACME\jdoe, “ACME” is the domain markup prefix, similarly in a UPN identity such as jdoe@acme.com, “acme.com” is the domain markup suffix. Domain prefix should match to the NetBIOS (NTLM) name of the Active Directory domain in your organization and domain suffix should match to the DNS name of Active Directory domain or to the alternative UPN suffix in your organization. For example jdoe@gmail.com is treated as without domain markup because gmail.com is not a DNS name of Active Directory domain.

The identity resolution settings allows you to configure important settings to tune the security and performance balance to match your Active Directory deployment. You can use these settings to tune authentications for usernames and hostnames without domain markup. In cases when Cisco ISE is not aware of the user's domain, it can be configured to search the user in all the authentication domains. Even if the user is found in one domain, Cisco ISE will wait for all responses in order to ensure that there is no identity ambiguity. This might be a lengthy process, subject to the number of domains, latency in the network, load, and so on.

Avoid Identity Resolution Issues

It is highly recommended to use fully qualified names (that is, names with domain markup) for users and hosts during authentication. For example, UPNs and NetBIOS names for users and FQDN SPNs for hosts. This is especially important if you hit ambiguity errors frequently, such as, several Active Directory accounts match to the incoming username; for example, jdoe matches to jdoe@emea.acme.com and jdoe@amer.acme.com. In some cases, using fully qualified names is the only way to resolve issue. In others, it may be sufficient to guarantee that the users have unique passwords. So, it is more efficient and leads to less password lockout issues if unique identities are used initially.

Configure Identity Resolution Settings

Note This configuration task is optional. You can perform it to reduce authentication failures that can arise because of various reasons such as ambiguous identity errors.

Before you begin

You must join the Cisco ISE node to the Active Directory domain.

Step 1 Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

Step 2 Click the **Advanced Settings** tab.

Step 3 Define the following settings for identity resolution for usernames or machine names under the **Identity Resolution** section. This setting provides you advanced control for user search and authentication.

The first setting is for the identities without a markup. In such cases, you can select any of the following options:

- **Reject the request**: This option will fail the authentication for users who do not have any domain markups, such as a SAM name. This is useful in case of multi join domains where Cisco ISE will have to look up for the identity in all the joined global catalogs, which might not be very secure. This option forces the users to use names with domain markups.
- **Only search in the “Authentication Domains” from the joined forest**: This option will search for the identity only in the domains in the forest of the join point which are specified in the authentication domains section. This is the default option.
- **Search in all the “Authentication Domains” sections**: This option will search for the identity in all authentication domains in all the trusted forests. This might increase latency and impact performance.

The selection is made based on how the authentication domains are configured in Cisco ISE. If only specific authentication domains are selected, only those domains will be searched (for both “joined forest” or “all forests” selections).

The second setting is used if Cisco ISE cannot communicate with all Global Catalogs (GCs) that it needs to in order to comply with the configuration specified in the “Authentication Domains” section. In such cases, you can select any of the following options:

- **Proceed with available domains**: This option will proceed with the authentication if it finds a match in any of the available domains.

- **Drop the request**: This option will drop the authentication request if the identity resolution encounters some unreachable or unavailable domain.

Test Users for Active Directory Authentication

The Test User tool can be used to verify user authentication from Active Directory. You can also fetch groups and attributes and examine them. You can run the test for a single join point or for scopes.

Step 1 Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

Step 2 Choose one of the following options:

- To run the test on all join points, choose **Advanced Tools** > **Test User for All Join Points**.
- To run the test for a specific join point, select the joint point and click **Edit**. Select the Cisco ISE node and click **Test User**.

Step 3 Enter the username and password of the user (or host) in Active Directory.

Step 4 Choose the authentication type. Password entry in Step 3 is not required if you choose the Lookup option.

Step 5 Select the Cisco ISE node on which you want to run this test, if you are running this test for all join points.

Step 6 Check the Retrieve Groups and Attributes check boxes if you want to retrieve the groups and attributes from Active Directory.

Step 7 Click **Test**.
The result and steps of the test operation are displayed. The steps can help to identify the failure reason and troubleshoot.

You can also view the time taken (in milliseconds) for Active Directory to perform each processing step (for authentication, lookup, or fetching groups/attributes). Cisco ISE displays a warning message if the time taken for an operation exceeds the threshold.

Delete Active Directory Configurations

You should delete Active Directory configurations if you are not going to use Active Directory as an external identity source. Do not delete the configuration if you want to join another Active Directory domain. You can leave the domain to which you are currently joined and join a new domain.

Before you begin

Ensure that you have left the Active Directory domain.

Step 1 Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

Step 2 Check the checkbox next to the configured Active Directory.

Step 3 Check and ensure that the Local Node status is listed as Not Joined.

Step 4 Click **Delete**.

You have removed the configuration from the Active Directory database. If you want to use Active Directory at a later point in time, you can resubmit a valid Active Directory configuration.

View Active Directory Joins for a Node

You can use the **Node View** button on the **Active Directory** page to view the status of all Active Directory join points for a given Cisco ISE node or a list of all join points on all Cisco ISE nodes.

Step 1 Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

Step 2 Click **Node View**.

Step 3 Select a node from the **ISE Node** drop-down list.
The table lists the status of Active Directory by node. If there are multiple join points and multiple Cisco ISE nodes in a deployment, this table may take several minutes to update.

Step 4 Click the join point **Name** link to go to that Active Directory join point page and perform other specific actions.

Step 5 Click the link in the **Diagnostic Summary** column to go to the **Diagnostic Tools** page to troubleshoot specific issues. The diagnostic tool displays the latest diagnostics results for each join point per node.

Diagnose Active Directory Problems

The Diagnostic Tool is a service that runs on every Cisco ISE node. It allows you to automatically test and diagnose the Active Directory deployment and execute a set of tests to detect issues that may cause functionality or performance failures when Cisco ISE uses Active Directory.

There are multiple reasons for which Cisco ISE might be unable to join or authenticate against Active Directory. This tool helps ensure that the prerequisites for connecting Cisco ISE to Active Directory are configured correctly. It helps detect problems with networking, firewall configurations, clock sync, user authentication, and so on. This tool works as a step-by-step guide and helps you fix problems with every layer in the middle, if needed .

Step 1 Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

Step 2 Click the **Advanced Tools** drop-down and choose **Diagnostic Tools**.

Step 3 Select a Cisco ISE node to run the diagnosis on.

If you do not select a Cisco ISE node then the test is run on all the nodes.

Step 4 Select a specific Active Directory join point.

If you do not select an Active Directory join point then the test is run on all the join points.

Step 5 You can run the diagnostic tests either on demand or on a scheduled basis.

- To run tests immediately, choose **Run Tests Now**.
- To run the tests at an scheduled interval, check the **Run Scheduled Tests** check box and specify the start time and the interval (in hours, days, or weeks) at which the tests must be run. When this option is enabled, all the diagnostic tests are run on all the nodes and instances and the failures are reported in the **Alarms** dashlet in the **Home** dashboard.

Step 6 Click **View Test Details** to view the details for tests with Warning or Failed status.
This table allows you to rerun specific tests, stop running tests, and view a report of specific tests.

Enable Active Directory Debug Logs

Active Directory debug logs are not logged by default. You must enable this option on the Cisco ISE node that has assumed the Policy Service persona in your deployment. Enabling Active Directory debug logs may affect ISE performance.

Step 1 Choose **Administration** > **System** > **Logging** > **Debug Log Configuration**.

Step 2 Click the radio button next to the Cisco ISE Policy Service node from which you want to obtain Active Directory debug information, and click **Edit**.

Step 3 Click the **Active Directory** radio button, and click **Edit**.

Step 4 Choose **DEBUG** from the drop-down list next to Active Directory. This will include errors, warnings, and verbose logs. To get full logs, choose **TRACE**.

Step 5 Click **Save**.

Obtain the Active Directory Log File for Troubleshooting

Download and view the Active Directory debug logs to troubleshoot issues you may have.

Before you begin

Active Directory debug logging must be enabled.

Step 1 Choose **Operations** > **Troubleshoot** > **Download Logs**.

Step 2 Click the node from which you want to obtain the Active Directory debug log file.

Step 3 Click the **Debug Logs** tab.

Step 4 Scroll down this page to locate the ad_agent.log file. Click this file to download it.

Active Directory Alarms and Reports

Cisco ISE provides various alarms and reports to monitor and troubleshoot Active Directory related activities.

Alarms

The following alarms are triggered for Active Directory errors and issues:

- Configured nameserver not available
- Joined domain is unavailable
- Authentication domain is unavailable
- Active Directory forest is unavailable
- AD Connector had to be restarted
- AD: ISE account password update failed

- AD: Machine TGT refresh failed

Reports

You can monitor Active Directory related activities through the following two reports:

- RADIUS Authentications report: This report shows detailed steps of the Active Directory authentication and authorization. You can find this report here: **Operations** > **Reports** > **Endpoints and Users** > **RADIUS Authentications**.
- AD Connector Operations report: The AD Connector Operations report provides a log of background operations performed by AD connector, such as Cisco ISE server password refresh, Kerberos ticket management, DNS queries, DC discovery, LDAP, and RPC connections management. If you encounter any Active Directory failures, you can review the details in this report to identify the possible causes. You can find this report here: **Operations** > **Reports** > **Diagnostics** > **AD Connector Operations**.

Active Directory Advanced Tuning

The advanced tuning feature provides node-specific settings used for support action under the supervision of Cisco support personnel, to adjust the parameters deeper in the system. These settings are not intended for normal administration flow, and should be used only under guidance.

Configure Preferred Domain Controllers

You can specify the domain controllers that you want to use in case of a domain failover. If a domain fails, Cisco ISE compares the priority scores of the domain controllers that are added to the preferred list and selects the one with the highest priority score. If that domain controller is offline or not reachable because of an issue, the next one in the preferred list with the highest priority score is used. If all the domain controllers in the preferred list are down, a domain controller outside the list is selected based on the priority score. When the domain controller that was used before the failover is restored, Cisco ISE switches back to that domain controller.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory** > **Advanced Tools** > **Advanced Tuning**.

Step 2 From the **ISE Node** drop-down list, choose the Cisco ISE node that you want to configure.

Step 3 Enter the following registry key in the **Name** field:

REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\PreferredDCs\<*Domain Name*>

Step 4 In the **Value** field, specify the domain controllers that you want to add to the preferred list, separated by a space. Here is an example: `dc01.domain.com dc03.domain.com dc05.domain.com`

Step 5 (Optional) In the **Comment** field, enter a description about the preferred list.

Step 6 Click **Update Value**.

Step 7 Click **Restart Active Directory Connector**.

If you do not want to use the preferred list, click **Reset Parameter to Factory Default**.

Active Directory Identity Search Attributes

Cisco ISE identifies users using the attributes SAM, CN, or both. Cisco ISE uses sAMAccountName attribute as the default attribute.

You can configure Cisco ISE to use SAM, CN, or both, if your environment requires it. When SAM and CN are used, and the value of the SAMAccountName attribute is not unique, Cisco ISE also compares the CN attribute value.

Note To modify this default behavior, change the value of the "IdentityLookupField" flag as mentioned in the "Configure Attributes for Active Directory Identity Search" section.

Configure Attributes for Active Directory Identity Search

1. Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory** .
2. In the **Active Directory** window, click **Advanced Tools**, and choose **Advanced Tuning**. Enter the following details:
    - **ISE Node**: Choose the ISE node that is connecting to Active Directory.
    - **Name**: Enter the registry key that you are changing. To change the Active Directory search attributes, enter: `REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField`
    - **Value**: Enter the attributes that ISE uses to identify a user:
        - *SAM*: To use only SAM in the query (this option is the default).
        - *CN*: To use only CN in the query.
        - *SAMCN*: To use CN and SAM in the query.
    - **Comment**: Describe what you are changing, for example: Changing the default behavior to SAM and CN
3. Click **Update Value** to update the registry.

    A pop-up window appears. Read the message and accept the change. The AD connector service in ISE restarts.

Example Search Strings

For the following examples, assume that the username is *userd2only*:

- SAM search string—

```
filter=[(&(|(objectCategory=person)(objectCategory=computer))(|(cn=userd2only)(sAMAccountName=userd2only)))]
```

- SAM and CN search string—

```
filter=[(&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=userd2only))]
```

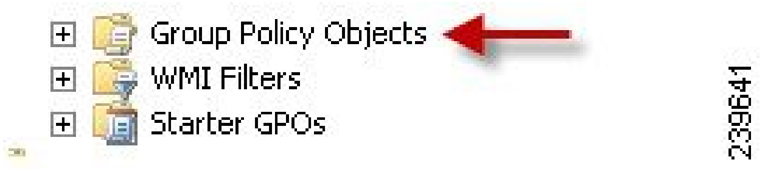
Supplemental Information for Setting Up Cisco ISE with Active Directory

For configuring Cisco ISE with Active Directory, you must configure group policies, and configure a supplicant for machine authentication.

Configure Group Policies in Active Directory

For more information about how to access the Group Policy management editor, refer to the Microsoft Active Directory documentation.

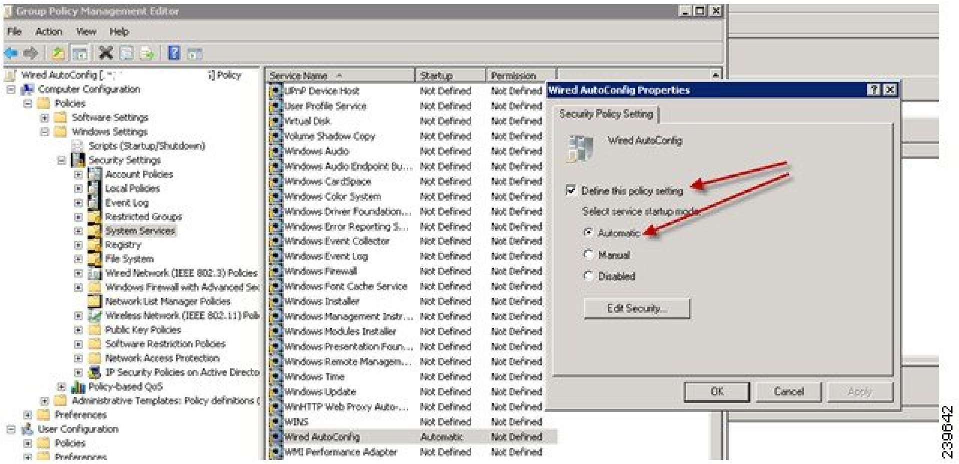
Step 1 Open the Group Policy management editor as shown in the following illustration.


Group Policy Objects
WMI Filters
Starter GPOs
239641

Step 2 Create a new policy and enter a descriptive name for it or add to an existing domain policy.

In example below, we used Wired Autoconfiguration for the policy name.

Step 3 Check the **Define this policy setting** check box, and click the **Automatic** radio button for the service startup mode as shown in the following illustration.


Group Policy Management Editor
File
Action
View
Help
Wired AutoConfig [ ] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Sec
Network List Manager Policies
Wireless Network (IEEE 802.11) Poli
Public Key Policies
Software Restriction Policies
Network Access Protection
IP Security Policies on Active Directo
Policy-based QoS
Administrative Templates: Policy definitions (
Preferences
User Configuration
Policies
Preferences
Wired AutoConfig Properties
Security Policy Setting
Wired AutoConfig
Edit Security...
OK
Cancel
Apply
239642

Service Name	Startup	Permission
UPnP Device Host	Not Defined	Not Defined
User Profile Service	Not Defined	Not Defined
Virtual Disk	Not Defined	Not Defined
Volume Shadow Copy	Not Defined	Not Defined
Windows Audio	Not Defined	Not Defined
Windows Audio Endpoint Bu...	Not Defined	Not Defined
Windows CardSpace	Not Defined	Not Defined
Windows Color System	Not Defined	Not Defined
Windows Driver Foundation...	Not Defined	Not Defined
Windows Error Reporting S...	Not Defined	Not Defined
Windows Event Collector	Not Defined	Not Defined
Windows Event Log	Not Defined	Not Defined
Windows Firewall	Not Defined	Not Defined
Windows Font Cache Service	Not Defined	Not Defined
Windows Installer	Not Defined	Not Defined
Windows Management Instr...	Not Defined	Not Defined
Windows Modules Installer	Not Defined	Not Defined
Windows Presentation Foun...	Not Defined	Not Defined
Windows Remote Managem...	Not Defined	Not Defined
Windows Time	Not Defined	Not Defined
Windows Update	Not Defined	Not Defined
WinHTTP Web Proxy Auto-...	Not Defined	Not Defined
WINS	Not Defined	Not Defined
Wired AutoConfig	Automatic	Not Defined
WMI Performance Adapter	Not Defined	Not Defined

☑ Define this policy setting

Select service startup mode:

● Automatic

○ Manual

○ Disabled

Step 4 Apply the policy at the desired organizational unit or domain Active Directory level.

Configure Odyssey 5.X Supplicant for EAP-TLS Machine Authentications Against Active Directory

If you are using the Odyssey 5.x supplicant for EAP-TLS machine authentications against Active Directory, you must configure the following in the supplicant.

Step 1 Start Odyssey Access Client.

Step 2 Choose **Odyssey Access Client Administrator** from the Tools menu.

Step 3 Double-click the **Machine Account** icon.

Step 4 From the **Machine Account** window, you must configure a profile for EAP-TLS authentications:

a) Choose **Configuration** > **Profiles**.
b) Enter a name for the EAP-TLS profile.
c) On the Authentication tab, choose **EAP-TLS** as the authentication method.
d) On the Certificate tab, check the **Permit login using my certificate** check box, and choose a certificate for the supplicant machine.
e) On the **User Info** tab, check the **Use machine credentials** check box.

If this option is enabled, the Odyssey supplicant sends the machine name in the format host\<*machine_name*> and Active Directory identifies the request as coming from a machine and will look up computer objects to perform authentication. If this option is disabled, the Odyssey supplicant sends the machine name without the host\ prefix and Active Directory will look up user objects and the authentication fails.

Configure Agent for Machine Authentication

When you configure the AnyConnect Agent for machine authentication, you can do one of the following:

- Use the default machine hostname, which includes the prefix “host/.”
- Configure a new profile, in which case you must include the prefix “host/” and then the machine name.

Active Directory Requirements to Support Easy Connect and Passive Identity services

Easy Connect and Passive Identity services use Active Directory login audit events generated by the Active Directory domain controller to gather user login information. The Active Directory server must be configured properly so the ISE user can connect and fetch the user login information. The following sections show how to configure the Active Directory domain controller (configurations from the Active Directory side) to support Easy Connect and Passive Identity services.

To configure Active Directory domain controllers (configurations from the Active Directory side) to support Easy Connect and Passive Identity services, follow these steps:

Note You must configure all the domain controllers in all the domains.

1. Set up Active Directory join points and domain controllers from ISE (see Add an Active Directory Join Point and Join Cisco ISE Node to the Join Point, on page 651).
2. Perform the following steps from Active Directory:
    - Configure Active Directory for Passive Identity service, on page 673
    - Set the Windows Audit Policy, on page 675

3. (Optional) Troubleshoot automatic configurations performed by ISE on Active Directory with these steps:
    - Set Permissions when Microsoft Active Directory Users are in Domain Admin Group, on page 676
    - Permissions for Microsoft Active Directory Users Not in Domain Admin Group, on page 676
    - Permissions to Use DCOM on the Domain Controller, on page 678

Configure Active Directory for Passive Identity service

ISE Easy Connect and Passive Identity services use Active Directory login audit events generated by the Active Directory domain controller to gather user login information. ISE connects to Active Directory and fetches the user login information.

The following steps should be performed from the Active Directory domain controller:

Step 1 Make sure relevant Microsoft patches are installed on the Active Directory domain controllers.

Step 2 Make sure the Active Directory logs the user login events in the Windows Security Log.

Verify that the Audit Policy settings (part of the Group Policy Management settings) allows successful logons to generate the necessary events in the Windows Security Log (this is the default Windows setting, but you must explicitly ensure that this setting is correct).

Step 3 You must have an Active Directory user with sufficient permissions for ISE to connect to the Active Directory. The following instructions show how to define permissions either for admin domain group user or none admin domain group user:

- Permissions Required when an Active Directory User is a Member of the Domain Admin Group
- Permissions Required when an Active Directory User is Not a Member of the Domain Admin Group

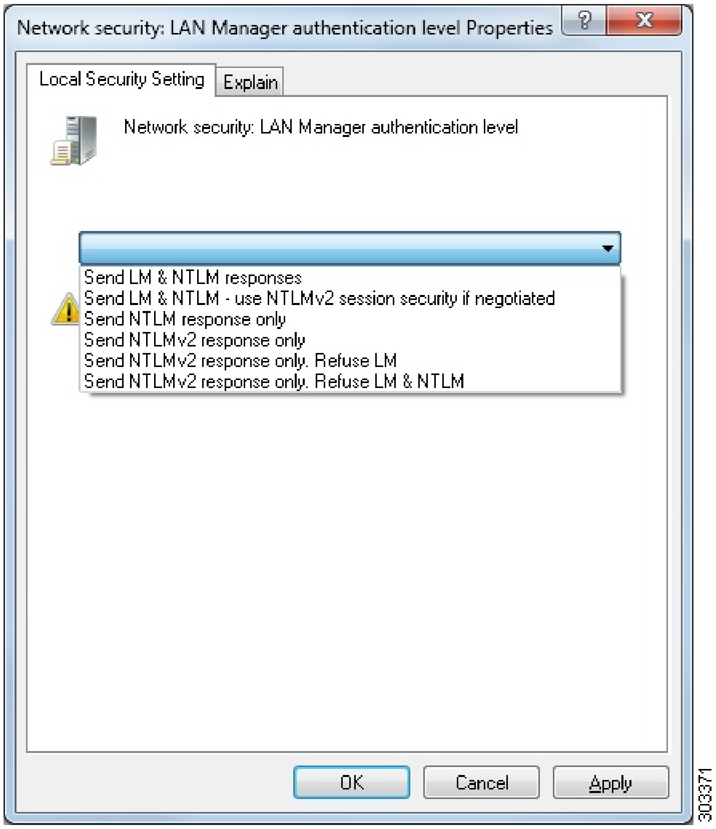
Step 4 The Active Directory user used by ISE can be authenticated either by NT Lan Manager (NTLM) v1 or v2. You need to verify that the Active Directory NTLM settings are aligned with ISE NTLM settings to ensure successful authenticated connection between ISE and the Active Directory Domain Controller. The following table shows all Microsoft NTLM options, and which ISE NTLM actions are supported. If ISE is set to NTLMv2, all six options described in are supported. If ISE is set to support NTLMv1, only the first five options are supported.

Table 75: Supported Authentication Types Based on ISE and AD NTLM Version Settings

ISE NTLM Setting Options / Active Directory (AD) NTLM Setting Options NTLMv1 NTLMv2	NTLMv1	NTLMv2
Send LM & NTLM responses connection is allowed connection is allowed	Connection is allowed	Connection is allowed
Send LM & NTLM - use NTLMv2 session security if negotiated connection is allowed connection is allowed	Connection is allowed	Connection is allowed

ISE NTLM Setting Options / Active Directory (AD) NTLM Setting Options NTLMv1 NTLMv2	NTLMv1	NTLMv2
Send NTLM response only connection is allowed connection is allowed	Connection is allowed	Connection is allowed
Send NTLMv2 response only connection is allowed connection is allowed	Connection is allowed	Connection is allowed
Send NTLMv2 response only. Refuse LM connection is allowed connection is allowed	Connection is allowed	Connection is allowed
Send NTLMv2 response only. Refuse LM & NTLM connection is refused connection is allowed	Connection is refused	Connection is allowed

Figure 15: MS NTLM Authentication Type Options


Network security: LAN Manager authentication level Properties
Local Security Setting
Explain
Network security: LAN Manager authentication level
Send LM & NTLM responses
Send LM & NTLM - use NTLMv2 session security if negotiated
Send NTLM response only
Send NTLMv2 response only
Send NTLMv2 response only. Refuse LM
Send NTLMv2 response only. Refuse LM & NTLM
OK
Cancel
Apply
303371

Step 5 Make sure that you have created a firewall rule to allow traffic to `dllhost.exe` on Active Directory domain controllers.

You can either turn the firewall off, or allow access on a specific IP (ISE IP address) to the following ports:

- TCP 135: General RPC Port. When doing asynchronous RPC calls, the service listening on this port tells the client which port the component servicing this request is using.
- UDP 137: Netbios Name Resolution
- UDP 138: Netbios Datagram Service
- TCP 139: Netbios Session Service
- TCP 445: SMB

Higher ports are assigned dynamically or you can configure them manually. We recommend that you add %SystemRoot%\System32\dllhost.exe as a target. This program manages ports dynamically.

All firewall rules can be assigned to specific IP (ISE IP).

Set the Windows Audit Policy

Ensure that the **Audit Policy** (part of the **Group Policy Management** settings) allows successful logons. This is required to generate the necessary events in the Windows Security Log of the AD domain controller machine. This is the default Windows setting, but you must verify that this setting is correct.

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Group Policy Management**.

Step 2 Navigate under Domains to the relevant domain and expand the navigation tree.

Step 3 Choose **Default Domain Controller Policy**, right click and choose **Edit**.

The Group Policy Management Editor appears.

Step 4 Choose **Default Domain Controllers Policy** > **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings**.

- For Windows Server 2003 or Windows Server 2008 (non-R2), choose **Local Policies** > **Audit Policy**. For the two Policy items, **Audit Account Logon Events** and **Audit Logon Events**, ensure that the corresponding **Policy Setting** either directly or indirectly includes the **Success** condition. To include the Success condition indirectly, the **Policy Setting** must be set to **Not Defined**, indicating that the effective value will be inherited from a higher level domain, and the **Policy Setting** for that higher level domain must be configured to explicitly include the **Success** condition.
- For Windows Server 2008 R2 and Windows 2012, choose **Advanced Audit Policy Configuration** > **Audit Policies** > **Account Logon**. For the two Policy items, **Audit Kerberos Authentication Service** and **Audit Kerberos Service Ticket Operations**, ensure that the corresponding Policy Setting either directly or indirectly includes the Success condition, as described above.

  Note Cisco ISE uses RC4 cipher in Kerberos protocol while communicating with Active Directory, unless this encryption type is disabled in Active Directory Domain Controller configuration. You can use the **Network Security: Configure Encryption Types Allowed for Kerberos** option in Active Directory to configure the allowed encrytion types for Kerberos protocol.

Step 5 If any Audit Policy item settings have been changed, you should then run `gpupdate /force` to force the new settings to take effect.

Set Permissions when Microsoft Active Directory Users are in Domain Admin Group

For Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2, the Domain Admin group does not have full control of certain registry keys in the Windows operating system by default. The Microsoft Active Directory administrator must give the Microsoft Active Directory user full control permissions on the following registry keys:

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

The following Microsoft Active Directory versions require no registry changes:

- Windows 2003
- Windows 2003R2
- Windows 2008

To grant full control, the Microsoft Active Directory admin must first take ownership of the key:

Step 1 Right-click the key icon and choose the **Owner** tab.

Step 2 Click **Permissions**.

Step 3 Click **Advanced**.

Permissions for Microsoft Active Directory Users Not in Domain Admin Group

For Windows Server 2012 R2, give the Microsoft AD user full control permissions on the following registry keys:

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

Use the following commands in Windows PowerShell to check if full permission is given to the registry keys:

-
  ```
  get-acl -path
  "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}"
  | format-list
  ```

-
  ```
  get-acl -path
  "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" |
  format-list
  ```

The following permissions are required when a Microsoft AD user is not in the Domain Admin group, but is in the Domain Users group:

- Add registry keys to allow Cisco ISE to connect to the domain controller.
- Permissions to Use DCOM on the Domain Controller, on page 678

- Set Permissions for Access to WMI Root and CIMv2 Namespace, on page 966

These permissions are only required for the following Microsoft AD versions:

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

Add Registry Keys to Allow Cisco ISE to Connect to the Domain Controller

You must manually add some registry keys to the domain controller to allow Cisco ISE to connect as a domain user, and retrieve login authentication events. An agent is not required on the domain controllers or on any machines in the domain.

The following registry script shows the keys to add. You can copy and paste this into a text file, save the file with a .reg extension, and double click the file to make the registry changes. To add registry keys, the user must be an owner of the root key.

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "

```

Make sure that you include two spaces in the value of the DllSurrogate key. If the registry is manually updated, you must include only the two spaces and do not include the quotes. While updating the registry manually, ensure that quotes are not included for AppID, DllSurrogate, and its values.

Retain the empty lines as shown in the preceding script, including the empty line at the end of the file.

Use the following commands in the Windows command prompt to confirm if the registry keys are created and have the correct values:

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`
- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`
- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`

Permissions to Use DCOM on the Domain Controller

The Microsoft Active Directory user who is used for Cisco ISE Passive Identity service must have the permissions to use DCOM on the domain controller server. Configure permissions with the **dcomcnfg** command line tool.

Step 1 Run the **dcomcnfg** tool from the command line.

Step 2 Expand `Component Services`.

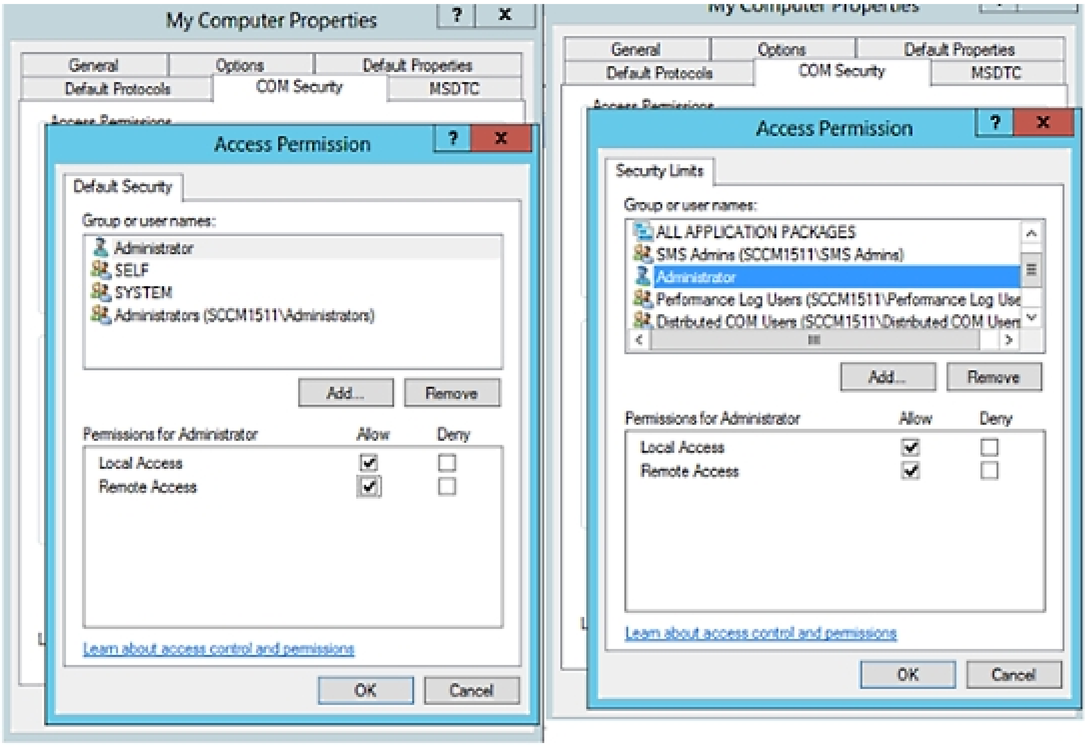
Step 3 Expand **Computers** > **My Computer**.

Step 4 Choose **Action** from the menu bar, click **Properties**, and click **COM Security**.

Step 5 The account that Cisco ISE uses for both access and launch must have Allow permissions. Add the Microsoft Active Directory user to all the four options, **Edit Limits** and **Edit Default** for both **Access Permissions** and **Launch and Activation Permissions**.

Step 6 Allow all local and remote accesses for both **Access Permissions** and **Launch and Activation Permissions**.

Figure 16: Local and Remote Accesses for Access Permissions


My Computer Properties
General
Options
Default Properties
Default Protocols
COM Security
MSDTC
Access Permission
Default Security
Security Limits
Add...
Remove
Learn about access control and permissions
OK
Cancel

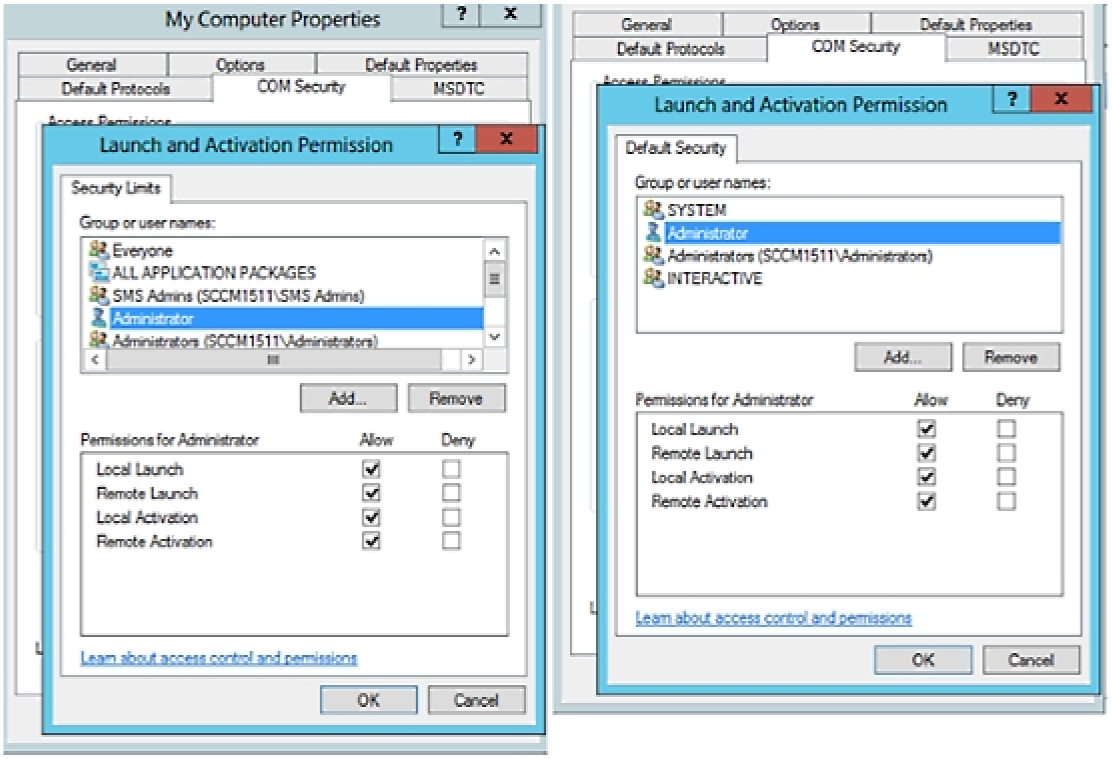
Group or user names:
Administrator
SELF
SYSTEM
Administrators (SCCM1511\Administrators)

Permissions for Administrator | Allow | Deny
Local Access ☑ ☐
Remote Access ☑ ☐

Group or user names:
ALL APPLICATION PACKAGES
SMS Admins (SCCM1511\SMS Admins)
Administrator
Performance Log Users (SCCM1511\Performance Log Use
Distributed COM Users (SCCM1511\Distributed COM Users

Permissions for Administrator | Allow | Deny
Local Access ☑ ☐
Remote Access ☑ ☐

Figure 17: Local and Remote Accesses for Launch and Activation Permissions


My Computer Properties
General
Options
Default Properties
Default Protocols
COM Security
MSDTC
Access Permissions
Launch and Activation Permission
Security Limits
Add...
Remove
Learn about access control and permissions
OK
Cancel
General
Options
Default Properties
Default Protocols
COM Security
MSDTC
Access Permissions
Launch and Activation Permission
Default Security
Add...
Remove
Learn about access control and permissions
OK
Cancel

Group or user names:

- Everyone
- ALL APPLICATION PACKAGES
- SMS Admins (SCCM1511\SMS Admins)
- Administrator
- Administrators (SCCM1511\Administrators)

Permissions for Administrator	Allow	Deny
Local Launch	☑	☐
Remote Launch	☑	☐
Local Activation	☑	☐
Remote Activation	☑	☐

Group or user names:

- SYSTEM
- Administrator
- Administrators (SCCM1511\Administrators)
- INTERACTIVE

Permissions for Administrator	Allow	Deny
Local Launch	☑	☐
Remote Launch	☑	☐
Local Activation	☑	☐
Remote Activation	☑	☐

Easy Connect

Easy Connect enables you to easily connect users from a wired endpoint to a network in a secure manner and monitor those users by authenticating them through an Active Directory Domain Controller and not by Cisco ISE. With Easy Connect, Cisco ISE collects user authentication information from the Active Directory Domain Controller. Easy Connect connects to a Windows system (Active Directory) using the MS WMI interface and queries logs from the Windows event messaging, hence it currently only supports Windows-installed endpoints. Easy Connect supports wired connections using MAB, which is much easier to configure than 802.1X. Unlike 802.1X, with Easy Connect and MAB:

- You don't need to configure supplicants
- You don't need to configure PKI
- ISE issues a CoA after the external server (AD) authenticates the user

Easy Connect supports these modes of operation:

- Enforcement-mode: ISE actively downloads the authorization policy to the network device for enforcement based on the user credentials.
- Visibility-mode: Cisco ISE publishes session merge and accounting information received from the NAD device sensor in order to send that information to pxGrid.

In both cases, users authenticated with Active Directory (AD) are shown in the Cisco ISE live sessions view, and can be queried from the session directory using Cisco pxGrid interface by third-party applications. The known information is the user name, IP address, the AD DC host name, and the AD DC NetBios name. For more information about pxGrid, see Cisco pxGrid Node, on page 210.

Once you have set up Easy Connect, you can then filter certain users, based on their name or IP address. For example, if you have an administrator from IT services who logs in to an endpoint in order to assist the regular user with that endpoint, you can filter out the administrator activity so it does not appear in Live Sessions, but rather only the regular user of that endpoint will appear. To filter passive identity services, see Filter Passive Identity Services, on page 724.

Easy Connect Restrictions

- MAC Authentication Bypass (MAB) supports Easy Connect. Both MAB and 802.1X can be configured on the same port, but you must have a different ISE policy for each service.
- Only MAB connections are currently supported. You do not need a unique authentication policy for connections, because the connection is authorized and permissions are granted by an Easy Connect condition defined in the authorization policy.
- Easy Connect is supported in High Availability mode. Multiple nodes can be defined and enabled with a Passive ID. ISE then automatically activates one PSN, while the other nodes remain in standby.
- Only Cisco Network Access Devices (NADs) are supported.
- IPv6 is not supported.
- Wireless connections are not currently supported.
- Only Kerberos auth events are tracked and therefore Easy Connect enables only user authentication and does not support machine authentication.

Easy Connect requires configuration in ISE, while the Active Directory Domain server must also have the correct patches and configuration based on instructions and guidelines issued by Microsoft. For information about configuring the Active Directory domain controller for Cisco ISE, see Active Directory Requirements to Support Easy Connect and Passive Identity services, on page 672

Easy Connect Enforcement Mode

Easy Connect enables users to log on to a secure network from a wired endpoint (usually a PC) with a Windows operating system, by using MAC address bypass (MAB) protocol, and accessing Active Directory (AD) for authentication. Easy Connect listens for a Windows Management Instrumentation (WMI) event from the Active Directory server for information about authenticated users. When AD authenticates a user, the Domain Controller generates an event log that includes the user name and IP address allocated for the user. Cisco ISE receives notification of log in from AD, and then issues a RADIUS Change of Authorization (CoA).

Note MAC address lookup is not done for a MAB request when the Radius service-type is set to call-check. Therefore the return to the request is access-accept. This is the default configuration.

Easy Connect Enforcement Mode Process Flow

The Easy Connect Enforcement mode process is as follows:

1. The user connects to the NAD from a wired endpoint (such as a PC for example).
2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD.
3. The user logs in to the domain and a security audit event is sent to Cisco ISE.
4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event.
5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy.

Figure 18: Easy Connect Enforcement Mode Basic Flow

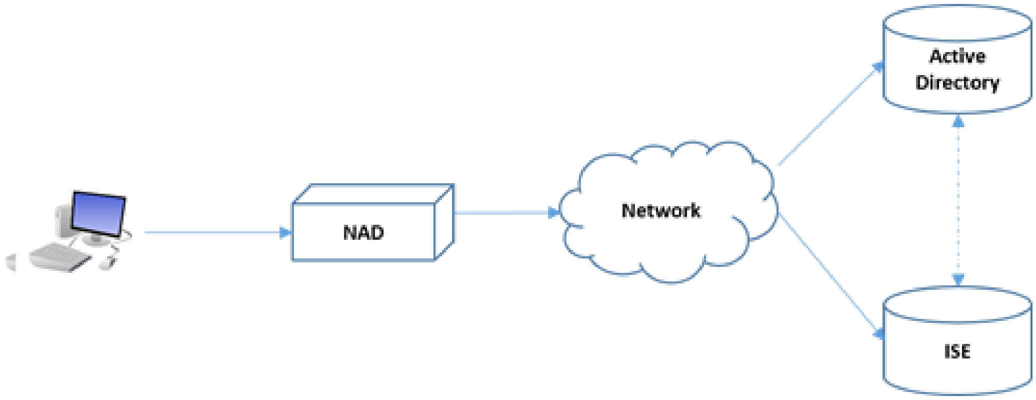
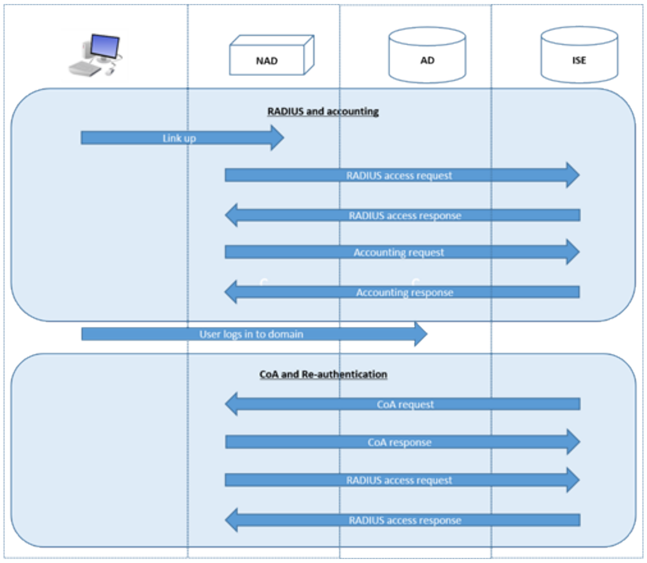

Active Directory
NAD
Network
ISE

Figure 19: Easy Connect Enforcement Mode Detailed Flow

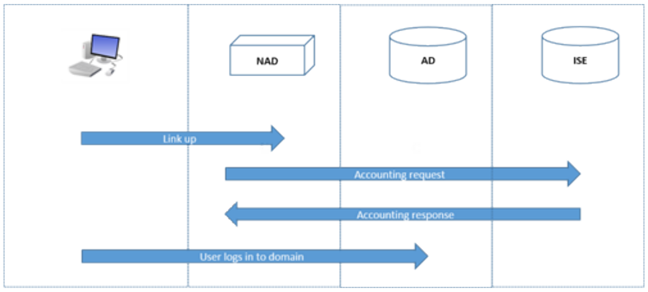

NAD
AD
ISE
RADIUS and accounting
Link up
RADIUS access request
RADIUS access response
Accounting request
Accounting response
User logs in to domain
CoA and Re-authentication
CoA request
CoA response
RADIUS access request
RADIUS access response

For more information about configuring Enforcement mode, see Configure Easy Connect Enforcement Mode, on page 682.

Easy Connect Visibility Mode

With the Visibility mode, Cisco ISE only monitors accounting information from RADIUS (part of the device sensor feature in the NAD) and does not perform authorization. Easy Connect listens for RADIUS Accounting and WMI events, and publishes that information to logs and reports, (and optionally, to pxGrid). Both RADIUS accounting start and session termination are published to pxGrid during user login using Active Directory when pxGrid is setup.

Figure 20: Easy Connect Visibility Mode Flow



For more information about configuring Easy Connect Visibility mode, see Configure Easy Connect Visibility Mode, on page 683 .

Configure Easy Connect Enforcement Mode

Before you begin

- For best performance, deploy a dedicated PSN to recieve WMI events.
- Create a list of Active Directory Domain Controllers for the WMI node, which receives AD login events.
- Determine the Microsoft Domain that Cisco ISE must join to fetch user groups from Active Directory.
- Determine the Active Directory groups that are used as a reference in the authorization policy.
- If you are using pxGrid to share session data from network devices with other pxGrid-enabled systems, then define a pxGrid persona in your deployment. For more information about pxGrid, see Cisco pxGrid Node, on page 210
- After successful MAB, the NAD must provide a limited-access profile, which allows the user on that port access to the Active Directory server.

Note Passive Identity Service can be enabled on multiple nodes, but Easy Connect can only operate on one node at a time. If you enable the service for multiple nodes, ISE will automatically determine which node to use for the active Easy Connect session.

Step 1 Choose **Administration** > **System** > **Deployment**, open a node, and under **General Settings**, enable **Enable Passive Identity Service**.

Step 2 Configure an Active Directory join point and domain controller to be used by Easy Connect. For more information, see Active Directory Requirements to Support Easy Connect and Passive Identity services, on page 672.

Step 3 (Optional) Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**. Click the **Groups** tab, and add the Active Directory groups you plan to use in your authorization policies.
The Active Directory groups that you map for the Domain Controller are dynamically updated in the PassiveID dictionary and can then be used when you set up your policy conditions rules.

Step 4 **Note** **Passive Identity Tracking** must be enabled for all profiles used for Easy Connect authorization in order for the Easy Connect process to run properly and enable ISE to issue a CoA.

Choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**. For any profiles to be used by Easy Connect, open the profile and enable **Passive Identify Tracking**.

Step 5 Choose **Policy** > **Policy Elements** > **Conditions** > **Authorization** > **Simple Conditions**, to create rules for Easy Connect. Click **Add** and define the condition:

a) Enter a name and description.
b) From **Attribute**, go to the PassiveID dictionary and select either PassiveID_Groups to create a condition for domain controller groups, or select PassiveID_user to create a condition for individual users.
c) Enter the correct operation.
d) Enter the user name or group name to be included in the policy.

Step 6 Click **Submit**.

Configure Easy Connect Visibility Mode

Before you begin

- For best performance, deploy a dedicated PSN to recieve WMI events.
- Create a list of Active Directory Domain Controllers for the WMI node, which receives AD login events.
- Determine the Microsoft Domain that Cisco ISE must join to fetch user groups from Active Directory.
- If you are using pxGrid to share session data from network devices with other pxGrid-enabled systems, then define a pxGrid persona in your deployment. For more information about pxGrid, see Cisco pxGrid Node, on page 210

Step 1 Choose **Administration** > **System** > **Deployment**, open a node, and under **General Settings**, enable **Enable Passive Identity Service**.

Step 2 Configure an Active Directory join point and domain controller to be used by Easy Connect. For more information, see Active Directory Requirements to Support Easy Connect and Passive Identity services, on page 672.

PassiveID Work Center

Passive Identity Connector (the PassiveID work center) offers a centralized, one-stop installation and implementation enabling you to easily and simply configure your network in order to receive and share user identity information with a variety of different security product subscribers such as Cisco Firepower Management Center (FMC) and Stealthwatch. As the full broker for passive identification, the PassiveID work center collects user identities from different provider sources, such as Active Directory Domain Controllers

(AD DC), maps the user login information to the relevant IP addresses in use and then shares that mapping information with any of the subscriber security products that you have configured.

Note For information about the FMC and Stealthwatch releases that are validated with ISE, see *Cisco Identity Services Engine Network Component Compatibility*.

What is Passive Identity?

Standard flows offered by Cisco Identity Services Engine (ISE), which provide an authentication, authorization and accounting (AAA) server, and utilize technologies such as 802.1X or Web Authentication, communicate directly with the user or endpoint, requesting access to the network, and then using their login credentials in order to verify and actively authenticate their identity.

Passive identity services do not authenticate users directly, but rather gather user identities and IP addresses from external authentication servers such as Active Directory, known as providers, and then share that information with subscribers. the PassiveID work center first receives the user identity information from the provider, usually based on the user login and password, and then performs the necessary checks and services in order to match the user identity with the relevant IP address, thereby delivering the authenticated IP address to the subscriber.

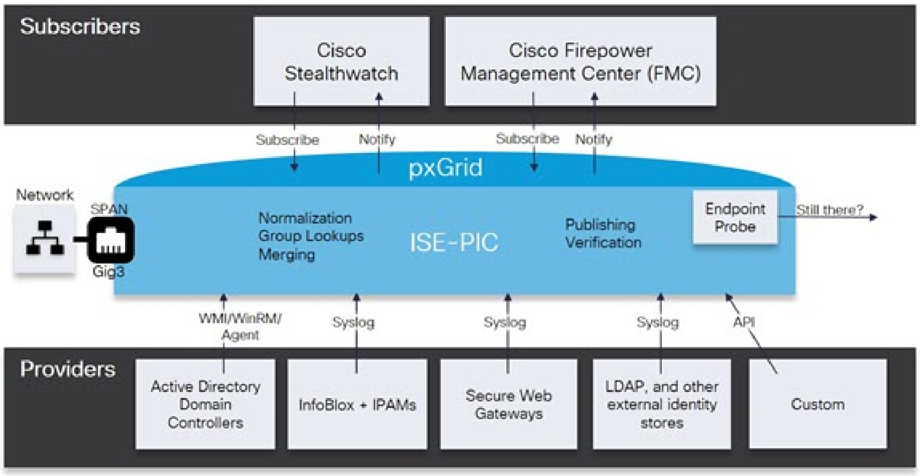
Passive Identity Connector (PassiveID work center) Flow

The flow for the PassiveID work center is as follows:

1. Provider performs the authentication of the user or endpoint.
2. Provider sends authenticated user information to Cisco ISE.
3. Cisco ISE normalizes, performs lookups, merges, parses and maps user information to IP addresses and publishes mapped details to pxGrid.
4. pxGrid subscribers receive the mapped user details.

The following diagram illustrates the high-level flow offered by Cisco ISE.

Figure 21: High Level Flow


Subscribers
Cisco Stealthwatch
Cisco Firepower Management Center (FMC)
Subscribe
Notify
Subscribe
Notify
pxGrid
Network
SPAN
Gig3
Normalization
Group Lookups
Merging
ISE-PIC
Publishing
Verification
Endpoint Probe
Still there?
WMI/WinRM/ Agent
Syslog
Syslog
Syslog
API
Providers
Active Directory Domain Controllers
InfoBlox + IPAMs
Secure Web Gateways
LDAP, and other external identity stores
Custom

Initial Setup and Configuration

To get started using Cisco PassiveID work center quickly, follow this flow:

1. Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from Cisco ISE. For more information, see DNS Server, on page 650.
2. Enable the Passive Identity and pxGrid services on the dedicated Policy server (PSN) you intend to use for any of the Passive Identity services. Choose **Administration** > **System** > **Deployment**, open the relevant node, and under **General Settings**, enable **Enable Passive Identity Service** and **pxGrid**.
3. Synchronize clock settings for the NTP servers.
4. Configure an initial provider with the ISE Passive Identity Setup. For more information, see Getting Started with the PassiveID Setup, on page 686.
5. Configure a single or multiple subscribers.

After setting up an initial provider and subscriber, you can easily create additional providers (see Additional Passive Identity Service Providers, on page 690) and manage your passive identification from the different providers in the PassiveID work center.

PassiveID Work Center Dashboard

The Cisco PassiveID Work Center dashboard displays consolidated and correlated summary and statistical data that is essential for effective monitoring and troubleshooting, and is updated in real time. Dashlets show activity over the last 24 hours, unless otherwise noted. To access the dashboard, choose **Work Centers** > **PassiveID** and then from the left panel choose **Dashboard**. You can only view the Cisco PassiveID Work Center Dashboard in the Primary Administration Node (PAN).

- The **Main** view has a linear Metrics dashboard, chart dashlets, and list dashlets. In the PassiveID Work Center, the dashlets are not configurable. Available dashlets include:
    - **Passive Identity Metrics**: Displays the total number of unique live sessions currently being tracked, the total number of identity providers configured in the system, the total number of agents actively delivering identity data, and the total number of subscribers currently configured.
    - **Providers**: Providers provide user identity information to PassiveID Work Center. You configure the ISE probe (mechanisms that collect data from a given source) through which to receive information from the provider sources. For example, an Active Directory (AD) probe and an Agents probe both help ISE-PIC collect data from AD (each with different technology) while a Syslog probe collects data from a parser that reads syslog messages.
    - **Subscribers**: Subscribers connect to ISE to retrieve user identity information.
    - **OS Types**: The only OS type that can be displayed is Windows. Windows types display by Windows versions. Providers do not report the OS type, but ISE can query Active Directory to get that information. Up to 1000 entries are displayed in the dashlet.
    - **Alarms**: User identity-related alarms.

Active Directory as a Probe and a Provider

Active Directory (AD) is a highly secure and precise source from which to receive user identity information, including user name, IP address, and domain name.

By configuring the Active Directory probe you can also then quickly configure and enable these other probes (which also use Active Directory as their source):

- Active Directory Agents, on page 693

Note The Active Directory agents are only supported on Windows Server 2008 and higher.

- SPAN, on page 701
- Endpoint Probe, on page 724

In addition, configure the Active Directory probe in order to use AD user groups when collecting user information. You can use AD user groups for the AD, Agents, SPAN, and Syslog probes. For more information about AD groups, see Configure Active Directory User Groups, on page 657.

Getting Started with the PassiveID Setup

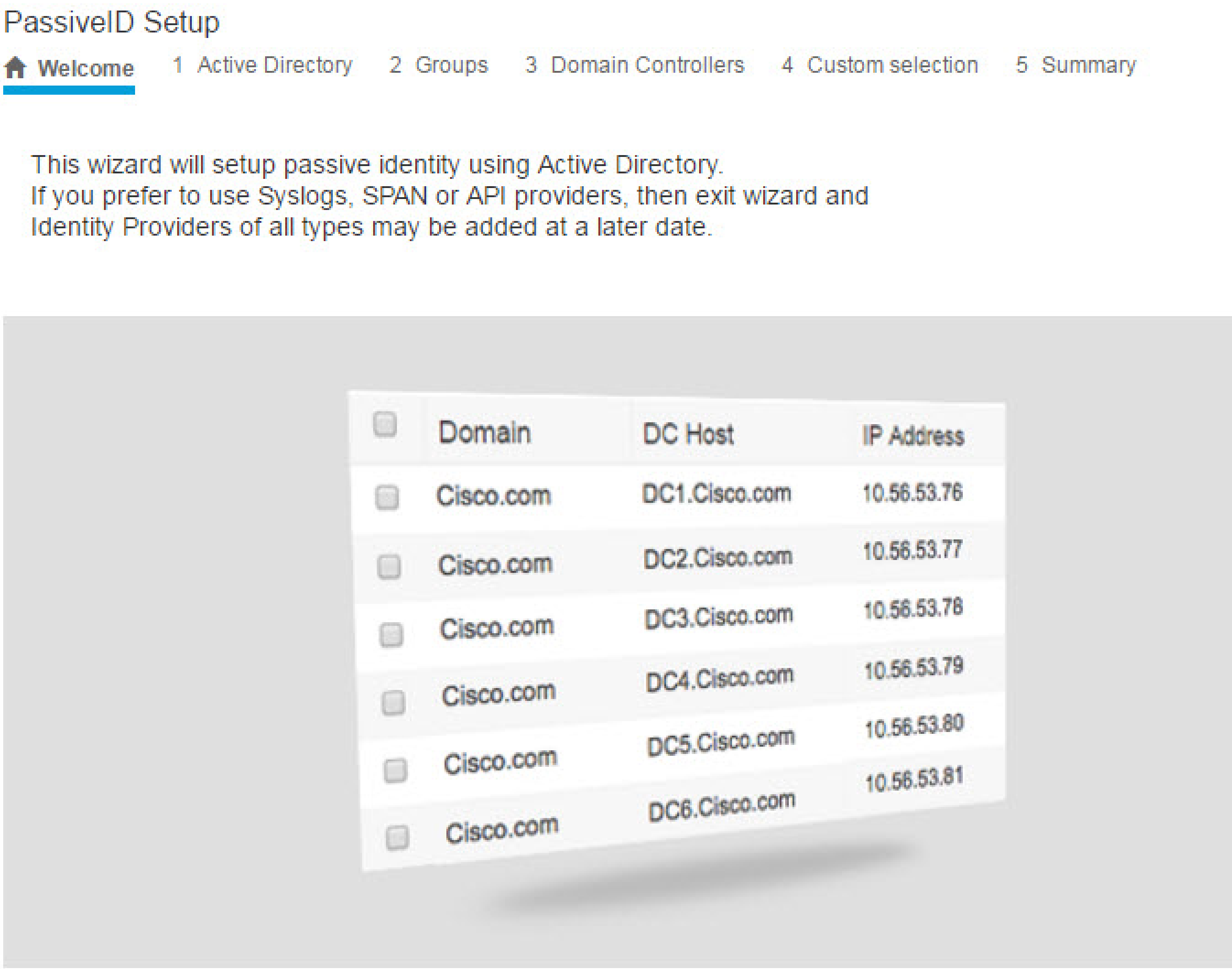
ISE-PIC offers a wizard from which you can easily and quickly configure Active Directory as your first user identity provider, in order to receive user identities from Active Directory. By configuring Active Directory for ISE-PIC, you also simplify the process for configuring other provider types later on. Once you have configured Active Directory, you must then configure a Subscriber (such as Cisco Firepower Management Center (FMC) or Stealthwatch), in order to define the client that is to receive the user data.

Before you begin

- Ensure the Microsoft Active Directory server does not reside behind a network address translator and does not have a Network Address Translation (NAT) address.
- Ensure the Microsoft Active Directory account intended for the join operation is valid and is not configured with the Change Password on Next Login.
- Ensure you have the privileges of a Super Admin or System Admin in ISE.
- Enable the Passive Identity and pxGrid services on the dedicated Policy server (PSN) you intend to use for any of the Passive Identity services. Choose **Administration** > **System** > **Deployment**, open the relevant node, and under **General Settings**, enable **Enable Passive Identity Service** and **pxGrid**.
- Ensure that ISE has an entry in the domain name server (DNS). Ensure you have properly configured reverse lookup for the client machine from ISE. For more information, see DNS Server, on page 650

Step 1 Choose **Work Centers** > **PassiveID**. From the Passive Identity Connector Overview screen, click **Passive Identity Wizard**.

Figure 22: The PassiveID Setup



PassiveID Setup

This wizard will setup passive identity using Active Directory.
If you prefer to use Syslogs, SPAN or API providers, then exit wizard and
Identity Providers of all types may be added at a later date.

☐	Domain	DC Host	IP Address
☐	Cisco.com	DC1.Cisco.com	10.56.53.76
☐	Cisco.com	DC2.Cisco.com	10.56.53.77
☐	Cisco.com	DC3.Cisco.com	10.56.53.78
☐	Cisco.com	DC4.Cisco.com	10.56.53.79
☐	Cisco.com	DC5.Cisco.com	10.56.53.80
☐	Cisco.com	DC6.Cisco.com	10.56.53.81

Step 2 Click **Next** to begin the wizard.

Step 3 Enter a unique name for this Active Directory join point. Enter the domain name for the Active Directory Domain to which this node is connected, and enter your Active Directory administrator user name and password.

It is strongly recommended that you choose **Store credentials**, in which case your administrator's user name and password will be saved in order to be used for all Domain Controllers (DC) that are configured for monitoring.

Step 4 Click **Next** to define Active Directory groups and check any user groups to be included and monitored.
The Active Directory user groups automatically appear based on the Active Directory join point you configured in the previous step.

Step 5 Click **Next**. Select the DCs to be monitored. If you choose Custom, then from the next screen select the specific DCs for monitoring. When finished, click **Next**.

Step 6 Click **Exit** to complete the wizard.

What to do next

When you finish configuring Active Directory as your initial provider, you can easily configure additional provider types as well. For more information, see Additional Passive Identity Service Providers, on page 690. Furthermore, you can now also configure a subscriber, designated to receive the user identity information that is collected by any of the providers you have defined.

Manage the Active Directory Provider

Once you have created and configured your Active Directory join points, continue to manage the Active Directory probe with these tasks:

- Test Users for Active Directory Authentication, on page 666
- View Active Directory Joins for a Node, on page 667
- Diagnose Active Directory Problems, on page 667
- Leave the Active Directory Domain, on page 656
- Delete Active Directory Configurations, on page 666
- Enable Active Directory Debug Logs, on page 668

Active Directory Settings

Active Directory (AD) is a highly secure and precise source from which to receive user information, including user name and IP address.

To create and manage Active Directory probes by creating and editing join points, choose **Work Centers** > **PassiveID** > **Providers** > **Active Directory**.

For more information, see Add an Active Directory Join Point and Join Cisco ISE Node to the Join Point, on page 651.

Table 76: Active Directory Join Point Name Settings and Join Domain Window

Field Name	Description
Join Point Name	A unique name that distinguishes this configured join point quickly and easily.
Active Directory Domain	The domain name for the Active Directory Domain to which this node is connected.
Domain Administrator	This is the user principal name or the user account name for the Active Directory user with administrator priveleges.
Password	This is the domain administrator's password as configured in Active Directory.

Field Name	Description
Specifiy Organizational Unit	Enter the administrator's organizational unit information
Store Credentials	It is strongly recommended that you choose **Store credentials**, in which case your administrator's user name and password will be saved in order to be used for all Domain Controllers (DC) that are configured for monitoring. For the Endpoint probe, you must choose **Store credentials**.

Table 77: Active Directory Join/Leave Window

Field Name	Description
ISE Node	The URL for the specific node in the installation.
ISE Node Role	Indicates whether the node is the Primary or Secondary node in the installation.
Status	Indicates whether the node is actively joined to the Active Directory domain.
Domain Controller	For nodes that are joined to Active Directory, this column indicates the specific Domain Controller to which the node is connected in the Active Directory Domain.
Site	When an Active Directory forest is joined with ISE, this field indicates the specific Active Directory site within the forest as it appears in the Active Directory Sites and Services area.

Table 78: Passive ID Domain Controllers (DC) List

Field	Description
Domain	The fully qualified domain name of the server on which the domain controller is located.
DC Host	The host on which the domain controller is located.
Site	When an Active Directory forest is joined with ISE, this field indicates the specific Active Directory site within the forest as it appears in the Active Directory Sites and Services area.
IP Address	The IP address of the domain controller.
Monitor Using	Monitor Active Directory domain controllers for user identity information by one of these methods: • WMI: Monitor Active Directory directly with the WMI infrastructure. • Agent name: If you have defined agents to monitor Active Directory for user information, select the Agent protocol and choose the agent from the dropdown list that you would like to use. For more information about agents, see Active Directory Agents, on page 693.

Table 79: Passive ID Domain Controllers (DC) Edit Window

Field Name	Description
Host FQDN	Enter the fully qualified domain name of the server on which the domain controller is located.
Description	Enter a unique description for this domain controller in order to easily identiy it.
User Name	The administrator's user name for accessing Active Directory.
Password	The administrator's password for accessing Active Directory.
Protocol	Monitor Active Directory domain controllers for user identity information by one of these methods: • WMI: Monitor Active Directory directly with the WMI infrastructure. • Agent name: If you have defined agents to monitor Active Directory for user information, select the Agent protocol and choose the agent from the dropdown list that you would like to use. For more information about agents, see Active Directory Agents, on page 693.

Active Directory groups are defined and managed from Active Directory and the groups for the Active Directory that is joined to this node can be viewed from this tab. For more information about Active Directory, see https://msdn.microsoft.com/en-us/library/bb742437.aspx.

Table 80: Active Directory Advanced Settings

Field Name	Description
History interval	The time during which the Passive Identity service reads user login information that already occurred. This is required upon startup or restart of the Passive Identity service to catch up with events generated while it was unavailable. When the Endpoint probe is active, it maintains the frequency of this interval.
User session aging time	The amount of time the user can be logged in. The Passive Identity service identifies new user login events from the DC, however the DC does not report when the user logs off. The aging time enables Cisco ISE to determine the time interval for which the user is logged in.
NTLM Protocol settings	You can select either NTLMv1 or NTLMv2 as the communications protocol between Cisco ISE and the DC. NTLMv2 is the recommended default.

Additional Passive Identity Service Providers

In order to enable ISE to provide identity information (Passive Identity Service) to consumers that subscribe to the service (subscribers), you must first configure an ISE probe, which connects to the identity provider.

The table below provides details about all of the provider and probe types available from ISE. For more information about Active Directory, see Active Directory as a Probe and a Provider, on page 686.

You can define these provider types:

Table 81: Provider Types

Provider Type (Probe)	Description	Source System (Provider)	Technology	User Identity Information Collected	Document Link
Active Directory (AD)	A highly secure and precise source, as well as the most common, from which to receive user information. As a probe, AD works with WMI technology to deliver authenticated user identities. In addition, AD itself, rather than the probe, functions as a source system (a provider) from which other probes retrieve user data as well.	Active Directory Domain Controller	WMI	• User name • IP address • Domain	Active Directory as a Probe and a Provider, on page 686
Agents	A native 32-bit application installed on Active Directory domain controllers or on member servers. The Agent probe is a quick and efficient solution when using Active Directory for user identity information.		Agents installed on the domain controller or on a member server.	• User name • IP address • Domain	Active Directory Agents, on page 693
Endpoint			WMI	Whether the user is still connected	Endpoint Probe, on page 724

Provider Type (Probe)	Description	Source System (Provider)	Technology	User Identity Information Collected	Document Link
	Always runs in the background in addition to other configured probes, in order to verify whether the user is still connected.				
SPAN	Sits on the network switch in order to listen to network traffic, and extract user identity information based on Active Directory data.		SPAN, installed on the switch, and Kerberos messages	• User name • IP address • Domain	SPAN, on page 701
API providers	Gather user identity information from any system programmed to communicate with a RESTful API client, using the RESTful API service offered by ISE.	Any system programmed to communicate with a REST API client.	RESTful APIs. User identity sent to subscribers in JSON format.	• User name • IP address • Port range • Domain	API Providers, on page 697
Syslog	Parse syslog messages and retrieve user identities, including MAC addresses.	• Regular syslog message providers • DHCP servers	Syslog messages	• User name • IP address • MAC address • Domain	Syslog Providers, on page 703

Note pxGrid sends 200 events per second for session topics to avoid overloading the clients. If the publisher sends more than 200 events, the additional events are queued and sent in next batch.

If pxGrid consistently receives more than 200 events per second for a prolonged period of time, it might consume more memory than usual for storing the backlog events. This might affect the performance of pxGrid.

Active Directory Agents

From the Passive Identity service work center install the native 32-bit application, Domain Controller (DC) agents, anywhere on the Active Directory (AD) domain controller (DC) or on a member server (based on your configurations) to retrieve user identity information from AD and then send those identities to the subscribers you have configured. The Agent probe is a quick and efficient solution when using Active Directory for user identity information. Agents can be installed on a separate domain, or on the AD domain, and once installed, they provide status updates to ISE once every minute.

The agents can be either automatically installed and configured by ISE, or you can manually install them. Upon installation, the following occurs:

- The agent and its associated files are installed at the following path: **`Program Files/Cisco/Cisco ISE PassiveID Agent`**
- A config file called **`PICAgent.exe.config`** is installed indicating the logging level for the agent. You can manually change the logging level from within the config file.
- The CiscoISEPICAgent.log file is stored with all logging messages.
- The nodes.txt file contains the list of all nodes in the deployment with which the agent can communicate. The agent contacts the first node in the list. If that node cannot be contacted, the agent continues to attempt communication according to the order of the nodes in the list. For manual installations, you must open the file and enter the node IP addresses. Once installed (manually or automatically), you can only change this file by manually updating it. Open the file and add, change or delete node IP addresses as necessary.
- The Cisco ISE PassiveID Agent service runs on the machine, which you can manage from the Windows Services dialog box.
- The Active Directory agents are only supported on Windows Server 2008 and higher. If you cannot install agents, then use the Active Directory probe for passive identity services. For more information, see Active Directory as a Probe and a Provider, on page 686.

Note Even if you are running the AD agent on a member server, it still queries the Active Directory for the login requests.

Automatically Install and Deploy Active Directory Agents

When configuring the Agent provider to monitor domain controllers for user identities, the agent must be installed on either a member server or on a domain controller. The agents can be either automatically installed by ISE, or you can manually install them. After installation, automatic or manual, you must then configure the installed agent to monitor specified domain controllers rather than the default WMI. This process describes how to enable automatic installation and configure the agent to monitor a domain controller.

Before you begin

Before you begin:

- Configure reverse lookup for the relevant DNS servers from the server side. For more information about the DNS server configuration requirements for ISE, see DNS Server, on page 650

- Ensure Microsoft .NET Framework is updated for the machine designated for the agents, to a minimum of version 4.0. For more information about the .NET framework, see https://www.microsoft.com/net/framework.
- Active Passive ID and pxGrid services. For more information, see Initial Setup and Configuration, on page 685.
- Create an AD join point and add at least one domain controller. For more information about creating join points, see Active Directory as a Probe and a Provider, on page 686.

  Use AD user groups for the AD, Agents, SPAN and Syslog probes. For more information about AD groups, see Configure Active Directory User Groups, on page 657.

Step 1 Choose **Work Centers** > **PassiveID** > **Providers** and then choose **Agents** from the left panel.

Step 2 To add a new agent, click **Add** from the top of the table.

Step 3 To create the new agent and automatically install it on the host that you indicate in this configuration, select **Deploy New Agent**.

Step 4 Complete all mandatory fields in order to configure the client correctly. For more information, see Active Directory Agent Settings, on page 696.

Step 5 Click **Deploy**.
The agent is automatically installed on the host according to the domain that you indicated in the configuration, and the settings are saved. The agent now also appears in the Agents table and can be applied to monitor specified domain controllers, as described in the following steps.

Step 6 Choose **Work Centers** > **PassiveID** > **Providers** and then choose **Active Directory** from the left panel to view all currently configured join points.

Step 7 Click the link for the join point from which you would like to enable the agent you created.

Step 8 Choose the **Passive ID** tab to configure the domain controllers that you added as part of the prerequisites.

Step 9 Select the domain controller that you would like to monitor with the agent you created and click **Edit**.

Step 10 From the **Protocol** drop-down list, select **Agent**

Step 11 Select the agent you created from the **Agent** drop-down list. Enter the user name and password credentials of the agent that you created, and click **Save**.

The user name and password credentials are used to install the agent on the domain controller. Finally, when you click on **Deploy**, the *picagent.exe* is copied from */opt/pbis/bin* to the specified Windows machine.

Manually Install and Deploy Active Directory Agents

When configuring the Agent provider to monitor domain controllers for user identities, the agent must be installed on either a member server or on a domain controller. The agents can be either automatically installed by ISE, or you can manually install them. After installation, automatic or manual, you must then configure the installed agent to monitor specified domain controllers rather than the default WMI. This process describes how to manually install and configure the agent to monitor a domain controller.

Before you begin

Before you begin:

- Configure reverse lookup for the relevant DNS servers from the server side. For more information about the DNS server configuration requirements for ISE, see DNS Server, on page 650
- Ensure Microsoft .NET Framework is updated for the machine designated for the agents, to a minimum of version 4.0. For more information about the .NET framework, see https://www.microsoft.com/net/framework.
- Active Passive ID and pxGrid services. For more information, see Initial Setup and Configuration, on page 685.
- Create an AD join point and add at least one domain controller. For more information about creating join points, see Active Directory as a Probe and a Provider, on page 686.

  Use AD user groups for the AD, Agents, SPAN and Syslog probes. For more information about AD groups, see Configure Active Directory User Groups, on page 657.

Step 1 Choose **Work Centers** > **PassiveID** > **Providers** and then choose **Agents** from the left panel.

Step 2 Click **Download Agent** to download the `picagent-installer.zip` file for manual installation.
The file is downloaded to your standard Windows Download folder.

Step 3 Place the zip file on the designated host machine and run the installation.

Step 4 From the ISE GUI, again choose **Work Centers** > **PassiveID** > **Providers** and then choose **Agents** from the left panel.

Step 5 To configure a new agent, click **Add** from the top of the table.

Step 6 To configure the agent that you have already installed on the host machine, select **Register Existing Agent**.

Step 7 Complete all mandatory fields in order to configure the client correctly. For more information, see Active Directory Agent Settings, on page 696.

Step 8 Click **Save**.
The agent settings are saved. The agent now also appears in the Agents table and can be applied to monitor specified domain controllers, as described in the following steps.

Step 9 Choose **Work Centers** > **PassiveID** > **Providers** and then choose **Active Directory** from the left panel to view all currently configured join points.

Step 10 Click the link for the join point from which you would like to enable the agent you created.

Step 11 Choose the **Passive ID** tab to configure the domain controllers that you added as part of the prerequisites.

Step 12 Select the domain controller that you would like to monitor with the agent you created and click **Edit**.

Step 13 From the **Protocol** drop-down list, select **Agent**.

Step 14 Select the agent you created from the **Agent** drop-down list. Enter the user name and password to connect to the agent, and click **Save**

The user account must have the necessary permissions to read security events. A user account for a WMI-based agent must have WMI/DCOM permissions.

Uninstall the Agent

Agents, installed automatically or manually, can be easily (manually) uninstalled directly from Windows.

Step 1 From the Windows dialog, go to **Programs and Features**.

Step 2 Find and select the Cisco ISE PassiveID Agent in the list of installed programs.

Step 3 Click **Uninstall**.

Active Directory Agent Settings

Allow ISE to automatically install agents on a specified host in the network in order to retrieve user identity information from different Domain Controllers (DC) and deliver that information to Passive Identity service subscribers.

To create and manage agents, choose **Providers** > **Agents**. See Automatically Install and Deploy Active Directory Agents, on page 693.

Table 82: Agents Window

Field Name	Description
Name	The agent name as you configured it.
Host	The fully qualified domain name of the host on which the agent is installed.
Monitoring	This is a comma separated list of domain controllers that the specified agent is monitoring.

Table 83: Agents New

Field	Description
Deploy New Agent or Register Existing Agent	• Deploy New Agent: Install a new agent on the specified host. **Note** The user must have Domain User and Domain Admin privileges to deploy an agent on the specified host. • Register Existing Agent: Manually install the agent on the host and then configure that agent from this screen for Passive Identity service to enable the service.
Name	Enter a name by which you can easily recognize the agent.
Description	Enter a description by which you can easily recognize the agent.
Host FQDN	This is the fully qualified domain name for the host on which the agent is installed (register existing agent), or is to be installed (automatic deployment).
User Name	Enter your user name in order to access the host on which to install the agent. Passive Identity service uses these credentials in order to install the agent for you. The user account must have permissions to connect remotely and install the PIC agent.
Password	Enter your user password in order to access the host on which to install the agent. Passive Identity service uses these credentials in order to install the agent for you.

API Providers

The API Providers feature in Cisco ISE enables you to push user identity information from your customized program or from the terminal server (TS)-Agent to the built-in ISE passive identity services REST API service. In this way, you can customize a programmable client from your network to send user identities that were collected from any network access control (NAC) system to the service. Furthermore, the Cisco ISE API provider enables you to interface with network applications such as the TS-Agent on a Citrix server, where all users have the same IP address but are assigned unique ports.

For example, an agent running on a Citrix server that provides identity mappings for users authenticated against an Active Directory (AD) server can send REST requests to ISE to add or delete a user session whenever a new user logs in or off. ISE then takes the user identity information, including the IP address and assigned ports, delivered from the client and sends it to pre-configured subscribers, such as the Cisco Firepower Management Center (FMC).

The ISE REST API framework implements the REST service over the HTTPS protocol (no client certificate validation necessary) and the user identity information is delivered in JSON (JavaScript Object Notation) format. For more information about JSON, see http://www.json.org/ .

The ISE REST API service parses user identities and in addition, maps that information to port ranges, in order to distinguish between the different users logged in simultaneously to one system. Everytime a port is allocated to a user, the API sends a message to ISE.

The REST API Provider Flow

After you have configured a bridge to your customized client from ISE by declaring that client as a Provider for ISE and enabling that specific customized program (the client) to send RESTful requests, the ISE REST service works in the following way:

1. For client authentication, Cisco ISE requires an authentication token. A customized program on the client machine sends a request for an authentication token when initiating contact and then every time ISE notifies that the previous token has expired. The token is returned in response to the request, enabling ongoing communication between the client, and the ISE service.
2. After a user has logged into the network, the client retrieves user identity information and posts that information to the ISE REST service using the API Add command.
3. Cisco ISE receives and maps the user identity information.
4. Cisco ISE sends the mapped user identity information to the subscriber.
5. Whenever necessary, the customized machine can send a request to remove user information by sending a Remove API call and including the user ID received as the response when the Add call was sent.

Work with REST API Providers in ISE

Follow these steps to activate the REST service in ISE:

1. Configure the client side. For more information, see the client user documentation.
2. Activate Passive ID and pxGrid services. For more information, see Initial Setup and Configuration, on page 685.
3. Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from ISE. For more information about the DNS server configuration requirements for , see DNS Server, on page 650

4. See Configure a Bridge to the ISE REST Service for Passive Identity Services, on page 698.

Note To configure the API Provider to work with a TS-Agent add the TS-Agent information when creating a bridge from ISE to that agent, and then consult with the TS-Agent documentation for information about sending API calls.

5. Generate an authentication token and send add and remove requests to the API service.

Configure a Bridge to the ISE REST Service for Passive Identity Services

In order to enable the ISE REST API service to receive information from a specific client, you must first define the specific client from Cisco ISE. You can define multiple REST API clients with different IP addresses.

Before you begin

Before you begin:

- Ensure you have activated Passive ID and pxGrid services. For more information, see Initial Setup and Configuration, on page 685.
- Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from Cisco ISE. For more information about the DNS server configuration requirements for Cisco ISE, see DNS Server, on page 650

Step 1 Choose **Work Centers** > **PassiveID** > **Providers** and then choose **API Providers** from the left panel
The API Providers table is displayed, including status information for each existing client.

Step 2 To add a new client, click **Add** from the top of the table.

Step 3 Complete all mandatory fields in order to configure the client correctly. For more information, see API Provider Settings, on page 699.

Step 4 Click **Submit**.
The client configuration is saved and the screen displays the updated API Providers table. The client can now send posts to the ISE REST service.

What to do next

Set up your customized client to post authentication tokens and user identities to the ISE REST service. See Send API Calls to the Passive ID REST Service, on page 698.

Send API Calls to the Passive ID REST Service

Before you begin

Configure a Bridge to the ISE REST Service for Passive Identity Services, on page 698

Step 1 Enter the Cisco ISE URL in the address bar of your browser (for example, *https://<ise hostname or ip address>/admin/*)

Step 2 Enter the username and password that you specified and configured from the **API Providers** window. For more information, see Configure a Bridge to the ISE REST Service for Passive Identity Services, on page 698.

Step 3 Press **Enter**.

Step 4 Enter the API call in the URL Address field of the target node.

Step 5 Click **Send** to issue the API call.

What to do next

See API Calls, on page 699 for more information and details about the different API calls, their schemas and their results.

API Provider Settings

Note The full API definition and object schemas can be retrieved with a request call as follows:

- For the full API specifications (wadl)—https://YOUR_ISE:9094/application.wadl
- For the API model and object schemas—https://YOUR_ISE:9094/application.wadl/xsd0.xsd

Table 84: API Providers Settings

Field	Description
Name	Enter a unique name for this client that distinguishes it quickly and easily from other clients.
Description	Enter a clear description of this client.
Status	Select **Enabled** to enable the client to interact with the REST services immediately upon completing configuration.
Host/ IP	Enter the IP address for the client host machine. Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from ISE.
User name	Create a unique user name to be used when posting to the REST service.
Password	Create a unique password to be used when posting to the REST service.

API Calls

Use these API calls to manage user identity events for Passive Identity services with Cisco ISE.

Purpose: Generate Authentication Token

- **Request**

  POST

  https://<PIC IP address>:9094/api/fmi_platform/v1/identityauth/generatetoken

The request should contain the BasicAuth authorization header. Provide the API provider's credentials as previously created from the ISE-PIC GUI. For more information see API Provider Settings, on page 699.

- **Response Header**

  The header includes the X-auth-access-token. This is the token to be used when posting additional REST requests.

- **Response Body**

  HTTP 204 No Content

Purpose: Add User

- **Request**

  POST

  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity

  Add X-auth-access-token in the header of the POST request, for example, Header: X-auth-access-token, Value: f3f25d81-3ac5-43ee-bbfb-20955643f6a7

- **Response Header**

  201 Created

- **Response Body**

  ```
  {
  "user": "<username>",
  "srcPatRange": {
  "userPatStart": <user PAT start value>,
  "userPatEnd": <user PAT end value>,
  "patRangeStart": <PAT range start value>
  },
  "srcIpAddress": "<src IP address>",
  "agentInfo": "<Agent name>",
  "timestamp": "<ISO_8601 format i.e. “YYYY-MM-DDTHH:MM:SSZ" >",
  "domain": "<domain>"
  }
  ```

- **Notes**

  - srcPatRange can be removed in above json to create a single IP user binding.
  - Response body contains the "ID" which is the unique identifier for the user session binding created. Use this ID when sending a DELETE request to indicate which user should be removed.
  - This reponse also contains the self link which is the URL for this newly created user session binding.

Purpose: Remove User

- **Request**

  DELETE

  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity/<id>

  In <id> enter the ID as was received from the Add response.

  Add the X-auth-access-token in the header of the DELETE request, for example, Header: X-auth-access-token, Value: f3f25d81-3ac5-43ee-bbfb-20955643f6a7

- **Response Header**

  200 OK

- **Response Body**

  Response body contains the details about the user session binding which got deleted.

SPAN

SPAN is a Passive Identity service that allows you to quickly and easily enable Cisco ISE to listen to the network and retrieve user information without having to configure Active Directory to work directly with Cisco ISE. SPAN sniffs network traffic, specifically examining Kerberos messages, extracts user identity information also stored by Active Directory and sends that information to ISE. ISE then parses the information, ultimately delivering user name, IP address and domain name to the subscribers that you have also already configured from ISE.

In order for SPAN to listen to the network and extract Active Directory user information, ISE and Active Directory must both be connected to the same switch on the network. In this way, SPAN can copy and mirror all user identity data from Active Directory.

With SPAN, user information is retrieved in the following way:

1. The user endpoint logs in to the network.
2. Log in and user data are stored in Kerberos messages.
3. When the user logs in and the user data passes through the switch, SPAN mirrors the network data.
4. Cisco ISE listens to the network for user information and retrieves the mirrored data from the switch.
5. Cisco ISE parses the user information and updates passive ID mappings.
6. Cisco ISE delivers the parsed user information to the subscribers.

Working with SPAN

Before you begin

In order to enable ISE to receive SPAN traffic from a network switch, you must first define which nodes and node interfaces are to listen to the switch. You can configure SPAN in order to listen to the different installed ISE nodes. For each node, only one interface can be configured to listen to the network and the interface used to listen must be dedicated to SPAN only.

Before you begin, ensure you have activated Passive ID and pxGrid services. Only nodes for which Passive ID has been turned on will appear in the list of available interfaces for configuring SPAN. For more information, see Initial Setup and Configuration, on page 685.

In addition, you must:

- Ensure Active Directory is configured on your network.
- Run a CLI on the switch in the network that is also connected to Active Directory in order to ensure the switch can communicate with ISE.
- Configure the switch to mirror the network from AD.
- Configure a dedicated ISE network interface card (NIC) for SPAN. This NIC is used only for SPAN traffic.
- Ensure the NIC that you have dedicated to SPAN is activated via the command line interface.
- Create a VACL that sends only Kerberos traffic into the SPAN port.

Step 1 Choose **Work Centers** > **PassiveID** > **Providers** and then choose **SPAN** from the left panel to configure SPAN.

Step 2

Note We recommend that the GigabitEthernet0 network interface card (NIC) remain available and that you select any other available NIC for configuring SPAN. GigabitEthernet0 is used for system management purposes.

Enter a meaningful description (optional), select status **Enabled**, and choose the nodes and the relevant NICs that will be used to listen to the network switch. For more information, see SPAN Settings, on page 702.

Step 3 Click **Save**.

The SPAN configuration is saved and ISE-PIC ISE is now actively listening to network traffic.

SPAN Settings

From each node that you have deployed, quickly and easily configure ISE to receive user identities by installing SPAN on a client network.

Table 85: SPAN Settings

Field	Description
Description	Enter a unique description to remind you of which nodes and interfaces are currently enabled.
Status	Select **Enabled** to enable the client immediately upon completing configuration.
Interface NIC	Select one or more of the nodes installed for ISE, and then for each selected node, choose the node interface that is to listen to the network for information. **Note** We recommend that the GigabitEthernet0 NIC remain available and that you select any other available NIC for configuring SPAN. GigabitEthernet0 is used for system management purposes.

Syslog Providers

Passive Identity service parses syslog messages from any client (identity data provider) that delivers syslog messages, including regular syslog messages (from providers such as InfoBlox, Blue Coat, BlueCat, and Lucent) as well as DHCP syslog messages, and sends back user identity information, including MAC addresses. This mapped user identity data is then delivered to subscribers.

You can specify the syslog clients from which to receive the user identity data (see Configure Syslog Clients, on page 703). While configuring the provider, you must specify the connection method (TCP or UDP) and the syslog template to be used for parsing.

Note When TCP is the configured connection type, if there is a problem with the message header and the host name cannot be parsed, ISE attempts to match the IP address received in the packet to the IP address of any of the providers in the list of providers that have already been configured for Syslog messages in ISE. To view this list, choose **Work Centers** > **PassiveID** > **Providers** > **Syslog Providers**. We recommend that you check the message headers and customize if necessary to guarantee parsing succeeds. For more information about customizing headers, see Customize Syslog Headers, on page 708.

The syslog probe sends syslog messages that are received to the ISE parser, which maps the user identity information, and publishes that information to ISE. ISE then delivers the parsed and mapped user identity information to the Passive Identity service subscribers.

To parse syslog messages for user identity from ISE-PIC ISE:

- Configure syslog clients from which to receive user identity data. See Configure Syslog Clients, on page 703.
- Customize a single message header. See Customize Syslog Headers, on page 708.
- Customize message bodies by creating templates. See Customize the Syslog Message Body, on page 708.
- Use the message templates pre-defined in ISE when configuring your syslog client as the message template used for parsing, or base your customized header or body templates on these pre-defined templates. See Work with Syslog Predefined Message Templates, on page 712.

Configure Syslog Clients

In order to enable Cisco ISE to listen to syslog messages from a specific client, you must first define the specific client from Cisco ISE. You can define multiple providers with different IP addresses.

Before you begin

Before you begin, ensure you have activated Passive ID and pxGrid services. For more information, see Initial Setup and Configuration, on page 685.

Step 1 Choose **Work Centers** > **PassiveID** > **Providers** and then choose **Syslog Providers** from the left panel.
The Syslog Providers table is displayed, including status information for each existing client.

Step 2 To configure a new syslog client, click **Add** from the top of the table.

Step 3 Complete all mandatory fields (see Syslog Settings, on page 704 for more details) and create a message template if necessary (see Customize the Syslog Message Body, on page 708 for more details) to configure the client correctly.

Step 4 Click **Submit**.

Syslog Settings

Configure Cisco ISE to receive user identities, including MAC addresses, by way of syslog messages from a specific client. You can define multiple providers with different IP addresses.

Table 86: Syslog Providers

Field Name	Description
Name	Enter a unique name that distinguishes this configured client quickly and easily.
Description	A meaningful description of this Syslog provider.
Status	Select **Enabled** to enable the client immediately upon completing configuration.
Host	Enter the FQDN of the host machine.
Connection Type	Enter UDP or TCP to indicate the channel by which ISE listens for syslog messages. **Note** When TCP is the configured connection type, if there is a problem with the message header and the host name cannot be parsed, then Cisco ISE attempts to match the IP address received in the packet to the IP address of any of the providers in the list of providers that have already been configured for Syslog messages in Cisco ISE. To view this list, choose **Work Centers** > **PassiveID** > **Providers** > **Syslog Providers**. We recommend that you check the message headers and customize if necessary to ensure that parsing succeeds. For more information about customizing headers, see Customize Syslog Headers, on page 708.

Field Name	Description
Template	

Field Name	Description
	A template indicates precise body message structure so that the parser can identify the pieces of information within the syslog message that should be parsed, mapped and delivered. For example, a template can indicate the exact position of the user name so that the parser can find the user name in every message received. From this field, indicate the template (for the body of the syslog message) to be used in order to recognize and correctly parse the syslog message. Choose either from the pre-defined dropdown list, or click **New** to create your own customized template. For more information about creating new templates, see Customize the Syslog Message Body, on page 708. Most of the pre-defined templates use regular expressions, and customized templates should also use regular expressions. **Note** Only customized templates can be edited or removed, while pre-defined system templates in the dropdown cannot be altered. ISE currently offers these pre-defined DHCP provider templates: • InfoBlox • BlueCat • Lucent_QIP • DHCPD • MSAD DHCP **Note** DHCP syslog messages do not contain user names. Therefore, these messages are delivered from the parser with a delay so that Cisco ISE can first check users registered in the local session directory (displayed from Live Sessionss) and attempt to match those users by their IP addresses to the IP addresses listed in the DHCP syslog messages received, in order to correctly parse and deliver user identity information. If the data received from a DHCP syslog message cannot be matched to any of the currently logged in users, then the message is not parsed and user identity is not delivered. Cisco ISE offers these pre-defined regular syslog provider templates: • ISE • ACS • F5_VPN • ASA_VPN • Blue Coat • Aerohive • Safe connect_NAC

Field Name	Description
	• Nortel_VPN For information about templates, see Work with Syslog Predefined Message Templates, on page 712.
Default Domain	If the domain is not identified in the syslog message for the specific user, this default domain is automatically assigned to the user in order to ensure that all users are assigned a domain. With the default domain or with the domain that was parsed from the message, the user name is appended to username@domain, thereby including that domain, in order to get more information about the user and user groups.

Customize Syslog Message Structures (Templates)

A template indicates precise message structure so that the parser can identify the pieces of information within the syslog message that should be parsed, mapped and delivered. For example, a template can indicate the exact position of the user name so that the parser can find the user name in every message received. Templates determine the supported structures for both new and remove mapping messages.

Cisco ISE enables you to customize a single message header and multiple body structures, to be used by the Passive ID parser.

The templates should include regular expressions to define the structure for user name, IP address, MAC address and domain in order to enable the Passive ID parser to correctly identify whether the message is to add or remove user identity mapping and to correctly parse the user details.

When customizing your message templates, you can choose to base your customization on the message templates pre-defined in ISE-PIC ISE by consulting with the regular expressions and message structures used within those pre-defined options. For more information about the pre-defined template regular expressions, message structures, examples and more, see Work with Syslog Predefined Message Templates, on page 712.

You can customize:

- A single message header—Customize Syslog Headers, on page 708
- Multiple message bodies—Customize the Syslog Message Body, on page 708.

Note DHCP syslog messages do not contain user names. Therefore, these messages are delivered from the parser with a delay so that Cisco ISE can first check users registered in the local session directory (displayed from Live Sessionss) and attempt to match those users by their IP addresses to the IP addresses listed in the DHCP syslog messages received, in order to correctly parse and deliver user identity information. If the data received from a DHCP syslog message cannot be matched to any of the currently logged in users, then the message is not parsed and user identity is not delivered.

The delay necessary to properly match, parse and map details from DHCP messages cannot be applied to customized templates, and therefore it is not recommended that DHCP message templates be customized. Instead, use any of the pre-defined DHCP templates.

Customize the Syslog Message Body

Cisco ISE enables you to customize your own syslog message templates (by customizing the message body) to be parsed by the Passive ID parser. The templates should include regular expressions to define the structure for user name, IP address, MAC address and domain.

Note DHCP syslog messages do not contain user names. Therefore, these messages are delivered from the parser with a delay so that Cisco ISE can first check users registered in the local session directory (displayed from Live Sessionss) and attempt to match those users by their IP addresses to the IP addresses listed in the DHCP syslog messages received, to correctly parse and deliver user identity information. If the data received from a DHCP syslog message cannot be matched to any of the currently logged in users, then the message is not parsed and user identity is not delivered.

The delay necessary to properly match, parse and map details from DHCP messages cannot be applied to customized templates, and therefore it is not recommended that DHCP message templates be customized. Instead, use any of the pre-defined DHCP templates.

Create and edit syslog message body templates from within the syslog client configuration screen.

Note You can only edit your own customized templates. Pre-defined templates offered by the system cannot be changed.

Step 1 Choose **Work Centers** > **PassiveID** > **Providers** and then choose **Syslog Providers** from the left panel.
The Syslog Providers table is displayed, including status information for each existing client.

Step 2 Click **Add** to add a new syslog client or **Edit** to update an already configured client. For more information about configuring and updating syslog clients, see Configure Syslog Clients, on page 703.

Step 3 In the **Syslog Providers** window, click **New** to create a new message template. To edit an existing template, select the template from the dropdown list and click **Edit**.

Step 4 Complete all mandatory fields.

For information about how to enter the values correctly, see Syslog Customized Template Settings and Examples, on page 710.

Step 5 Click **Test** to ensure the message is correctly parsed based on the strings you have entered.

Step 6 Click **Save**.

Customize Syslog Headers

Syslog headers also contain the host name from which the message originated. If your syslog messages are not recognized by the Cisco ISE message parser, you may need to customize the message header by configuring the delimiter that proceeds the host name, thereby enabling Cisco ISE to recognize the host name and parse the message correctly. For more details about the fields in this screen, see Syslog Customized Template Settings and Examples, on page 710. The customized header configuration is saved and added to the header types that are used by the parser whenever messages are received.

Note You can only customize a single header. After you customize a header, when you click **Custom Header** and create a template, only the newest configuration is saved.

Step 1 Choose **Work Centers** > **PassiveID** > **Providers** and then choose **Syslog Providers** from the left panel.
The Syslog Providers table is displayed, including status information for each existing client.

Step 2 Click **Custom Header** to open the Syslog Custom Header screen.

Step 3 In the **Paste sample syslog** field, enter an example of the header format in your syslog messages. For example, copy and paste this header from one of your messages: **`<181>Oct 10 15:14:08 Cisco.com`**.

Step 4 In the **Separator** field, indicate whether words are separated by spaces or tabs.

Step 5 In the **Position of hostname in header** field, indicate which place in the header is the host name. For example, in the header offered above, the host name is the fourth word in the header. Enter 4 to indicate this.

The **Hostname** field displays the host name based on the details indicated in the first three fields. For example, if the header example in **Paste sample syslog** is as follows:

<181>Oct 10 15:14:08 Cisco.com

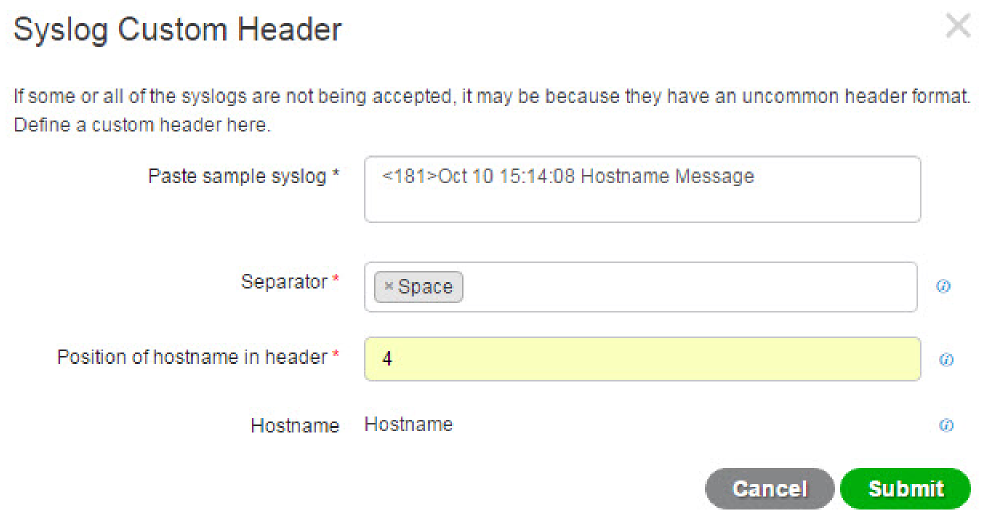
The separator is indicated as **Space** and the **Position of hostname in header** is entered as 4.

The **Hostname** will automatically appear as Cisco.com, which is the fourth word in the header phrase pasted in the **Paste sample syslog** field.

If the host name is incorrectly displayed, check the data you have entered in the **Separator** and **Position of hostname in header** fields.

This example is as in the following screen capture:

Figure 23: Customize Syslog Headers



Syslog Custom Header

If some or all of the syslogs are not being accepted, it may be because they have an uncommon header format.
Define a custom header here.

Paste sample syslog * <181>Oct 10 15:14:08 Hostname Message

Separator * Space

Position of hostname in header * 4

Hostname Hostname

Step 6 Click **Submit**.

The customized header configuration is saved and added to the header types that are used by the parser whenever messages are received.

Syslog Customized Template Settings and Examples

Cisco ISE enables you to customize your own syslog message templates to be parsed by the Passive ID parser. Customized templates determine the supported structures for both new and remove mapping messages. The templates should include regular expressions to define the structure for user name, IP address, MAC address and domain in order to enable the Passive ID parser to correctly identify whether the message is to add or remove user identity mapping and to correctly parse the user details.

Note Most of the pre-defined templates use regular expressions. Customized templates should also use regular expressions.

Syslog Header Parts

You can customize a single header that is recognized by the Syslog probe by configuring the delimiter that proceeds the host name.

The following table describes the different parts and fields that can be included in your customized syslog header. For more information about regular expressions, see Table 89: Regular Expressions for Customized Templates, on page 712.

Table 87: Syslog Custom Header

Field	Description
Paste sample syslog	Enter an example of the header format in your syslog messages. For example, copy and paste this header: `<181>Oct 10 15:14:08 Hostname Message`
Separator	Indicate whether words are separated by spaces or tabs.
Position of hostname in header	Indicate which place in the header is the host name. For example, in the header offered above, the host name is the fourth word in the header. Enter 4 to indicate this.
Hostname	Displays the hostname based on the details indicated in the first three fields. For example, if the header example in **Paste sample syslog** is as follows: <181>Oct 10 15:14:08 Hostname Message The separator is indicated as **Space** and the **Position of hostname in header** is entered as 4. The **Hostname** will automatically appear as Hostname. If the host name is incorrectly displayed, check the data you have entered in the **Separator** and **Position of hostname in header** fields.

Syslog Template Parts and Descriptions for the Message Body

The following table describes the different parts and fields that can be included in your customized syslog message templates. For more information about regular expressions, see Table 89: Regular Expressions for Customized Templates, on page 712.

Table 88: Syslog Template

Part	Field	Description
	Name	A unique name by which to recognize the purpose of this template.
Mapping Operations	New Mapping	A regular expression that describes the kind of mapping used with this template to add a new user. For example, enter "logged on from" in this field to indicate a new user that has logged on to the F5 VPN.
	Removed Mapping	A regular expression that describes the kind of mapping used with this template to remove a user. For example, enter "session disconnect" in this field to indicate a user that should be removed for ASA VPN.
User Data	IP Address	A regular expression that indicates the IP addresses to be captured. For example, for Bluecat messages, to capture identities for users within this IP address range, enter: (on\s|to\s)((?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?))
	User Name	A regular expression that indicates the user name format to be captured.
	Domain	A regular expression that indicates the domain to be captured.
	Mac Address	A regular expression that indicates the MAC address format to be captured.

Regular Expression Examples

In order to parse messages use regular expressions. This sections offers regular expression examples in order to parse IP address, user name and add mapping messages.

For example, use regular expressions to parse the following messages:

<174>192.168.0.1 %ASA-4-722051: Group <DfltGrpPolicy> User <user1> IP <192.168.0.10> IPv4 Address <192.168.0.6> IPv6 address <::> assigned to session

<174>192.168.0.1 %ASA-6-713228: Group = xyz, Username = user1, IP = 192.168.0.12, Assigned private IP address 192.168.0.8 to remote user

The regular expressions are as defined in the following table.

Table 89: Regular Expressions for Customized Templates

Part	Regular Expression
IP address	Address <([^\s]+)>|address ([^\s]+)
User name	User <([^\s]+)>| Username = ([^\s]+)
Add mapping message	(%ASA-4-722051|%ASA-6-713228)

Work with Syslog Predefined Message Templates

Syslog messages have a standard structure which include a header and the message body.

The predefined templates offered by Cisco ISE are described in this section, including content details for the headers that are supported, as well as the supported body structure, based on the origin of the messages.

In addition, you can create your own templates with customized body content for sources that are not predefined in the system. The supported structure for customized templates is also described in this section. You can configure a single customized header to be used in addition to the headers predefined in the system, when parsing messages, and you can configure multiple customized templates for the message body. For more information about customizing the header, see Customize Syslog Headers, on page 708. For more information about customizing the body, see Customize the Syslog Message Body, on page 708.

Note Most of the predefined templates use regular expressions, and customized templates should also use regular expressions.

Message Headers

There are two header types recognized by the parser, for all message types (new and remove), for all client machines. These headers are as follows:

- <171>Host message
- <171>Oct 10 15:14:08 Host message

Once received, the header is parsed for host name, which can be IP address, hostname, or full FQDN.

Headers can also be customized. To customize your headers, see Customize Syslog Headers, on page 708.

Syslog ASA VPN Pre-Defined Template

The supported syslog message format and types for ASA VPN are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 712.

New Mapping Body Messages

There are different ASA VPN body messages that are recognized by the parser as described in the following table.

Body Message	Parsing Example
%ASA-6-109005 Authentication succeeded for user UserA from 10.0.0.11/100 to 10.10.11.11/20 on interface eth1/1	[UserA,10.0.0.11]
%ASA-6-602303 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.0.0.11 (UserA) has been created.	
%ASA-6-721016 (device) WebVPN session for client user UserA, IP 10.0.0.11 has been created.	
%ASA-6-603104 PPTP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11,ffg123 #% UserA is UserA, MPPE_key_strength is string	
%ASA-6-603106 L2TP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11, UserA is user	

Body Message	Parsing Example
%ASA-6-113039 Group group User UserA IP 10.0.0.11 AnyConnect parent session started.	
%ASA-6-802001 User UserA IP 10.100.1.1 OS os_name UDID number MDM action session started.	
%ASA-6-713228: Group = xyz, UserA = xxxx227, IP = 192.168.0.11, Assigned private IP address 172.16.0.11 to remote user	[UserA,172.16.0.11] **Note** The parsed IP address from this message type is the private IP address, as indicated in the message.
%ASA-4-722051: Group <DfltGrpPolicy> User <UserA> IP <172.16.0.12> IPv4 Address <172.16.0.21> IPv6 address <::> assigned to session	[UserA,172.16.0.12] **Note** The parsed IP address from this message type is the IPv4 address.

Remove Mapping Body Messages

The Remove Mapping messages supported for ASA VPN by the parser are as described in this section.

Once received, the body is parsed for user details as follows:

[UserA,10.1.1.1]

Body Message
%ASA-4-113019 Group = group, UserA = UserA, IP = 10.1.1.1, Session disconnected. Session Type: type, Duration:\ duration, Bytes xmt: count,Bytes rcv: count, Reason: reason
%ASA-4-717052 Group group name User UserA IP 10.1.1.1 Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name\ Serial Number id serial number
%ASA-6-602304 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.1.1.1 (UserA) has been deleted.

Body Message
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.
%ASA-4-722049 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled or invalid image on the ASA
%ASA-4-722050 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled for the user.
%ASA-6-802002 User UserA IP 10.1.1.1 OS os_name UDID number MDM action session terminated.
%ASA-3-716057 Group group User UserA IP 10.1.1.1 Session terminated, no type license available.
%ASA-3-722046 Group group User UserA IP 10.1.1.1 Session terminated: unable to establish tunnel.
%ASA-4-113035 Group group User UserA IP 10.1.1.1 Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.
%ASA-4-716052 Group group-name User UserA IP 10.1.1.1 Pending session terminated.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.

Syslog Bluecat Pre-Defined Template

The supported syslog message format and types for Bluecat are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 712.

New Mapping Body Messages

The messages supported for New Mapping for Bluecat syslog are as described in this section.

Once received, the body is parsed for user details as follows:

[macAddress=nn:xx:nn:ca:xx:nn,ip=172.16.0.12]

Body
Nov 7 23:37:32 xx-campus1 dhcpd: DHCPACK on 172.16.0.13 to nn:xx:nn:ca:xx:nn via 172.16.0.17

Remove Mapping Messages

There are no remove mapping messages known for Bluecat.

Syslog F5 VPN Pre-Defined Template

The supported syslog message format and types for F5 VPN are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 712.

New Mapping Body Messages

There are different F5 VPN body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

[user=UserA,ip=172.16.0.12]

Body
Apr 10 09:33:58 Oct 2 08:28:32 abc.xyz.org security[nnnnn]: [UserA@vendor-abcr] User UserA logged on from 172.16.0.21 to \ 172.16.0.12 Sid = xyz\

Remove Mapping Messages

Currently there are no remove messages for F5 VPN that are supported.

Syslog Infoblox Pre-Defined Template

The supported syslog message format and types for Infoblox are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 712.

New Mapping Body Messages

There are different ASA VPN body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

[macAddress= nn:xx:xx:xx:nn:nn,ip=10.0.10.100]

Body Message
Nov 15 11:37:26 user1-lnx dhcpd[3179]: DHCPACK on 10.0.0.14 to nn:xx:xx:nx:nn:nn (android-df67ddcbb1271593) via eth2 relay 10.0.0.24 lease-duration 3600
Nov 15 11:38:11 user1-lnx dhcpd[3179]: DHCPACK on 172.16.0.18 to nn:xx:xx:xn:nn:nn (DESKTOP-HUDGAAQ) via eth2 relay 172.16.0.13 lease-duration 691200 (RENEW)
Nov 15 11:38:11 192.168.0.12 dhcpd[25595]: DHCPACK to 10.0.0.11 (nn:xx:xx:xn:nn:nx) via eth1

Remove Mapping Messages

Once received, the body is parsed for user details as follows:

- If MAC address is included:

  [00:0c:29:a2:18:34,10.0.10.100]

- If MAC address is not included:

  [10.0.10.100]

Body Message
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPEXPIRE 10.0.10.100 has expired
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 \ (win10) via eth1 uid 01:00:0c:29:a2:18:34
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[25595]: RELEASE on 10.20.31.172 to c0:ce:cd:44:4f:bd

Syslog Linux DHCPd3 Pre-Defined Template

The supported syslog message format and types for Linux DHCPd3 are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 712.

New Mapping Messages

There are different Linux DHCPd3 body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

[macAddress=24:ab:81:ca:f2:72,ip=172.16.0.21]

Body Message
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 to 00:0c:29:a2:18:34 (win10) via eth1
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 (00:0c:29:a2:18:34) via eth1

Remove Mapping Body Messages

The Remove Mapping messages supported for Linux DHCPd3 by the parser are as described in this section.

Once received, the body is parsed for user details as follows:

[00:0c:29:a2:18:34 ,10.0.10.100]

Body Message
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPEXPIRE 10.0.10.100 has expired
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 (win10) via eth1

Syslog MS DHCP Pre-Defined Template

The supported syslog message format and types for MS DHCP are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 712.

New Mapping Body Messages

There are different MS DHCP body messages that are recognized by the parser as described in the following table.

Once received, the parser divides data by searching for the comma (,) and then messages of these formats are parsed as in the following example:

[macAddress=000C29912E5D,ip=10.0.10.123]

Body Message
Nov 11 23:37:32 10,07/21/16,16:55:22,Assign,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,724476048,0,,,,,0x4D53465420352E30,MSFT,5.0

Remove Mapping Body Messages

The Remove Mapping messages supported for MS DHCP by the parser are as described in this section.

Once received, the parser divides data by searching for the comma (,) and then messages of these formats are parsed as in the following example:

[macAddress=000C29912E5D,ip=10.0.10.123]

Body Message
Nov 11 23:37:32 12,07/21/16,16:55:18,Release,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,3128563632,\ 0,,,,,,,,,0

Syslog SafeConnect NAC Pre-Defined Template

The supported syslog message format and types for SafeConnect NAC are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 712.

New Mapping Body Messages

There are different SafeConnect NAC body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

[user=galindk1i,p=xxxx.xx.xxx.xxd,domain=Resnet-Macs]

<table>
<tr><th>Body Message</th></tr>
<tr><td>Apr 10 09:33:58 nac Safe*Connect: authenticationResult|xxx.xx.xxx.xxx|xxx.xx.xxx.xxx|UserA|true|Resnet-Macs|TCNJ-Chain|001b63b79018|MAC</td></tr>
</table>

Remove Mapping Messages

Currently there are no remove messages for Safe Connect that are supported.

Syslog Aerohive Pre-Defined Templates

The supported syslog message format and types for Aerohive are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 712.

New Mapping Body Messages

There are different Aerohive body messages that are recognized by the parser as described in the following table.

Details parsed from the body include user name and IP address. The regular expression used for parsing is as in the following examples:

- `New mapping—auth\:`
- `IP—ip ([A-F0-9a-f:.]+)`
- `User name—UserA ([a-zA-Z0-9\_]+)`

Once received, the body is parsed for user details as follows:

[UserA,10.5.50.52]

Body Message
2013-04-01 14:06:05 info ah auth: Station 1cab:a7e6:cf7f ip 10.5.50.52 UserA UserA

Remove Mapping Messages

Currently the system does not support remove mapping messages from Aerohive.

Syslog Blue Coat Pre-Defined Templates—Main Proxy, Proxy SG, Squid Web Proxy

The system supports the following message types for Blue Coat:

- BlueCoat Main Proxy
- BlueCoat Proxy SG
- BlueCoat Squid Web Proxy

The supported syslog message format and types for Bluecoat messages are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 712.

New Mapping Body Messages

There are different Blue Coat body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

[UserA,192.168.10.24]

Body Message (this example is taken from a BlueCoat Proxy SG message)
2016-09-21 23:05:33 58 10.0.0.1 UserA - - PROXIED "none" http://www.example.com/ 200 TCP_MISS GET application/json;charset=UTF-8 http site.api.example.com 80 /apis/v2/scoreboard/header ?rand=1474499133503 - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36 Edge/13.10586" 192.168.10.24 7186 708 - "unavailable

The following table describes the different regular expression structures used per client for new mapping messages.

<table>
<tr><th>Client</th><th>Regular expressions</th></tr>
<tr><td>BlueCoat Main Proxy</td><td>New mapping
(TCP_HIT|TCP_MEM){1}
IP
\s((?:(?:[0-9]{1,3}\.){3}[0-9]{1,3})|(?:(?:[a-zA-Z0-9]{1,4}\:{1,2}){1,7}[a-zA-Z0-9]{1,4}))\s
User name
\s\-\s([a-zA-Z0-9_]+)\s\-\s</td></tr>
<tr><td>BlueCoat Proxy SG</td><td>New mapping
(\-\sPROXIED){1}
IP
\s((?:(?:[0-9]{1,3}\.){3}[0-9]{1,3})|(?:(?:[a-zA-Z0-9]{1,4}\:{1,2}){1,7}[a-zA-Z0-9]{1,4}))\s[a-zA-Z0-9_]+\s\-
User name
\s[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\s([a-zA-Z0-9_]+)\s\-</td></tr>
<tr><td>BlueCoat Squid Web Proxy</td><td>New mapping
(TCP_HIT|TCP_MEM){1}
IP
\s((?:(?:[0-9]{1,3}\.){3}[0-9]{1,3})|(?:(?:[a-zA-Z0-9]{1,4}\:{1,2}){1,7}[a-zA-Z0-9]{1,4}))\sTCP
User name
\s([a-zA-Z0-9\._]+)\s\-\/</td></tr>
</table>

Remove Mapping Messages

Remove mapping messages are supported for Blue Coat clients, though no examples are currently available.

The following table describes the different known regular expression structure examples used per client for remove mapping messages.

Client	Regular expressions
BlueCoat Main Proxy	**(TCP_MISS|TCP_NC_MISS){1}**
BlueCoat Proxy SG	No example currently available.
BlueCoat Squid Web Proxy	**(TCP_MISS|TCP_NC_MISS){1}**

Syslog ISE and ACS Pre-Defined Templates

When listening to ISE or ACS clients, the parser receives the following message types:

- Pass authentication: When the user is authenticated by ISE or ACS, the pass authentication message is issued notifying that authentication succeeded, and including user details. The message is parsed and the user details and session ID are saved from this message.
- Accounting start and accounting update messages (new mapping): The accounting start or accounting update message is parsed with the user details and session ID that were saved from the Pass Authentication message and then the user is mapped.
- Accounting stop (remove mapping): The user mapping is deleted from the system.

The supported syslog message format and types for ISE and ACS are as described below.

Pass Authentication Messages

The following messages are supported for Pass Authentication.

- **Header**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  For example: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **Body**

  Passed-Authentication 000011 1 0 2016-05-09 12:48:11.011 +03:00 0000012435 5200 NOTICE Passed-Authentication: Authentication succeeded, ConfigVersionId=104, Device IP Address=10.0.0.12, DestinationIPAddress=10.0.0.18, DestinationPort=1812, UserA=UserA, Protocol=Radius, RequestLatency=45, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Session-Timeout=90, Calling-Station-ID=, cisco-av-pair=audit-session-id=5

- **Parsing Example**

  User name and session ID only are parsed.

  [UserA,5]

Accounting Start/Update (New Mapping) Messages

The following messages are supported for New Mapping.

- **Header**

`<181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message`

For example: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **Body**

  CISE_RADIUS_Accounting 000011 1 0 2016-05-09 12:53:52.823 +03:00 0000012451 3000 NOTICE Radius-Accounting: RADIUS Accounting start request, ConfigVersionId=104, Device IP Address=10.0.0.12, RequestLatency=12, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Start, Acct-Session-Id=6, cisco-av-pair=audit-session-id=5

- **Parsing Example**

  Parsed details include user name, and framed IP address, as well as the MAC address if it is included in the message.

  [UserA,10.0.0.16]

Remove Mapping Messages

The following messages are supported for Remove Mapping.

- **Header**

  `<181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message`

  For example: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **Body**

  2016-05-09 12:56:27.274 +03:00 0000012482 3001 NOTICE Radius-Accounting: RADIUS Accounting stop request, ConfigVersionId=104, Device IP Address=10.0.0.17, RequestLatency=13, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Stop, Acct-Session-Id=104, cisco-av-pair=audit-session-id=5

- **Parsing Example**

  Parsed details include user name, and framed IP address, as well as the MAC address if it is included in the message.

  [UserA,10.0.0.16]

Syslog Lucent QIP Pre-Defined Template

The supported syslog message format and types for Lucent QIP are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 712.

New Mapping Body Messages

There are different Lucent QIP body messages that are recognized by the parser as described in the following table.

The regular expression structure for these messages is as follows:

DHCP_GrantLease|:DHCP_RenewLease

Once received, the body is parsed for user details as follows:

[00:0C:29:91:2E:5D,10.0.0.11]

Body Message
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_GrantLease: Host=$HOSTNAME$ P=10.0.0.11 MAC= 00:0C:29:91:2E:5D
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_RenewLease: Host=$HOSTNAME$ P=10.0.0.11 MAC= 00:0C:29:91:2E:5D

Remove Mapping Body Messages

The regular expression structure for these messages is as follows:

Delete Lease:|DHCP Auto Release:

Once received, the body is parsed for user details as follows:

[10.0.0.11]

Body Message
DHCP:subtype=0:Single:$IGNORE_N$ Delete Lease: IP=10.0.0.11 $IGNORE_N$
DHCP:subtype=0:Single:$IGNORE_N$ DHCP Auto Release: IP=10.0.0.11 $IGNORE_N$

Filter Passive Identity Services

You can filter certain users, based on their name or IP address. For example, if you have an administrator from IT services who logs in to an endpoint in order to assist the regular user with that endpoint, you can filter out the administrator activity so it does not appear in Live Sessions, but rather only the regular user of that endpoint will appear. The Live Session shows Passive Identity service components that are not filtered out by the Mapping Filters. You can add as many filters as needed. The “OR” logic operator applies between filters. If both the fields are specified in a single filter, the “AND” logic operator applies between these fields.

Step 1 Choose **Work Centers** > **PassiveID** > **Providers** and then from the left panel choose **Mapping Filters**.

Step 2 Choose **Providers** > **Mapping Filters**.

Step 3 Click **Add**, enter the Username and or IP address of the user you want to filter and click **Submit**.

Step 4 To view the non-filtered users that are currently logged into the Monitoring session directory, choose **Operations** > **RADIUS Livelog**.

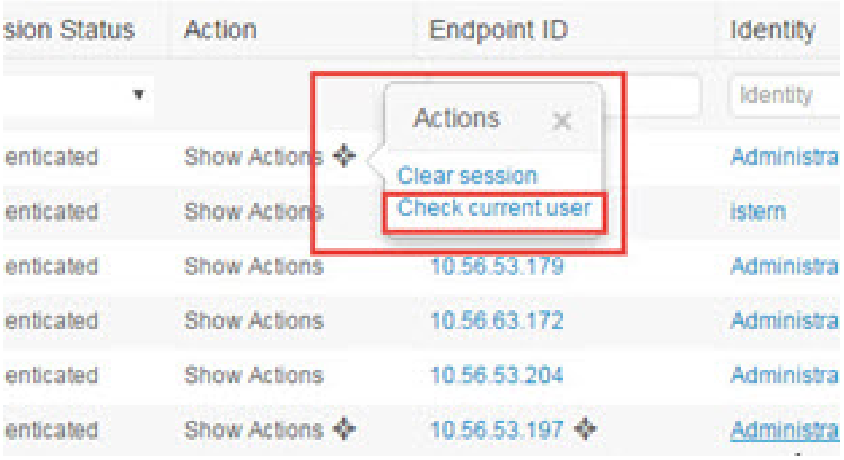
Endpoint Probe

In addition to the customized providers that you can configure the Endpoint probe is enabled in ISE when the Passive Identity service is activated and always runs in the background. The Endpoint probe periodically checks whether each specific user is still logged in to the system.

Note In order to ensure Endpoint runs in the background, you must first configure an initial Active Directory join point and ensure you choose to **Store Credentials**. For more information about configuring the Endpoint probe, see Work with the Endpoint Probe, on page 726.

To manually check for endpoint status go to **Live Sessions** , from the **Actions** column, click **Show Actions** and choose **Check current user**, as in the following figure.

Figure 24: Check Current User


sion Status
Action
Endpoint ID
Identity
Identity
Actions
Clear session
Check current user
enticated
Show Actions
Administra
istern
10.56.53.179
10.56.63.172
10.56.53.204
10.56.53.197

For more information about endpoint user status, and manually running the check, see RADIUS Live Sessions, on page 446.

When the Endpoint probe recognizes that a user has connected, if 4 hours have passed since the last time the session was updated for the specific endpoint, it checks whether that user is still logged in and collects the following data:

- MAC address
- Operating system version

Based on the this check, the probe does the following:

- When the user is still logged in, the probe updates Cisco ISE with the status Active User.
- When the user has logged out, the session state is updated as Terminated and fifteen minutes later, the user is removed from the Session Directory.
- When the user cannot be contacted, for example, when a firewall prevents contact or the endpoint has shut down, the status is updated as Unreachable and the Subscriber policy will determine how to handle the user session. The endpoint will remain in the Session Directory.

Work with the Endpoint Probe

Before you begin

Create and enable Endpoint probes based on subnet ranges. One Endpoint probe can be created per PSN. To work with Endpoint probes, first ensure you have configured the following:

- Endpoints must have network connectivity to port 445.
- From ISE, configure an initial Active Directory join point and ensure you select **Select Credentials** when prompted. For more information about join points, see Active Directory as a Probe and a Provider, on page 686.

Note In order to ensure Endpoint runs in the background, you must first configure an initial Active Directory join point, which enables the Endpoint probe to run even when the Active Directory probe is not fully configured.

Step 1 Choose **Work Centers** > **Passive ID** > **Providers** and then choose **Endpoint Probes**.

Step 2 Click **Add** to create a new Endpoint probe.

Step 3 Complete the mandatory fields, ensuring you select **Enable** from the **Status** field, and click **Submit**. See Endpoint Probe Settings, on page 726 for more information.

Endpoint Probe Settings

Create a single Endpoint probe per PSN, based on subnet ranges. If you have multiple PSNs in your deployment, then you can allot each PSN for a separate set of subnets.

Table 90: Endpoint Probes Settings

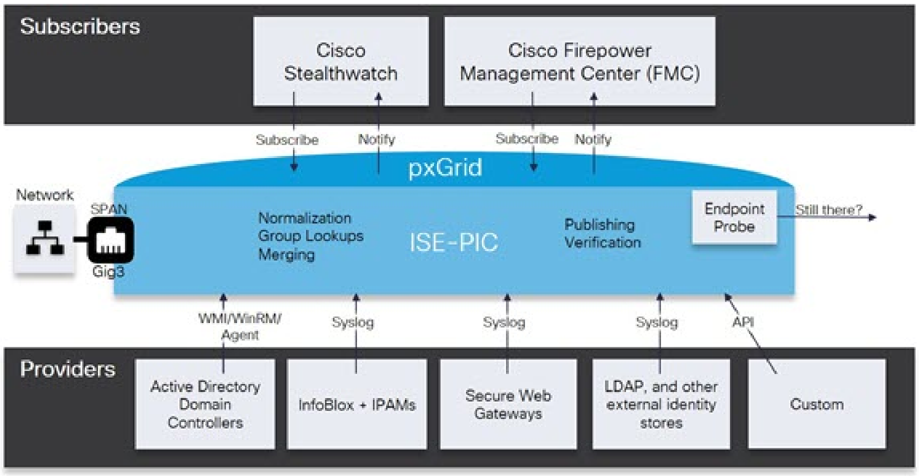
Field Name	Description
Name	Enter a unique name by which to identify the use of this probe.
Description	Enter a unique description that explains the use for this probe.
Status	Choose **Enable** to activate this probe.
Host Name	Choose a PSN for this probe from the list of available PSNs in your deployment.
Subnets	Enter the subnet range for the group of endpoints that should be checked by this probe. Use standard subnet mask ranges and separate subnet addresses with commas. For example: 10.56.14.111/32,2.55.2.0/16,2.2.3.0/16,1.2.3.4/32 Each range must be unique and separate from all other ranges. For example, you cannot enter the following ranges for the same probe because they overlap with each other: 2.2.2.0/16,2.2.3.0/16

Subscribers

The Passive Identity services use Cisco pxGrid services to deliver authenticated user identities that are collected from various providers and stored by the Cisco ISE session directory, to other network systems such as Cisco Stealthwatch or Cisco Firepower Management Center (FMC).

In the following figure, the pxGrid node collects user identities from external providers. Those identities are parsed, mapped and formatted. pxGrid takes those formatted user identities and sends them to Passive Identity service subscribers.

Figure 25: Passive Identity Service Flow


Subscribers
Cisco Stealthwatch
Cisco Firepower Management Center (FMC)
Subscribe
Notify
Subscribe
Notify
pxGrid
Network
SPAN
Gig3
Normalization
Group Lookups
Merging
ISE-PIC
Publishing
Verification
Endpoint Probe
Still there?
WMI/WinRM/ Agent
Syslog
Syslog
Syslog
API
Providers
Active Directory Domain Controllers
InfoBlox + IPAMs
Secure Web Gateways
LDAP, and other external identity stores
Custom

Subscribers connected to Cisco ISE must register to use the pxGrid services. Subscribers should adopt the pxGrid Client Library available from Cisco through the pxGrid SDK to become the clients. A subscriber can log in to pxGrid using a unique name and certificate-based mutual authentication. Once they have sent a valid certificate, Cisco pxGrid subscribers are automatically approved by ISE.

Subscribers can connect to either a configured pxGrid server hostname or an IP Address. We recommend that you use hostname to avoid unnecessary errors, particularly to ensure the DNS queries work properly. Capabilities are information topics or channels that are created on pxGrid for subscribers to publish and subscribe. In Cisco ISE, only SessionDirectory and IdentityGroup are supported. You can view capability information that is available from the publisher through publish, directed query, or bulk download query, by navigating to **Subscribers** in the **Capabilities** tab.

To enable subscribers to receive information from ISE, you must:

1. Optionally, generate a certificate from the subscriber's side.
2. Generate pxGrid Certificates for Subscribers, on page 728 from the PassiveID work center.
3. Enable Subscribers, on page 729. Either perform this step, or automatically enable approvals, in order to allow subscribers to receive user identities from ISE. See Configure Subscriber Settings, on page 729.

Generate pxGrid Certificates for Subscribers

Before you begin

You can generate certificates for pxGrid subscribers in order to guarantee mutual trust between pxGrid and the subscribers, thereby enabling user identities to be passed from ISE to the subscribers. To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose**Work Centers** > **PassiveID** > **Subscribers** and go to the **Certificates** tab.

Step 2 Select one of the following options from the **I want to** drop-down list:

- **Generate a single certificate without a certificate signing request**: You must enter the Common Name (CN) if you select this option. In the Common Name field, enter the pxGrid FQDN which includes pxGrid as the prefix. For example, www.pxgrid-ise.ise.net. Or, alternatively, use wildcards. For example, *.ise.net
- **Generate a single certificate with a certificate signing request**: You must enter the Certificate Signing Request details if you select this option.
- **Generate bulk certificates**: You can upload a CSV file that contains the required details.
- **Download Root Certificate Chain**: Download the ISE public root certificates in order to add them to the pxGrid client's trusted certificate store. The ISE pxGrid node only trusts the newly signed pxGrid client certificate and vice-versa, eliminating the need for outside certificate authorities.

Step 3 (optional) You can enter a description for this certificate.

Step 4 View or edit the pxGrid Certificate template on which this certificate is based. Certificate templates contain properties that are common to all certificates issued by the Certificate Authority (CA) based on that template. The certificate template defines the Subject, Subject Alternative Name (SAN), key type, key size, SCEP RA profile that must be used, validity period of the certificate, and the extended key usage (EKU) that specifies whether the certificate has to be used for client or server authentication or both. The internal Cisco ISE CA (ISE CA) uses a certificate template to issue certificates based on that template. To edit this template, choose **Administration** > **Certificates** > **Certificate Authority** > **Certificate Templates**.

Step 5 Specify the Subject Alternative Name (SAN). You can add multiple SANs. The following options are available:

- **FQDN**: Enter the fully qualified domain name of the ISE node. For example www.isepic.ise.net. Or, alternatively, use wildcards for the FQDN. For example, *.ise.net

  An additional line can be added for FQDN in which the pxGrid FQDN can also be entered. This should be identical to the FQDN you used in the Common Name field.
- **IP address**: Enter the IP address of the ISE node to be associated with the certificate. This information must be entered if the subscriber uses IP addresses instead of an FQDN.

Note This field is not displayed if you have selected the Generate Bulk Certificate option.

Step 6 Select one of the following options from the **Certificate Download Format** drop-down list:

- **Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)**: The root certificate, the intermediate CA certificates, and the end entity certificate are represented in the PEM format. PEM formatted certificate are BASE64-encoded ASCII files. Each certificate starts with the "--------BEGIN CERTIFICATE-----" tag and ends with the "-------END CERTIFICATE----" tag. The end entity's private key is stored using PKCS* PEM. It starts with the "-----BEGIN ENCRYPTED PRIVATE KEY----" tag and ends with the "-----END ENCRYPTED PRIVATE KEY----" tag.

- **PKCS12 format (including certificate chain; one file for both the certificate chain and key)**: A binary format to store the root CA certificate, the intermediate CA certificate, and the end entity 's certificate and private key in one encrypted file.

Step 7 Enter a certificate password.

Step 8 Click **Create**.

Enable Subscribers

You must perform this task, or alternatively automatically enable approvals, in order to allow subscribers to receive user identities from Cisco ISE. See Configure Subscriber Settings, on page 729.

Before you begin

- Enable the pxGrid persona on at least one node to view the requests from the Cisco pxGrid clients.
- Enable Passive Identity Service. For more information, see Easy Connect, on page 679.

Step 1 Choose **Work Centers** > **PassiveID** > **Subscribers** and ensure you are viewing the **Clients** tab.

Step 2 Check the checkbox next to the subscriber and click **Approve**.

Step 3 Click **Refresh** to view the latest status.

View Subscriber Events from Live Logs

The Live Logs page displays all the Subscriber events. Event information includes the subscriber and capability names along with the event type and timestamp.

Navigate to **Subscribers** and select the **Live Log** tab to view the list of events. You can also clear the logs and resynchronize or refresh the list.

Configure Subscriber Settings

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration** > **pxGrid Services** > **Settings**.

Step 2 Select the following options based on your requirements:

- **Automatically Approve New Accounts**: Check this checkbox to automatically approve the connection requests from new pxGrid clients.

- **Allow Password Based Account Creation**: Check this checkbox to enable username/password based authentication for pxGrid clients. If this option is enabled, the pxGrid clients cannot be automatically approved.

  A pxGrid client can register itself with the pxGrid controller by sending the username via REST API. The pxGrid controller generates a password for the pxGrid client during client registration. The administrator can approve or deny the connection request.

Step 3 Click **Save**.

Monitoring and Troubleshooting Service in PassiveID Work Center

Learn about how you can manage PassiveID Work Center with monitoring, troubleshooting and reporting tools.

- RADIUS Live Sessions, on page 446
- See the Reports section in Cisco ISE Reports, on page 412
- TCP Dump Utility to Validate Incoming Traffic, on page 1392

LDAP

Lightweight Directory Access Protocol (LDAP) is a networking protocol defined by RFC 2251 for querying and modifying directory services that run on TCP/IP. LDAP is a lightweight mechanism for accessing an X.500-based directory server.

Cisco ISE integrates with an LDAP external database, which is also called an identity source, by using the LDAP protocol.

LDAP Directory Service

LDAP directory service is based on a client-server model. A client starts an LDAP session by connecting to an LDAP server and sending operation requests to the server. The server then sends its responses. One or more LDAP servers contain data from the LDAP directory tree or the LDAP backend database.

The directory service manages a directory, which is a database that holds information. Directory services use a distributed model for storing information, and that information is usually replicated between directory servers.

An LDAP directory is organized in a simple tree hierarchy and can be distributed among many servers. Each server can have a replicated version of the total directory, which is synchronized periodically.

An entry in the tree contains a set of attributes, where each attribute has a name (an attribute type or attribute description) and one or more values. The attributes are defined in a schema.

Each entry has a unique identifier: its distinguished name (DN). This name contains the relative distinguished name (RDN), which is constructed from attributes in the entry, followed by the DN of the parent entry. You can think of the DN as a full filename, and the RDN as a relative filename in a folder.

Multiple LDAP Instances

By creating more than one LDAP instance with different IP addresses or port settings, you can configure Cisco ISE to authenticate using different LDAP servers or different databases on the same LDAP server. Each primary server IP address and port configuration, along with the secondary server IP address and port configuration, forms an LDAP instance that corresponds to one Cisco ISE LDAP identity source instance.

Cisco ISE does not require that each LDAP instance correspond to a unique LDAP database. You can have more than one LDAP instance set to access the same database. This method is useful when your LDAP database contains more than one subtree for users or groups. Because each LDAP instance supports only one subtree directory for users and one subtree directory for groups, you must configure separate LDAP instances for each user directory and group directory subtree combination for which Cisco ISE submits authentication requests.

LDAP Failover

Cisco ISE supports failover between a primary LDAP server and a secondary LDAP server. A failover occurs when an authentication request fails because Cisco ISE could not connect to an LDAP server because it is down or is otherwise unreachable.

If you establish failover settings and the first LDAP server that Cisco ISE attempts to contact cannot be reached, Cisco ISE always attempts to contact a second LDAP server. If you want Cisco ISE to use the first LDAP server again, you must enter a value in the Failback Retry Delay text box.

Note Cisco ISE always uses the primary LDAP server to obtain groups and attributes for use in authorization policies from the Admin portal, so the primary LDAP server must be accessible when you configure these items. Cisco ISE uses the secondary LDAP server only for authentications and authorizations at run time, according to the failover configuration.

LDAP Connection Management

Cisco ISE supports multiple concurrent LDAP connections. Connections are opened on demand at the time of the first LDAP authentication. The maximum number of connections is configured for each LDAP server. Opening connections in advance shortens the authentication time. You can set the maximum number of connections to use for concurrent binding connections. The number of open connections can be different for each LDAP server (primary or secondary) and is determined based on the maximum number of administration connections configured for each server.

Cisco ISE retains a list of open LDAP connections (including the binding information) for each LDAP server that is configured in Cisco ISE. During the authentication process, the connection manager attempts to find an open connection from the pool. If an open connection does not exist, a new one is opened.

If the LDAP server closed the connection, the connection manager reports an error during the first call to search the directory, and tries to renew the connection. After the authentication process is complete, the connection manager releases the connection.

LDAP User Authentication

You can configure LDAP as an external identity store. Cisco ISE uses plain password authentication. User authentication includes:

- Searching the LDAP server for an entry that matches the username in the request.
- Checking the user password with the one that is found in the LDAP server.
- Retrieving a group's membership information for use in policies.
- Retrieving values for specified attributes for use in policies and authorization profiles.

To authenticate a user, Cisco ISE sends a bind request to the LDAP server. The bind request contains the DN and password of the user in clear text. If the DN and password of the user match the username and password in the LDAP directory, then the user is authenticated.

When Active Directory is used as LDAP, UPN names are used for user authentication. When Sun ONE Directory Server is used as LDAP, SAM names are used for user authentication

Note

- Cisco ISE sends two searchRequest messages for every user authentication. This does not impact Cisco ISE authorization or network performance. The second LDAP request is to make sure the Ciso ISE is talking to the right identity.
- Cisco ISE as a DNS client, uses only the first IP returned in the DNS response to perform the LDAP bind.

We recommend that you protect the connection to the LDAP server using Secure Sockets Layer (SSL).

Note Password change is supported for LDAP only if there are remaining grace logins for the account after the password has expired. If password change is successful, the LDAP server's bindResponse is LDAP_SUCCESS, and includes the remaining grace logins control field in the bindResponse message. If the bindResponse message contains any additional control fields (other than remaining grace logins), Cisco ISE might not be able to decode the message.

LDAP Group and Attribute Retrieval for Use in Authorization Policies

Cisco ISE can authenticate a subject (user or host) against an LDAP identity source by performing a bind operation on the directory server to find and authenticate the subject. After a successful authentication, Cisco ISE can retrieve groups and attributes that belong to the subject whenever they are required. You can configure the attributes to retrieve in the Cisco ISE Admin portal by choosing **Administration** > **Identity Management** > **External Identity Sources** > **LDAP**. These groups and attributes can be used by Cisco ISE to authorize the subject.

To authenticate a user or query the LDAP identity source, Cisco ISE connects to the LDAP server and maintains a connection pool.

You should note the following restrictions on group memberships when Active Directory is configured as an LDAP store:

- Users or computers must be direct members of the group defined in the policy conditions to match the policy rule.
- The defined group may not be a user's or computer's primary group. This restriction is applicable only when Active Directory is configured as an LDAP store.

LDAP Group Membership Information Retrieval

For user authentication, user lookup, and MAC address lookup, Cisco ISE must retrieve group membership information from LDAP databases. LDAP servers represent the association between a subject (a user or a host) and a group in one of the following ways:

- Groups Refer to Subjects: The group objects contain an attribute that specifies the subject. Identifiers for subjects can be sourced in the group as the following:
  - Distinguished names
  - Plain usernames
- Subjects Refer to Groups: The subject objects contain an attribute that specifies the group to which they belong.

LDAP identity sources contain the following parameters for group membership information retrieval:

- Reference direction: This parameter specifies the method to use when determining group membership (either groups to subjects or subjects to groups).
- Group map attribute: This parameter indicates the attribute that contains group membership information.
- Group object class: This parameter determines that certain objects are recognized as groups.
- Group search subtree: This parameter indicates the search base for group searches.
- Member type option: This parameter specifies how members are stored in the group member attribute (either as DNs or plain usernames).

LDAP Attributes Retrieval

For user authentication, user lookup, and MAC address lookup, Cisco ISE must retrieve the subject attributes from LDAP databases. For each instance of an LDAP identity source, an identity source dictionary is created. These dictionaries support attributes of the following data types:

- String
- Unsigned integer 32
- IPv4 address

For unsigned integers and IPv4 attributes, Cisco ISE converts the strings that it has retrieved to the corresponding data types. If conversion fails or if no values are retrieved for the attributes, Cisco ISE logs a debug message, but the authentication or lookup process does not fail.

You can optionally configure default values for the attributes that Cisco ISE can use when the conversion fails or when Cisco ISE does not retrieve any values for the attributes.

LDAP Certificate Retrieval

If you have configured certificate retrieval as part of user lookup, then Cisco ISE must retrieve the value of the certificate attribute from LDAP. To retrieve the value of the certificate attribute from LDAP, you must have previously configured the certificate attribute in the list of attributes to be accessed while configuring an LDAP identity source.

Errors Returned by the LDAP Server

The following errors can occur during the authentication process:

- Authentication Errors—Cisco ISE logs authentication errors in the Cisco ISE log files.

  Possible reasons for an LDAP server to return binding (authentication) errors include the following:

  - Parameter errors—Invalid parameters were entered
  - User account is restricted (disabled, locked out, expired, password expired, and so on)
  - Initialization Errors—Use the LDAP server timeout settings to configure the number of seconds that Cisco ISE should wait for a response from an LDAP server before determining that the connection or authentication on that server has failed.

    Possible reasons for an LDAP server to return an initialization error are:

    - LDAP is not supported.
    - The server is down.
    - The server is out of memory.
    - The user has no privileges.
    - Administrator credentials are configured incorrectly.

The following errors are logged as external resource errors, indicating a possible problem with the LDAP server:

- A connection error occurred
- The timeout expired
- The server is down
- The server is out of memory

The following error is logged as an Unknown User error:

- A user does not exist in the database

The following error is logged as an Invalid Password error, where the user exists, but the password sent is invalid:

- An invalid password was entered

LDAP User Lookup

Cisco ISE supports the user lookup feature with an LDAP server. This feature allows you to search for a user in the LDAP database and retrieve information without authentication. The user lookup process includes the following actions:

- Searching the LDAP server for an entry that matches the username in the request
- Retrieving a user's group membership information for use in policies
- Retrieving values for specified attributes for use in policies and authorization profiles

LDAP MAC Address Lookup

Cisco ISE supports the MAC address lookup feature. This feature allows you to search for a MAC address in the LDAP database and retrieve information without authentication. The MAC address lookup process includes the following actions:

- Searching the LDAP server for an entry that matches the MAC address of the device
- Retrieving a MAC Address group information for the device for use in policies
- Retrieving values for specified attributes for use in policies

Add LDAP Identity Sources

Before you begin

- To perform the following task, you must be a Super Admin or System Admin.
- Cisco ISE always uses the primary LDAP server to obtain groups and attributes for use in authorization policies. Therefore, your primary LDAP server must be reachable when you configure these items.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **LDAP** > **Add**.

Step 2 Enter the values.

Step 3 Click **Submit** to create an LDAP instance.

LDAP Identity Source Settings

The following table describes the fields on the LDAP Identity Sources window, which you can use to create an LDAP instance and connect to it. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **LDAP**.

LDAP General Settings

The following table describes the fields in the **General** tab.

Table 91: LDAP General Settings

Field Name	Usage Guidelines
Name	Enter a name for the LDAP instance. This value is used in searches to obtain the subject DN and attributes. The value is of type string and the maximum length is 64 characters.
Description	Enter a description for the LDAP instance. This value is of type string, and has a maximum length of 1024 characters.
Schema	You can choose any one of the following built-in schema types or create a custom schema: • Active Directory • Sun Directory Server • Novell eDirectory You can click the arrow next to Schema to view the schema details. If you edit the attributes of the predefined schema, Cisco ISE automatically creates a Custom schema.
Note The following fields can be edited only when you choose the Custom schema.	
Subject Objectclass	Enter a value to be used in searches to obtain the subject DN and attributes. The value is of type string and the maximum length is 256 characters.
Subject Name Attribute	Enter the name of the attribute containing the username in the request. The value is of type string and the maximum length is 256 characters. **Note** The subject name attributes that are configured should be an indexed one in the external ID store.
Group Name Attribute	• CN: To retrieve the LDAP Identity Store Groups based on Common Name. • DN: To retrieve the LDAP Identity Store Groups based on Distinguished Name.
Certificate Attribute	Enter the attribute that contains the certificate definitions. For certificate-based authentication, these definitions are used to validate certificates that are presented by clients.
Group Objectclass	Enter a value to be used in searches to specify the objects that are recognized as groups. The value is of type string and the maximum length is 256 characters.
Group Map Attribute	Specifies the attribute that contains the mapping information. This attribute can be a user or group attribute based on the reference direction that is chosen.
Subject Objects Contain Reference To Groups	Click this option if the subject objects contain an attribute that specifies the group to which they belong.

Field Name	Usage Guidelines
Group Objects Contain Reference To Subjects	Click this option if the group objects contain an attribute that specifies the subject. This value is the default value.
Subjects in Groups Are Stored in Member Attribute As	(Only available when you enable the **Group Objects Contain Reference To Subjects** option) Specifies how members are sourced in the group member attribute and defaults to the DN.
User Info Attributes	By default, predefined attributes are used to collect user information (such as, first name, last name, email, telephone, locality, and so on) for the following built-in schema types: • Active Directory • Sun Directory Server • Novell eDirectory If you edit the attributes of the predefined schema, Cisco ISE automatically creates a Custom schema. You can also select the Custom option from the Schema drop-down list to edit the user information attributes based on your requirements.

Note The subject name attributes that are configured should be an indexed one in the external ID store.

LDAP Connection Settings

The following table describes the fields in the **Connection Settings** tab.

Table 92: LDAP Connection Settings

Field Name	Usage Guidelines
Enable Secondary Server	Check this option to enable the secondary LDAP server to be used as a backup if the primary LDAP server fails. If you check this check box, you must enter configuration parameters for the secondary LDAP server.
Primary and Secondary Servers	
Hostname/IP	Enter the IP address or DNS name of the machine that is running the LDAP software. The hostname can contain from 1 to 256 characters or a valid IP address expressed as a string. The only valid characters for hostnames are alphanumeric characters (a to z, A to Z, 0 to 9), the dot (.), and the hyphen (-).
Port	Enter the TCP/IP port number on which the LDAP server is listening. Valid values are from 1 to 65,535. The default is 389, as stated in the LDAP specification. If you do not know the port number, you can find this information from the LDAP server administrator.

Field Name	Usage Guidelines
Specify server for each ISE node	Check this check box to configure primary and secondary LDAP server hostnames/IP and their ports for each PSN. When this option is enabled, a table listing all the nodes in the deployment is displayed. You need to select the node and configure the primary and secondary LDAP server hostname/IP and their ports for the selected node.
Access	**Anonymous Access**: Click to ensure that searches on the LDAP directory occur anonymously. The server does not distinguish who the client is and will allow the client read access to any data that is configured as accessible to any unauthenticated client. In the absence of a specific policy permitting authentication information to be sent to a server, a client should use an anonymous connection. **Authenticated Access**: Click to ensure that searches on the LDAP directory occur with administrative credentials. If so, enter information for the Admin DN and Password fields.
Admin DN	Enter the DN of the administrator. The Admin DN is the LDAP account that has permission to search all required users under the User Directory Subtree and to search groups. If the administrator specified does not have permission to see the group name attribute in searches, group mapping fails for users who are authenticated by that LDAP server.
Password	Enter the LDAP administrator account password.
Secure Authentication	Click to use SSL to encrypt communication between Cisco ISE and the primary LDAP server. Verify that the Port field contains the port number used for SSL on the LDAP server. If you enable this option, you must choose a root CA.
LDAP Server Root CA	Choose a trusted root certificate authority from the drop-down list to enable secure authentication with a certificate.
Server Timeout	Enter the number of seconds that Cisco ISE waits for a response from the primary LDAP server before determining that the connection or authentication with that server has failed. Valid values are 1 to 99. The default is 10.
Max. Admin Connections	Enter the maximum number of concurrent connections (greater than 0) with LDAP administrator account permissions that can run for a specific LDAP configuration. These connections are used to search the directory for users and groups under the User Directory Subtree and the Group Directory Subtree. Valid values are 1 to 99. The default is 20.
Force reconnect every N seconds	Check this check box and enter the desired value in the **Seconds** field to force the server to renew LDAP connection at the specified time interval. The valid range is from 1 to 60 minutes.
Test Bind to Server	Click to test and ensure that the LDAP server details and credentials can successfully bind. If the test fails, edit your LDAP server details and retest.
Failover	

Field Name	Usage Guidelines
Always Access Primary Server First	Click this option if you want Cisco ISE to always access the primary LDAP server first for authentications and authorizations.
Failback to Primary Server After	If the primary LDAP server that Cisco ISE attempts to contact cannot be reached, Cisco ISE attempts to contact the secondary LDAP server. If you want Cisco ISE to use the primary LDAP server again, click this option and enter a value in the text box.

LDAP Directory Organization Settings

The following table describes the fields in the **Directory Organization** tab.

Table 93: LDAP Directory Organization Settings

Field Name	Usage Guidelines
Subject Search Base	Enter the DN for the subtree that contains all subjects. For example: o=corporation.com If the tree containing subjects is the base DN, enter: o=corporation.com or dc=corporation,dc=com as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.
Group Search Base	Enter the DN for the subtree that contains all groups. For example: ou=organizational unit, ou=next organizational unit, o=corporation.com If the tree containing groups is the base DN, type: o=corporation.com or dc=corporation,dc=com as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.

Field Name	Usage Guidelines
Search for MAC Address in Format	Enter a MAC Address format for Cisco ISE to use for search in the LDAP database. MAC addresses in internal identity sources are sourced in the format xx-xx-xx-xx-xx-xx. MAC addresses in LDAP databases can be sourced in different formats. However, when Cisco ISE receives a host lookup request, Cisco ISE converts the MAC address from the internal format to the format that is specified in this field. Use the drop-down list to enable searching for MAC addresses in a specific format, where <*format*> can be any one of the following: • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx The format you choose must match the format of the MAC address sourced in the LDAP server.
Strip Start of Subject Name Up To the Last Occurrence of the Separator	Enter the appropriate text to remove domain prefixes from usernames. If Cisco ISE finds the delimiter character that is specified in this field in the username, it strips all characters from the beginning of the username through the delimiter character. If the username contains more than one of the characters that are specified in the <start_string> box, Cisco ISE strips characters through the last occurrence of the delimiter character. For example, if the delimiter character is the backslash (\) and the username is DOMAIN\user1, Cisco ISE submits user1 to an LDAP server. **Note** The <start_string> cannot contain the following special characters: the pound sign (#), the question mark (?), the quotation mark (“), the asterisk (*), the right angle bracket (>), and the left angle bracket (<). Cisco ISE does not allow these characters in usernames.
Strip End of Subject Name from the First Occurrence of the Separator	Enter the appropriate text to remove domain suffixes from usernames. If Cisco ISE finds the delimiter character that is specified in this field in the username, it strips all characters from the delimiter character through the end of the username. If the username contains more than one of the characters that are specified in this field, Cisco ISE strips characters starting with the first occurrence of the delimiter character. For example, if the delimiter character is @ and the username is *user1@domain*, then Cisco ISE submits *user1* to the LDAP server. **Note** The <*end_string*> box cannot contain the following special characters: the pound sign (#), the question mark (?), the quotation mark ("), the asterisk (*), the right angle bracket (>), and the left angle bracket (<). Cisco ISE does not allow these characters in usernames.

LDAP Group Settings

Table 94: LDAP Group Settings

Field Name	Usage Guidelines
Add	Choose **Add** > **Add Group** to add a new group or choose **Add** > **Select Groups From Directory** to select the groups from the LDAP directory. If you choose to add a group, enter a name for the new group. If you are selecting from the directory, enter the filter criteria, and click **Retrieve Groups**. Check the check boxes next to the groups that you want to select and click **OK**. The groups that you have selected will appear in the **Groups** window.

LDAP Attribute Settings

Table 95: LDAP Attribute Settings

Field Name	Usage Guidelines
Add	Choose **Add** > **Add Attribute** to add a new attribute or choose **Add** > **Select Attributes From Directory** to select attributes from the LDAP server. If you choose to add an attribute, enter a name for the new attribute. If you are selecting from the directory, enter the username and click **Retrieve Attributes** to retrieve the attributes. Check the check boxes next to the attributes that you want to select, and then click OK.

LDAP Advanced Settings

The following table describes the field in the Advanced Settings tab.

Table 96: LDAP Advanced Settings

Field Name	Usage Guidelines
Enable Password Change	Check this check box to enable the user to change the password in case of password expiry or password reset while using PAP protocol for device admin and RADIUS EAP-GTC protocol for network access. User authentication fails for the unsupported protocols. This option also enables the user to change the password on their next login.

Related Topics

- LDAP Directory Service, on page 730
- LDAP User Authentication, on page 732
- LDAP User Lookup, on page 735
- Add LDAP Identity Sources, on page 735

Configure LDAP Schema

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **LDAP**.

Step 2 Select the LDAP instance.

Step 3 Click the **General** tab.

Step 4 Click the drop-down arrow near the **Schema** option.

Step 5 Select the required schema from the **Schema** drop-down list. You can select the **Custom** option to update the attributes based on your requirements.

Predefined attributes are used for the built-in schema, such as Active Directory, Sun directory Server, Novell eDirectory. If you edit the attributes of the predefined schema, Cisco ISE automatically creates a custom schema.

Configure Primary and Secondary LDAP Servers

After you create an LDAP instance, you must configure the connection settings for the primary LDAP server. Configuring a secondary LDAP server is optional.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **LDAP**.

Step 2 Check the check box next to the LDAP instance that you want to edit and click **Edit**.

Step 3 Click the **Connection** tab to configure the primary and secondary servers.

Step 4 Enter the values as described in LDAP Identity Source Settings.

Step 5 Click **Submit** to save the connection parameters.

Enable Cisco ISE to Obtain Attributes from the LDAP Server

For Cisco ISE to obtain user and group data from an LDAP server, you must configure LDAP directory details in Cisco ISE. For LDAP identity source, the following three searches are applicable:

- Search for all groups in group subtree for administration
- Search for user in subject subtree to locate user
- Search for groups in which the user is a member

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **LDAP**.

Step 2 Check the check box next to the LDAP instance that you want to edit and click **Edit**.

Step 3 Click the **Directory Organization** tab.

Step 4 Enter the values as described in LDAP Identity Source Settings.

Step 5 Click **Submit** to save the configuration.

Retrieve Group Membership Details from the LDAP Server

You can add new groups or select groups from the LDAP directory.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **LDAP**.

Step 2 Check the check box next to the LDAP instance that you want to edit and click **Edit**.

Step 3 Click the **Groups** tab.

Step 4 Choose **Add** > **Add Group** to add a new group or choose **Add** > **Select Groups From Directory** to select the groups from the LDAP directory.

a) If you choose to add a group, enter a name for the new group.
b) If you are selecting from the directory, enter the filter criteria, and click **Retrieve Groups**. Your search criteria can contain the asterisk (*) wildcard character.

Step 5 Check the check boxes next to the groups that you want to select and click **OK**.

The groups that you have selected will appear in the Groups page.

Step 6 Click **Submit** to save the group selection.

Note Active Directory built-in groups are not supported when Active Directory is configured as LDAP Identity Store in Cisco ISE.

Retrieve User Attributes from the LDAP Server

You can obtain user attributes from the LDAP server for use in authorization policies.

Step 1 Choose **Administration** > **Identity Management** > **External Identity Sources** > **LDAP**.

Step 2 Check the check box next to the LDAP instance that you want to edit and click **Edit**.

Step 3 Click the **Attributes** tab.

Step 4 Choose **Add** > **Add Attribute** to add a new attribute or choose **Add** > **Select Attributes From Directory** to select attributes from the LDAP server.

a) If you choose to add an attribute, enter a name for the new attribute.
b) If you are selecting from the directory, enter an example user and click **Retrieve Attributes** to retrieve the user's attributes. You can use the asterisk (*) wildcard character.

Cisco ISE allows you to configure the LDAP server with IPv4 or IPv6 address for user authentication when you manually add the attribute type IP.

Step 5 Check the check boxes next to the attributes that you want to select, then click **OK**.

Step 6 Click **Submit** to save the attribute selections.

Enable Secure Authentication with LDAP Identity Source

When you choose the Secure Authentication option in the LDAP configuration page, Cisco ISE uses SSL to secure communication with the LDAP identity source. Secure connection to LDAP identity source is established using:

- SSL tunnel: Using SSL v3 or TLS v1 (the strongest version supported by the LDAP server)
- Server authentication (authentication of LDAP server): Certificate based
- Client authentication (authentication of Cisco ISE): None (Administrator bind is used inside the SSL tunnel)
- Cipher suites: All cipher suites supported by Cisco ISE

We recommend that you use TLS v1 with the strongest encryption and ciphers that Cisco ISE supports.

To enable Cisco ISE to communicate securely with the LDAP identity source:

Before you begin

- Cisco ISE must be connected to an LDAP server
- TCP port 636 should be open

Step 1 Import the full Certificate Authority (CA) chain of the CA that issued the server certificate to the LDAP server in to Cisco ISE (**Administration** > **System** > **Certificates** > **Trusted Certificates**).

The full CA chain refers to the root CA and intermediate CA certificates; not the LDAP server certificate.

Step 2 Configure Cisco ISE to use secure authentication when communicating with the LDAP identity source (**Administration** > **Identity Management** > **External Identity Sources** > **LDAP**; be sure to check the Secure Authentication check box in the Connection Settings tab).

Step 3 Select the root CA certificate in the LDAP identity store.

When the LDAP Identity Source is used as the Identity Source Sequence to access a Sponsor Portal, users within the LDAP group will have access to the Sponsor Portal based on Sponsor Group permissions. To restrict access to the Sponsor Portal, do not use the LDAP Identity Source as the Identity Source Sequence.

ODBC Identity Source

You can use an Open Database Connectivity (ODBC)-compliant database as an external identity source to authenticate users and endpoints. ODBC identity source can be used in an identity store sequence and for Guest and Sponsor authentications. It can also be used for BYOD flow.

The following database engines are supported:

- MySQL
- Oracle
- PostgreSQL

- Microsoft SQL Server
- Sybase

Configuring Cisco ISE to authenticate against an ODBC-compliant database does not affect the configuration of the database. To manage your database, refer to your database documentation.

Note Cisco ISE does not support encryption with ODBC. Hence, ODBC connections are not secured.

Credential Check for ODBC Database

Cisco ISE supports three different types of credential check for an ODBC database. You must configure appropriate SQL stored procedure for each credential check type. Cisco ISE uses the stored procedure to query the appropriate tables in the ODBC database and receive the output parameters or recordset from the ODBC database. The database can return a recordset or a set of named parameters in response to an ODBC query.

The password can be stored in an ODBC database in clear text or encrypted format. The stored procedure can decrypt it back to clear text when it is called by Cisco ISE.

Credential Check Type	ODBC Input Parameters	ODBC Output Parameters	Credential Check	Authentication Protocols
Plain text password authentication in ODBC database	Username Password	Result Group Account Info Error string	If the username and password are matched, relevant user information is returned.	PAP EAP-GTC (as inner method of PEAP or EAP-FAST) TACACS
Plain text password fetching from ODBC database	Username	Result Group Account Info Error string Password	If the username is found, its password and relevant user information is returned by the stored procedure. Cisco ISE calculates the password hash based on the authentication method and compares it with the one that is received from the client.	CHAP MSCHAPv1/v2 EAP-MD5 LEAP EAP-MSCHAPv2 (as inner method of PEAP or EAP-FAST) TACACS
Lookup	Username	Result Group Account Info Error string	If the username is found, relevant user information is returned.	MAB Fast reconnect of PEAP, EAP-FAST, and EAP-TTLS

Note If ODBC is used as the lookup source for authorization, ensure that the ODBC database and incoming request MAB format are same.

The groups that are returned in the output parameters are not used in Cisco ISE. Only the groups that are retrieved by the Fetch Groups stored procedure are used in Cisco ISE. The account information is included only in the authentication audit log.

The following table lists the mapping between the result codes returned by the ODBC database stored procedure and Cisco ISE authentication result codes:

Result code (returned by the stored procedure)	Description	Cisco ISE authentication result code
0	CODE_SUCCESS	NA (authentication passed)
1	CODE_UNKNOWN_USER	UnknownUser
2	CODE_INVALID_PASSWORD	Failed
3	CODE_UNKNOWN_USER_OR_INVALID_PASSWORD	UnknownUser
4	CODE_INTERNAL_ERROR	Error
10001	CODE_ACCOUNT_DISABLED	DisabledUser
10002	CODE_PASSWORD_EXPIRED	NotPerformedPasswordExpired

Note Cisco ISE performs the actual authentication or lookup operation based on this mapped authentication result code.

You can use the stored procedures to fetch groups and attributes from the ODBC database.

Here is a sample procedure that returns recordset for plain text password authentication (for Microsoft SQL Server):

```
CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsRecordset]
        @username varchar(64), @password varchar(255)
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username
        AND  password  = @password )
        SELECT 0,11,'give full access','No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

Here is a sample procedure that returns recordset for plain text password fetching (for Microsoft SQL Server):

```
CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsRecordset]
        @username varchar(64)
```

```
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT 0,11,'give full access','No Error',password
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

Here is a sample procedure that returns recordset for Lookup (for Microsoft SQL Server):

```
CREATE PROCEDURE [dbo].[ISEUserLookupReturnsRecordset]
        @username varchar(64)
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT 0,11,'give full access','No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

Here is a sample procedure that returns parameters for plain text password authentication (for Microsoft SQL Server):

```
CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsParameters]
       @username varchar(64), @password varchar(255), @result INT OUTPUT, @group varchar(255)
 OUTPUT, @acctInfo varchar(255) OUTPUT, @errorString varchar(255) OUTPUT
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username
        AND  password  = @password )
        SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT @result=3, @group=0, @acctInfo='odbc',  @errorString='ODBC Authen Error'
END
```

Here is a sample procedure that returns parameters for plain text password fetching (for Microsoft SQL Server):

```
CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsParameters]
        @username varchar(64), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo
varchar(255) OUTPUT, @errorString varchar(255) OUTPUT, @password varchar(255) OUTPUT
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
       SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No Error',
 @password=password
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen Error'
END
```

Here is a sample procedure that returns parameters for Lookup (for Microsoft SQL Server):

```
CREATE PROCEDURE [dbo].[ISEUserLookupReturnsParameters]
        @username varchar(64), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo
varchar(255) OUTPUT, @errorString varchar(255) OUTPUT
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen Error'
END
```

Here is a sample procedure that fetches groups from Microsoft SQL Server:

```
CREATE PROCEDURE [dbo].[ISEGroupsH]
        @username varchar(64), @result int output
AS
BEGIN
        if exists (select * from NetworkUsers where username = @username)
        begin
                set @result = 0
                select 'accountants', 'engineers', 'sales','test_group2'
        end
        else
                set @result = 1
END
```

Here is a sample procedure that fetches all the groups of all the users if the username is "*" (for Microsoft SQL Server):

```
ALTER PROCEDURE [dbo].[ISEGroupsH]
                @username varchar(64), @result int output
AS
BEGIN
                if @username = '*'
                begin
                                -- if username is equal to '*' then return all existing
groups
                                set @result = 0
                                select 'accountants', 'engineers',
'sales','test_group1','test_group2','test_group3','test_group4'
                end
                else
                if exists (select * from NetworkUsers where username = @username)
                begin
                                set @result = 0
                                select 'accountants'
                end
                else
                                set @result = 1
END
```

Here is a sample procedure that fetches attributes from Microsoft SQL Server:

```
CREATE PROCEDURE [dbo].[ISEAttrsH]
        @username varchar(64), @result int output
AS
BEGIN
        if exists (select * from NetworkUsers where username = @username)
        begin
                set @result = 0
                                select phone as phone, username as username, department as
 department, floor as floor, memberOf as memberOf, isManager as isManager from NetworkUsers
 where username = @username
        end
        else
                set @result = 1
END
```

Additional Examples of ODBC Configuration

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/211581-Configure-ODBC-on-ISE-2-3-with-Oracle-Da.html

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200544-Configure-ISE-2-1-with-MS-SQL-using-ODBC.html

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200644-Configure-ODBC-on-ISE-2-1-with-PostgreSQ.html

Add ODBC Identity Source

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources**.

Step 2 Click **ODBC**.

Step 3 Click **Add**.

Step 4 In the **General** tab, enter a name and description for the ODBC identity source.

Step 5 In the **Connection** tab, enter the following details:

- Hostname or IP address of the ODBC database. If you are using a nonstandard TCP port for the database, you can specify the port number in the following format: hostname or IP address:port
- Name of the ODBC database
- Admin username and password (Cisco ISE connects to the database using these credentials)
- Server timeout in seconds (default is 5 seconds)
- Connection attempts (default is 1)
- Database type. Choose one of the following:
  - **MySQL**
  - **Oracle**
  - **PostgreSQL**
  - **Microsoft SQL Server**
  - **Sybase**

Step 6 Click **Test Connection** to check the connectivity with the ODBC database and to verify the existence of the stored procedures for the configured use cases.

Step 7 In the **Stored Procedures** tab, enter the following details:

- **Stored Procedure Type**: Specify the type of output that your database provides:
  - **Returns Recordset**: The database returns a recordset in response to an ODBC query.
  - **Returns Parameters**: The database returns a set of named parameters in response to an ODBC query.
- **Plain Text Password Authentication**: Enter the name of the stored procedure that runs on the ODBC server for plain text password authentication. Used for PAP, EAP-GTC inner method, and TACACS.
- **Plain Text Password Fetching**: Enter the name of the stored procedure that runs on the ODBC server to fetch plain text passwords. Used for CHAP, MS-CHAPv1/v2, LEAP, EAP-MD5, EAP-MSCHAPv2 inner method, and TACACS.
- **Check Username or Machine Exists**: Enter the name of the stored procedure that runs on the ODBC server for User/MAC address lookup. Used for MAB and fast reconnect of PEAP, EAP-FAST, and EAP-TTLS.
- **Fetch Groups**: Enter the name of the stored procedure that retrieves the groups from the ODBC database.
- **Fetch Attributes**: Enter the name of the stored procedure that retrieves the attributes and their values from the ODBC database.
- **Advanced Settings**: Click this option to use the attributes under the following dictionaries as input parameters in the **Fetch Attributes** stored procedure (in addition to the username and password):
  - **RADIUS**
  - **Device**
  - **Network Access**

Note You can use only the following attributes in the **Network Access** dictionary: **AuthenticationMethod**, **Device IP Address**, **EapAuthentication**, **EapTunnel**, **ISE Host Name**, **Protocol**, **UserName**, **VN**, and **WasMachineAuthenticated**.

In the **Attribute Name in Stored Procedure** field, specify the attribute name that is used in the stored procedure.

You can configure the stored procedures to retrieve the following output parameters from the ODBC database:

- ACL
- Security Group
- VLAN (name or number)
- Web-redirect ACL
- Web-redirect portal name

You can use these attributes to configure the authorization profiles. These attributes are listed in the **Common Tasks** section in the **Authorization Profiles** window (under **Policy** > **Policy Elements** > **Results**). The following are a few sample use case scenarios where you can use these attributes:

- To configure an authorization profile to use the VLAN that is returned from the ODBC database, based on the specified input attributes (MAC address, username, called-station-ID, or device location), instead of manually specifying the VLAN for each authorization profile.
- To configure an authorization profile to block access for the calling station IDs that are blocked in the ODBC identity store.

- To configure an authorization profile to retrieve the web-redirect ACL or web-redirect portal name from the ODBC database, based on the MAC address, username, called-station-ID, or device location.

While configuring an authorization policy, you can select the security groups that are retrieved from the ODBC database in the **Policy Sets** window.

Note While using the **Advanced Settings** option, a new table named user_attributes_detail is created in the ODBC database to store the additional details. You must set the data type as VARCHAR2 for all the output parameters. Otherwise, the stored procedure might fail during the Union and Compilation process. For example, if SGTNAME is set as VARCHAR2 and VLANNUMBER is set as NUMBER, compilation of the following stored procedure might fail:

```
select  ATTR_NAME, value from ATTRIBUTES where user_id=userid
          union
          select 'SGTNAME', SGTNAME from user_attributes_detail where USER_ID = userid
and user_attributes_detail.DEVICELOCATIONS=ise_DEVICETYPE
          union
          select 'VLANNUMBER', VLANNUMBER from user_attributes_detail where USER_ID =
userid and user_attributes_detail.DEVICELOCATIONS=ise_DEVICETYPE;
```

- **Search for MAC Address in Format**: The incoming MAC address is normalized based on the selected MAC format.

Step 8 Add the required attributes in the **Attributes** tab. While adding an attribute, you can specify how the attribute name should appear in the authorization policy rules.

You can also fetch the attributes from the ODBC database. These attributes can be used in the authorization policies.

Step 9 Add the user groups in the **Groups** tab. You can also fetch the groups from the ODBC database by specifying the username or MAC address. These groups can be used in authorization policies.

You can rename the groups and attributes. By default, the name that is displayed in the **Name in ISE** field is same as that in ODBC database, however, you can modify this name. This name is used in the authorization policies.

Step 10 Click **Submit**.

For more information on how to configure the ODBC identity source, see the following links:

- Configure ODBC on Cisco ISE with Oracle Database
- Configure Cisco ISE with MS SQL using ODBC
- Configure ODBC on Cisco ISE with PostgreSQL
- Configure Cisco ISE for integration with MySQL server

Note If you have configured input attributes, you must do the following while duplicating an ODBC identity store. Otherwise, input parameters might be lost in the duplicated ODBC identity store.

1. Click **Advance Settings**.
2. Verify whether the input parameters are set properly.
3. Click **OK** to save these input parameters in the duplicated ODBC identity store.

RADIUS Token Identity Sources

A server that supports the RADIUS protocol and provides authentication, authorization, and accounting (AAA) services to users and devices is called a RADIUS server. A RADIUS identity source is simply an external identity source that contains a collection of subjects and their credentials and uses the RADIUS protocol for communication. For example, the Safeword token server is an identity source that can contain several users and their credentials as one-time passwords that provides an interface that you can query using the RADIUS protocol.

Cisco ISE supports any RADIUS RFC 2865-compliant server as an external identity source. Cisco ISE supports multiple RADIUS token server identities, for example the RSA SecurID server and the SafeWord server. RADIUS identity sources can work with any RADIUS token server that is used to authenticate a user.

Note The Process Host Lookup option must be enabled for MAB authentication. We recommend that you don’t configure the RADIUS token server that is used as the external identity source, for MAB authentication, because the devices that are using MAB authentication cannot generate an OTP or a RADIUS token (which is required for RADIUS token server authentication). Hence, the authentication will fail. You can use the external RADIUS server option to process the MAB requests.

RADIUS Token Server-Supported Authentication Protocols

Cisco ISE supports the following authentication protocols for RADIUS identity sources:

- RADIUS PAP
- Protected Extensible Authentication Protocol (PEAP) with inner Extensible Authentication Protocol-Generic Token Card (EAP-GTC)
- EAP-FAST with inner EAP-GTC

Ports Used by the RADIUS Token Servers for Communication

RADIUS token servers use the UDP port for authentication sessions. This port is used for all RADIUS communication. For Cisco ISE to send RADIUS one-time password (OTP) messages to a RADIUS-enabled token server, you must ensure that the gateway devices between Cisco ISE and the RADIUS-enabled token server allow communication over the UDP port. You can configure the UDP port through the Admin portal.

RADIUS Shared Secret

You must provide a shared secret while configuring RADIUS identity sources in Cisco ISE. This shared secret should be the same as the shared secret that is configured on the RADIUS token server.

Failover in RADIUS Token Servers

Cisco ISE allows you to configure multiple RADIUS identity sources. Each RADIUS identity source can have primary and secondary RADIUS servers. When Cisco ISE is unable to connect to the primary server, it uses the secondary server.

Configurable Password Prompt in RADIUS Token Servers

RADIUS identity sources allow you to configure the password prompt. You can configure the password prompt through the Admin portal.

RADIUS Token Server User Authentication

Cisco ISE obtains the user credentials (username and passcode) and passes them to the RADIUS token server. Cisco ISE also relays the results of the RADIUS token server authentication processing to the user.

User Attribute Cache in RADIUS Token Servers

RADIUS token servers, by default, do not support user lookups. However, the user lookup functionality is essential for the following Cisco ISE features:

- PEAP session resume: This feature allows the PEAP session to resume after successful authentication during EAP session establishment.
- EAP/FAST fast reconnect: This feature allows fast reconnection after successful authentication during EAP session establishment.
- TACACS+ Authorization: Happens after a successful TACACS+ authentication.

Cisco ISE caches the results of successful authentications to process user lookup requests for these features. For every successful authentication, the name of the authenticated user and the retrieved attributes are cached. Failed authentications are not written to the cache.

The cache is available in the memory at runtime and is not replicated between Cisco ISE nodes in a distributed deployment. You can configure the Time to Live (TTL) limit for the cache through the Admin portal. Starting with ISE 2.6, you may choose to enable the identity caching option and set the aging time in minutes. The option is disabled by default and when enabled, the cache will be available in the memory for the specified amount of time.

RADIUS Identity Source in Identity Sequence

You can add the RADIUS identity source for authentication sequence in an identity source sequence. However, you cannot add the RADIUS identity source for attribute retrieval sequence because you cannot query the RADIUS identity source without authentication. Cisco ISE cannot distinguish among different errors while authenticating with a RADIUS server. RADIUS servers return an Access-Reject message for all errors. For example, when a user is not found in the RADIUS server, instead of returning a User Unknown status, the RADIUS server returns an Access-Reject message.

RADIUS Server Returns the Same Message for All Errors

When a user is not found in the RADIUS server, the RADIUS server returns an Access-Reject message. Cisco ISE provides an option to configure this message through the Admin portal as either an Authentication Failed or a User Not Found message. However, this option returns a User Not Found message not only for cases where the user is not known, but for all failure cases.

The following table lists the different failure cases that are possible with RADIUS identity servers.

Table 97: Error Handling

Failure Cases	Reasons for Failure
Authentication Failed	• User is unknown. • User attempts to log in with an incorrect passcode. • User login hours expired.
Process Failed	• RADIUS server is configured incorrectly in Cisco ISE. • RADIUS server is unavailable. • RADIUS packet is detected as malformed. • Problem during sending or receiving a packet from the RADIUS server. • Timeout.
Unknown User	Authentication failed and the Fail on Reject option is set to false.

Safeword Server Supports Special Username Format

The Safeword token server supports authentication with the following username format:

Username—Username, OTP

As soon as Cisco ISE receives the authentication request, it parses the username and converts it to the following username:

Username—Username

The SafeWord token servers support both of these formats. Cisco ISE works with various token servers. While configuring a SafeWord server, you must check the SafeWord Server check box in the Admin portal for Cisco ISE to parse the username and convert it to the specified format. This conversion is done in the RADIUS token server identity source before the request is sent to the RADIUS token server.

Authentication Request and Response in RADIUS Token Servers

When Cisco ISE forwards an authentication request to a RADIUS-enabled token server, the RADIUS authentication request contains the following attributes:

- User-Name (RADIUS attribute 1)
- User-Password (RADIUS attribute 2)

  - NAS-IP-Address (RADIUS attribute 4)

Cisco ISE expects to receive any one of the following responses:

- Access-Accept: No attributes are required, however, the response can contain a variety of attributes based on the RADIUS token server configuration.
- Access-Reject: No attributes are required.
- Access-Challenge: The attributes that are required per RADIUS RFC are the following:
  - State (RADIUS attribute 24)
  - Reply-Message (RADIUS attribute 18)
  - One or more of the following attributes: Vendor-Specific, Idle-Timeout (RADIUS attribute 28), Session-Timeout (RADIUS attribute 27), Proxy-State (RADIUS attribute 33)

    No other attributes are allowed in Access-Challenge.

RADIUS Token Identity Sources Settings

The following table describes the fields on the RADIUS Token Identity Sources window, which you can use to configure and connect to an external RADIUS identity source. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **RADIUS Token**.

Table 98: RADIUS Token Identity Source Settings

Field Name	Usage Guidelines
Name	Enter a name for the RADIUS token server. The maximum number of characters allowed is 64.
Description	Enter a description for the RADIUS token server. The maximum number of characters is 1024.
SafeWord Server	Check this check box if your RADIUS identity source is a SafeWord server.
Enable Secondary Server	Check this check box to enable the secondary RADIUS token server for Cisco ISE to use as a backup in case the primary fails. If you check this check box, you must configure a secondary RADIUS token server.
Always Access Primary Server First	Click this option if you want Cisco ISE to always access the primary server first.
Fallback to Primary Server after	Click this option to specify the amount of time in minutes that Cisco ISE can authenticate using the secondary RADIUS token server if the primary server cannot be reached. After this time elapses, Cisco ISE reattempts to authenticate against the primary server.
Primary Server	

Field Name	Usage Guidelines
Host IP	Enter the IP address of the primary RADIUS token server. This field can take as input a valid IP address that is expressed as a string. Valid characters that are allowed in this field are numbers and dot (.).
Shared Secret	Enter the shared secret that is configured on the primary RADIUS token server for this connection.
Authentication Port	Enter the port number on which the primary RADIUS token server is listening.
Server Timeout	Specify the time in seconds that Cisco ISE should wait for a response from the primary RADIUS token server before it determines that the primary server is down.
Connection Attempts	Specify the number of attempts that Cisco ISE should make to reconnect to the primary server before moving on to the secondary server (if defined) or dropping the request if a secondary server is not defined.
Secondary Server	
Host IP	Enter the IP address of the secondary RADIUS token server. This field can take as input a valid IP address that is expressed as a string. Valid characters that are allowed in this field are numbers and dot (.).
Shared Secret	Enter the shared secret configured on the secondary RADIUS token server for this connection.
Authentication Port	Enter the port number on which the secondary RADIUS token server is listening. Valid values are from 1 to 65,535. The default is 1812.
Server Timeout	Specify the time in seconds that Cisco ISE should wait for a response from the secondary RADIUS token server before it determines that the secondary server is down.
Connection Attempts	Specify the number of attempts that Cisco ISE should make to reconnect to the secondary server before dropping the request.

Related Topics

RADIUS Token Identity Sources, on page 752

Add a RADIUS Token Server, on page 756

Add a RADIUS Token Server

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** **External Identity Sources** > **RADIUS Token** > **Add**.

Step 2 Enter the values in the **General** and **Connection** tabs.

Step 3 Click the **Authentication** tab.

This tab allows you to control the responses to an Access-Reject message from the RADIUS token server. This response could either mean that the credentials are invalid or that the user is not known. Cisco ISE accepts one of the following responses: Failed authentication or User not found. This tab also allows you to enable identity caching and to set the aging time for the cache. You can also configure a prompt to request the password.

a) Click the **Treat Rejects as 'authentication failed'** radio button if you want the Access-Reject response from the RADIUS token server to be treated as a failed authentication.
b) Click the **Treat Rejects as 'user not found'** radio button if you want the Access-Reject response from the RADIUS token server to be treated as an unknown user failure.

Step 4 Check the **Enable Passcode Caching** check box if you want Cisco ISE to store the passcode in the cache after the first successful authentication with an RADIUS token server and use the cached user credentials for the subsequent authentications if they happen within the configured time period.

Enter the number of seconds for which the passcode must be stored in the cache in the **Aging Time** field. Within this period of time, the user can perform more than one authentication with the same passcode. The default value is 30 seconds. The valid range is from 1 to 900 seconds.

Note Cisco ISE clears the cache after the first failed authentication. The user must enter a new, valid passcode.

The cache is available in the memory at runtime and it is not replicated between Cisco ISE nodes in a distributed deployment.

Note We strongly recommend that you enable this option only when you use a protocol that supports encryption of the passcode, for example, EAP-FAST-GTC. For information on supported authentication protocols for RADIUS Token server, see RADIUS Token Server-Supported Authentication Protocols, on page 752

Step 5 Check the **Enable Identity Caching** check box if you want to allow processing of requests that do not perform authentication against the server.

You can enable the identity caching option and set the aging time in minutes. The default value is 120 minutes. The valid range is from 1 to 1440 minutes. The results and attributes obtained from the last successful authentication are retained in the cache for the specified time period.

This option is disabled by default.

Step 6 Click the **Authorization** tab.

This tab allows you to configure a name that will appear for the attribute that is returned by the RADIUS token server while sending an Access-Accept response to Cisco ISE. This attribute can be used in authorization policy conditions. The default value is CiscoSecure-Group-Id.

Note If you want to send any attribute in Access-Accept from External ID source, Ext ID source needs to send <ciscoavpair> as attribute name and value in the format: ACS:<attrname>=<attrvalue> where <attrname> is configured in the **Authorization** tab.

Step 7 Click **Submit**.

Delete a RADIUS Token Server

Before you begin

- To perform the following task, you must be a Super Admin or System Admin.
- Ensure that you do not select the RADIUS token servers that are part of an identity source sequence. If you select a RADIUS token server that is part of an identity source sequence for deletion, the delete operation fails.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **RADIUS Token**.

Step 2 Check the check box next to the RADIUS token server or servers that you want to delete, then click **Delete**.

Step 3 Click **OK** to delete the RADIUS token server or servers that you have selected.

If you select multiple RADIUS token servers for deleting, and one of them is used in an identity source sequence, the delete operation fails and none of the RADIUS token servers are deleted.

RSA Identity Sources

Cisco ISE supports the RSA SecurID server as an external database. RSA SecurID two-factor authentication consists of the PIN of the user and an individually registered RSA SecurID token that generates single-use token codes based on a time code algorithm. A different token code is generated at fixed intervals (usually each at 30 or 60 seconds). The RSA SecurID server validates this dynamic authentication code. Each RSA SecurID token is unique, and it is not possible to predict the value of a future token based on past tokens. Thus, when a correct token code is supplied together with a PIN, there is a high degree of certainty that the person is a valid user. Therefore, RSA SecurID servers provide a more reliable authentication mechanism than conventional reusable passwords.

Cisco ISE supports the following RSA identity sources:

- RSA ACE/Server 6.x series
- RSA Authentication Manager 7.x and 8.0 series

You can integrate with RSA SecurID authentication technology in any one of the following ways:

- Using the RSA SecurID agent: Users are authenticated with their username and passcode through the RSA native protocol.
- Using the RADIUS protocol: Users are authenticated with their username and passcode through the RADIUS protocol.

The RSA SecurID token server in Cisco ISE connects with the RSA SecurID authentication technology by using the RSA SecurID Agent.

Cisco ISE supports only one RSA realm.

Cisco ISE and RSA SecurID Server Integration

These are the two administrative roles involved in connecting Cisco ISE with an RSA SecurID server:

- RSA Server Administrator: Configures and maintains RSA systems and integration
- Cisco ISE Administrator: Configures Cisco ISE to connect to the RSA SecurID server and maintains the configuration

This section describes the processes that are involved in connecting Cisco ISE with the RSA SecurID server as an external identity source. For more information on RSA servers, please refer to the RSA documentation.

RSA Configuration in Cisco ISE

The RSA administrative system generates an sdconf.rec file, which the RSA system administrator will provide to you. This file allows you to add Cisco ISE servers as RSA SecurID agents in the realm. You have to browse and add this file to Cisco ISE. By the process of replication, the primary Cisco ISE server distributes this file to all the secondary servers.

RSA Agent Authentication Against the RSA SecurID Server

After the sdconf.rec file is installed on all Cisco ISE servers, the RSA agent module initializes, and authentication with RSA-generated credentials proceeds on each of the Cisco ISE servers. After the agent on each of the Cisco ISE servers in a deployment has successfully authenticated, the RSA server and the agent module together download the securid file. This file resides in the Cisco ISE file system and is in a well-known place defined by the RSA agent.

RSA Identity Sources in a Distributed Cisco ISE Environment

Managing RSA identity sources in a distributed Cisco ISE environment involves the following:

- Distributing the sdconf.rec and sdopts.rec files from the primary server to the secondary servers.
- Deleting the securid and sdstatus.12 files.

RSA Server Updates in a Cisco ISE Deployment

After you have added the sdconf.rec file in Cisco ISE, the RSA SecurID administrator might update the sdconf.rec file in case of decommissioning an RSA server or adding a new RSA secondary server. The RSA SecurID administrator will provide you with an updated file. You can then reconfigure Cisco ISE with the updated file. The replication process in Cisco ISE distributes the updated file to the secondary Cisco ISE servers in the deployment. Cisco ISE first updates the file in the file system and coordinates with the RSA agent module to phase the restart process appropriately. When the sdconf.rec file is updated, the sdstatus.12 and securid files are reset (deleted).

Override Automatic RSA Routing

You can have more than one RSA server in a realm. The sdopts.rec file performs the role of a load balancer. Cisco ISE servers and RSA SecurID servers operate through the agent module. The agent module that resides on Cisco ISE maintains a cost-based routing table to make the best use of the RSA servers in the realm. You can, however, choose to override this routing with a manual configuration for each Cisco ISE server for the realm using a text file called sdopts.rec through the Admin portal. Refer to the RSA documentation for information on how to create this file.

RSA Node Secret Reset

The securid file is a secret node key file. When RSA is initially set up, it uses a secret to validate the agents. When the RSA agent that resides in Cisco ISE successfully authenticates against the RSA server for the first time, it creates a file on the client machine called securid and uses it to ensure that the data exchanged between the machines is valid. At times, you may have to delete the securid file from a specific Cisco ISE server or a group of servers in your deployment (for example, after a key reset on the RSA server). You can use the Cisco ISE Admin portal to delete this file from a Cisco ISE server for the realm. When the RSA agent in Cisco ISE authenticates successfully the next time, it creates a new securid file.

Note If authentications fail after upgrading to a latest release of Cisco ISE, reset the RSA secret.

RSA Automatic Availability Reset

The sdstatus.12 file provides information about the availability of RSA servers in the realm. For example, it provides information on which servers are active and which are down. The agent module works with the RSA servers in the realm to maintain this availability status. This information is serially listed in the sdstatus.12 file, which is sourced in a well-known location in the Cisco ISE file system. Sometimes this file becomes old and the current status is not reflected in this file. You must remove this file so that the current status can be recreated. You can use the Admin portal to delete the file from a specific Cisco ISE server for a specific realm. Cisco ISE coordinates with the RSA agent and ensures correct restart phasing.

The sdstatus.12 file is deleted whenever the securid file is reset, or the sdconf.rec or sdopts.rec files are updated.

RSA SecurID Identity Source Settings

The following table describes the fields on the RSA SecurID Identity Sources window, which you can use to create and connect to an RSA SecurID identity source. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **RSA SecurID**.

RSA Prompt Settings

The following table describes the fields in the **RSA Prompts** tab.

Table 99: RSA Prompt Settings

Field Name	Usage Guidelines
Enter Passcode Prompt	Enter a text string to obtain the passcode.
Enter Next Token Code	Enter a text string to request the next token.
Choose PIN Type	Enter a text string to request the PIN type.
Accept System PIN	Enter a text string to accept the system-generated PIN.
Enter Alphanumeric PIN	Enter a text string to request an alphanumeric PIN.

Field Name	Usage Guidelines
Enter Numeric PIN	Enter a text string to request a numeric PIN.
Re-enter PIN	Enter a text string to request the user to re-enter the PIN.

RSA Message Settings

The following table describes the fields in the **RSA Messages** tab.

Table 100: RSA Messages Settings

Field Name	Usage Guidelines
Display System PIN Message	Enter a text string to label the system PIN message.
Display System PIN Reminder	Enter a text string to inform the user to remember the new PIN.
Must Enter Numeric Error	Enter a message that instructs users to enter only numbers for the PIN.
Must Enter Alpha Error	Enter a message that instructs users to enter only alphanumeric characters for PINs.
PIN Accepted Message	Enter a message that the users see when their PIN is accepted by the system.
PIN Rejected Message	Enter a message that the users see when the system rejects their PIN.
User Pins Differ Error	Enter a message that the users see when they enter an incorrect PIN.
System PIN Accepted Message	Enter a message that the users see when the system accepts their PIN.
Bad Password Length Error	Enter a message that the users see when the PIN that they specify does not fall within the range specified in the PIN length policy.

Related Topics

RSA Identity Sources, on page 758
Cisco ISE and RSA SecurID Server Integration, on page 759
Add RSA Identity Sources, on page 761

Add RSA Identity Sources

To create an RSA identity source, you must import the RSA configuration file (sdconf.rec). You must obtain the sdconf.rec file from your RSA administrator. To perform this task, you must be a Super Admin or System Admin.

Adding an RSA identity source involves the following tasks:

Import the RSA Configuration File

You must import the RSA configuration file to add an RSA identity source in Cisco ISE.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **RSA SecurID** > **Add**.

Step 2 Click **Browse** to choose the new or updated sdconf.rec file from the system that is running your client browser.

When you create the RSA identity source for the first time, the Import new sdconf.rec file field will be a mandatory field. From then on, you can replace the existing sdconf.rec file with an updated one, but replacing the existing file is optional.

Step 3 Enter the server timeout value in seconds. Cisco ISE will wait for a response from the RSA server for the amount of time specified before it times out. This value can be any integer from 1 to 199. The default value is 30 seconds.

Step 4 Check the **Reauthenticate on Change PIN** check box to force a reauthentication when the PIN is changed.

Step 5 Click **Save**.

Cisco ISE also supports the following scenarios:

- Configuring the Options File for a Cisco ISE Server and Resetting SecurID and sdstatus.12 Files.
- Configuring Authentication Control Options for RSA Identity Source.

Configure the Options File for a Cisco ISE Server and Resetting SecurID and sdstatus.12 Files

Step 1 Log into the Cisco ISE server.

Step 2 Choose **Administration** > **Identity Management** > **External Identity Sources** > **RSA SecurID** > **Add**.

Step 3 Click the **RSA Instance Files** tab.

This page lists the sdopts.rec files for all the Cisco ISE servers in your deployment.

The Node Secret Status is displayed as *Created* when the user is authenticated against RSA SecurID token server. The Node Secret Status can be one of the following—Created or Not Created. The Node Secret Status is displayed as *Not Created* when it is cleared.

Step 4 Click the radio button next to the sdopts.rec file for a particular Cisco ISE server, and click **Update Options File**.

The existing file is displayed in the Current File region.

Step 5 Choose one of the following:

- Use the Automatic Load Balancing status maintained by the RSA agent—Choose this option if you want the RSA agent to automatically manage load balancing.
- Override the Automatic Load Balancing status with the sdopts.rec file selected below—Choose this option if you want to manually configure load balancing based on your specific needs. If you choose this option, you must click **Browse** and choose the new sdopts.rec file from the system that is running your client browser.

Step 6 Click **OK**.

Step 7 Click the row that corresponds to the Cisco ISE server to reset the securid and sdstatus.12 files for that server:

a) Click the drop-down arrow and choose **Remove on Submit** in the Reset securid File and Reset sdstatus.12 File columns.

Note The Reset sdstatus.12 File field is hidden from your view. Using the vertical and horizontal scroll bars in the innermost frame, scroll down and then to your right to view this field.

b) Click **Save** in this row to save the changes.

Step 8 Click **Save**.

Configure Authentication Control Options for RSA Identity Source

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **RSA SecurID** > **Add**.

Step 2 Click the **Authentication Control** tab.

Step 3 Choose one of the following:

- Treat Rejects as “authentication failed”—Choose this option if you want the rejected requests to be treated as failed authentications.
- Treat Rejects as “user not found”—Choose this option if you want the rejected requests to be treated as user not found errors.

Step 4 Check the **Enable Passcode Caching** check box if you want Cisco ISE to store the passcode in the cache after the first successful authentication and use the cached user credentials for the subsequent authentications if they happen within the configured time period.

Enter the number of seconds for which the passcode must be stored in the cache in the **Aging Time** field. Within this period of time, the user can perform more than one authentication with the same passcode. The default value is 30 seconds. The valid range is from 1 to 300 seconds.

Note Cisco ISE clears the cache after the first failed authentication. The user must enter a new, valid passcode.

Note We strongly recommend that you enable this option only when you use a protocol that supports encryption of the passcode, for example, EAP-FAST-GTC.

Step 5 Check the **Enable Identity Caching** check box if you want to allow processing of requests that do not perform authentication against the server.

You can enable the identity caching option and set the aging time in minutes. The default value is 120 minutes. The valid range is from 1 to 1440 minutes. The results and attributes obtained from the last successful authentication are retained in the cache for the specified time period.

This option is disabled by default.

Step 6 Click **Save** to save the configuration.

Configure RSA Prompts

Cisco ISE allows you to configure RSA prompts that are presented to the user while processing requests sent to the RSA SecurID server.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **RSA SecurID**.

Step 2 Click **Prompts**.

Step 3 Enter the values as described in RSA SecurID Identity Source Settings.

Step 4 Click **Submit**.

Configure RSA Messages

Cisco ISE allows you to configure messages that are presented to the user while processing requests sent to the RSA SecurID server.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **RSA SecurID**.

Step 2 Click **Prompts**.

Step 3 Click the **Messages** tab.

Step 4 Enter the values as described in RSA SecurID Identity Source Settings.

Step 5 Click **Submit**.

SAMLv2 Identity Provider as an External Identity Source

Security Assertion Markup Language (SAML) is an XML-based open standard data format that enables administrators to access a defined set of applications seamlessly after signing into one of those applications. SAML describes the exchange of security related information between trusted business partners. SAML enables exchange of security authentication information between an Identity Provider (IdP) and a service provider (in this case, ISE).

SAML Single Sign On (SSO) establishes a Circle of Trust (CoT) by exchanging metadata and certificates as part of the provisioning process between the IdP and the Service Provider. The Service Provider trusts the IdP's user information to provide access to the various services or applications.

Enabling SAML SSO results in several advantages:

- It reduces password fatigue by removing the need for entering different user name and password combinations.
- It improves productivity because you spend less time re-entering credentials for the same identity.
- It transfers the authentication from your system that hosts the applications to a third party system.
- It reduces costs as fewer help desk calls are made for password reset, thereby leading to more savings.

The IdP is an authentication module that creates, maintains, and manages identity information for users, systems, or services. The IdP stores and validates the user credentials and generates a SAML response that allows the user to access the service provider protected resources.

Note You must be familiar with your IdP service, and ensure that it is currently installed and operational.

SAML SSO is supported for the following portals:

- Guest portal (sponsored and self-registered)
- Sponsor portal
- My Devices portal
- Certificate Provisioning portal

You cannot select IdP as external identity source for BYOD portal, but you can select an IdP for a guest portal and enable BYOD flow.

Cisco ISE is SAMLv2 compliant and supports all SAMLv2 compliant IdPs that use Base64-encoded certificates. The IdPs listed below have been tested with Cisco ISE:

- Oracle Access Manager (OAM)
- Oracle Identity Federation (OIF)
- SecureAuth
- PingOne
- PingFederate
- Microsoft Entra ID

The IdP cannot be added to an identity source sequence.

The SSO session will be terminated and Session Timeout error message will be displayed if there is no activity for the specified time (default is 5 minutes).

If you want to add the Sign On Again button in the Error page of the portal, add the following JavaScript in the Optional Content field in the Portal Error page:

```
<button class="cisco-ise" data-inline="true" data-mini="true" data-theme="b"
id="ui_aup_accept_button" onclick="location.href='PortalSetup.action?portal=<Portal ID>'"
type="button">SignOn Again</button>
```

Enabling Session Services

Before you begin

The session services must be enabled on the node on which you want to enable SAML SSO. To enable this option:

Step 1 Choose **Administration** > **System** > **Deployment**.

Step 2 Select the node and click **Edit**.

Step 3 In the **General Settings** tab, enable the **Policy Service** toggle button.

Step 4 Check the **Enable Session Services** check box and click **Save**.

Configure SAML Identity Providers in Cisco ISE

To configure SAML Identity Providers in Cisco ISE:

- You must be a Super Admin or System Admin in Cisco ISE.
- If the certificate to be used is not self-signed by the Identity Provider (IdP), import the Certificate Authority (CA) certificate in to the Trusted Certificate Store.
- You must have admin access to the IdP portal being configured. The following task involves some steps to be performed in the IdP portal.

To configure SAML Identity Providers in Cisco ISE:

1. Add a SAML Identity Provider to Cisco ISE.
2. Add SAML Identity Provider as the authentication method of a portal.
3. Configure SAML ID Provider.

Add a SAML Identity Provider to Cisco ISE

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **External Identity Sources** > **SAML Id Providers**.

Step 2 Click **Add**.

Step 3 In the **SAML Identity Provider** window displayed, enter the **Id Provider Name** and **Description** in the **General** tab.

Step 4 Click **Submit**.

Step 5 In the **Identity Provider Config** tab, import the relevant metadata.xml file, and click **Submit**.

Note The **Want Authentication Requests Signed** check box is read-only. The selection or non-selection of the option is automatically done based on the information in the metadata XML file that you upload.

To choose whether authentication requests must be signed, use the Sign Authentication Request check box in the Advanced Settings tab. The Sign Authentication Request takes precedence in execution.

Add an SAML Identity Provider as Authentication Method of a Portal

You can add the SAML Identity Provider you just created to the following portals:

1. Self-registered Guest Portals and Sponsored Guest Portals (**Work Centers** > **Guest Access** > **Portals and Components**)
2. Certificate Provisioning Portals (**Administration** > **Device Portal Management** > **Certificate Provisoning** > **Certificate Provisioning Portal)**

Step 1 In the portal customization window of the portal you are configuring, click **Portal Settings**.

Step 2 In the drop-down section that is displayed, go to **Authentication Method** section and use the menu to select the SAML IP Provider you added.

Step 3 Click **Save**.

Configure SAML ID Provider

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **External Identity Sources** > **SAML Id Providers**. Select the IdP that you have just linked to a portal, and click **Edit**.

Step 2 (Optional) If you are using a load balancer to optimize the load on Cisco ISE nodes, you can add its details in the **Service Provider Info** tab to simplify the configuration of IdPs. Software or hardware load balancers can be added.

The load balancer should be able to forward requests to the Cisco ISE nodes in the deployment using the port specified in the **Portal Settings** window.

When a load balancer is added, its URL alone is provided in the service provider metadata file. If a load balancer is not present, multiple **AssertionConsumerService** URLs are included in the service provider metadata file.

Note We recommend that you avoid using the same IP address of the load balancer at the portal FQDN setting.

Step 3 In the **Service Provider Info** tab, click **Export** to export the service provider metadata file. The exported metadata includes the signing certificate of Cisco ISE, which is identical to the chosen portal's certificate.

The exported metadata zip folder includes a Readme file that contains basic instructions for configuring each IdP (including, Microsoft Entra ID, PingOne, PingFederate, SecureAuth, and OAM)

You must re-export the service provider metadata if there are any changes in the following:

- Registration of a new Cisco ISE node.
- Hostname or IP Address of a node.
- Fully qualified domain name (FQDN) of My Devices, Sponsor, or Certificate Provisioning portal.

- Port or interface settings.
- Associated load balancer.

If the updated metadata is not re-exported, the IdP may reject a user authentication request.

Step 4 Go to your IdP portal and log in as Admin user, and import the service provider metadata file that you just exported from Cisco ISE. You need to first unzip the exported folder and a metadata file with the name of the portal. The metadata file includes the Provider ID and Binding URI.

Step 5 Return to the Cisco ISE portal.

Step 6 (Optional) In the **Groups** tab of the **SAML Identity Provider** window, add the required user groups.

Enter the assertion attribute that specifies the group membership of users in the **Group Membership Attribute** field.

Step 7 (Optional) Add the user attributes in the **Attributes** tab to specify how the attribute appears in the assertions returned from the IdP.

The name you specify in the **Name in ISE** field will appear in policy rules.

The following data types are supported for the attributes:

- String
- Integer
- IPv4
- Boolean

Step 8 Configure the following options in the **Advanced Settings** tab:

Option	Description
Identity Attribute	Select the attribute that specifies the identity of the user that is being authenticated by clicking the radio button against the options displayed. **Note** Cisco ISE does not support SAML IdP responses that contain subject name (NameID) in transient or persistent formats. Cisco ISE cannot retrieve the Username attribute assertion from the SAML IdP response if these methods are used and the authentication will fail.
Email attribute	From the drop-down list, select the assertion attribute which returns the email address of the user. The email attribute must be configured if you plan to filter (limit) the list of sponsored guests to be approved by a sponsor.
Multi-Value Attributes	Select one of the following: • **Each value in a separate XML**: Click this option if your IdP returns multiple values of the same attribute in separate XML elements. • **Multiple values in a single XML**: Click this option if your IdP returns multiple values in a single XML element. Specify the delimiter in the text box.
Authentication Settings	Cisco ISE signs authentication requests with defined certificates. For an SAML-signing request, an SAML-signing certificate must be properly defined. **a. Request**

Option	Description
	• **Sign Authentication Request**: Check this check box if your external identity provider requires signed requests. Some identity providers like PingFederate need signed authentication requests. • **Include Certificate Info**: Check this check box to include information about a particular certificate in the authentication request. **b. Response Signature** **Note** By default, Cisco ISE requires at least one signed SAML response or signed SAML assertion. Cisco ISE will enforce this even if the **Require SAML Signed Response** and **Require Assertions Signed** check boxes are not checked. You can check the appropraite check box to choose a specific signature from the following options: • **Require SAML Signed Response**: Choosing this option ensures that Cisco ISE only accepts signed SAML responses. • **Require Assertions Signed**: Choosing this option ensures that Cisco ISE only accepts SAML responses with signed SAML assertions. **c. Assertion Encryption** • **Require Assertions Encrypted**: Choosing this option ensures that Cisco ISE only accepts encrypted SAML assertions.
Logout Settings	Check the **Sign Logout Requests** check box if you want logout requests to be signed. This option is not displayed if the IdP being configured is Oracle Access Manager or Oracle Identity Federation. **Note** SecureAuth does not support SAML logout. The following options are displayed only when configuring Oracle Access Manager or Oracle Identity Federation IdPs, and a load balancer is not configured: • **Logout URL**: Enter the URL for the page to which a user is redirected to terminate an SSO session, when they log out of either the Sponsor or the My Devices portal. • **Redirect Parameter Name**: When the SSO session is terminated, the user is brought back to the IdP's login page.The redirect parameter name may differ based on the IdP, for example, **end_url** or **returnURL**. This field is case sensitive. If the logout does not work as expected, check the IdP's documentation for details on using logout URLs and redirect parameter names.
Authentication Context	Use this section to edit SAML IdP authentication context class reference. Cisco ISE SAML requests have typically used **PasswordProtectedTransport** authentication method in SAML request headings. This resulted in authentication failure in the case of multi-factor authentications being used. To avoid this, you can use **AuthnContextClassRef SAML Element** section to specify an authentication method. If you are unsure of the authentication method used, we recommend that you leave this section empty to avoid authentication failures.

Step 9 Click **Submit**.

Delete an Identity Provider

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Ensure that the IdP that you want to delete is not linked to any portal. If the IdP is linked to any portal, the delete operation fails.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers > Network Access > Ext Id Sources > SAML Id Providers**.

Step 2 Check the check box next to the IdP that you want to delete, and then click **Delete**.

Step 3 Click **OK** to delete the IdP that you have selected.

SAML-Based Admin Login

SAML-based login adds a single sign-on (SSO) capability to Cisco ISE using the SAML 2.0 standard. You can use an external identity provider (IdP) such as Okta, or any other IdP that implements the SAML 2.0 standard.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **SAML Id Providers** > **Add** > **General**.

Step 2 Enter a value in the **Id Provider Name** field.

Step 3 Click **Submit**.

Step 4 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Admin Access** > **Authentication** > **Authentication Method**.

Step 5 Click **Password Based** radio button.

Step 6 From the **Identity Source** drop-down list, choose the IdP name that was created earlier in the procedure.

Step 7 Click **Save**.

Step 8 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **SAML Id Providers**.

Step 9 Check the check box next to the IdP you created earlier in the procedure, and click **Edit**.

Step 10 In the **Service Provider Info** tab, click **Export** to download the service provider metadata. Cisco ISE metadata is exported as a .xml file. This metadata XML file contains information such as the **entityID** and the **AssertionConsumerService** URLs of all the nodes in the deployment. This information can be used to configure the nodes in the external Identity Provider.

Step 11 Open the metadata file.

Step 12 Log out and click **Log in With SAML**.

Step 13 The URL redirects you to the PSN IP address. Use this IP Address in the external Identity Provider. Alternatively, you can also configure multiple Single Sign On (SSO) URLs for all the PSNs in the network in the external Identity Provider.

Step 14 In the external Identity Provider, use the **AssertionConsumerService** URL and **entityID** from the exported metadata.

Step 15 Configure the Group Attributes in the Identity Provider.

Step 16 Export the Identity Provider metadata.

Step 17 In the **Identity Provider Config** tab, click **Choose File** to upload the Identity Provider metadata.

Note Admin Cisco ISE Portal should use a dedicated IdP. Do not re-use any IdP created for other portals such as Guest Portal.

Step 18 Under the **Groups** tab, enter the required value in the **Group Membership Attribute** field. Use the group attribute name that was used in the Identity Provider.

Step 19 Click **Add**.

Step 20 Enter the group name that is configured in Identity Provider, in **Name in Assertion**.

Step 21 Choose the admin group from **Name in ISE** drop-down list.

Step 22 Click **Add**.

Step 23 Click **Save**.

Step 24 The modified Cisco ISE login page is displayed. Click **Log in With SAML** to redirect to the Identity Provider for authentication.

Note In case of a multi-node deployment, use the FQDN instead of the IP Address to login.

Authentication Failure Log

When authentication against SAML ID Store fails and the IdP redirects the user back to ISE portal (through SAML response), ISE will report a failure reason in the authentication log. For Guest portal (with or without BYOD flow enabled), you can check the RADIUS Livelog (Operations > RADIUS > Live Log) to know the authentication failure reason. For My Devices portal and Sponsor portal, you can check the My Devices Login/Audit report and Sponsor Login/Audit report (under Operations > Reports > Guest) to know the authentication failure reason.

In case of logout failure, you can check the reports and logs to know the failure reason for My Devices, Sponsor, and Guest portal.

Authentication can fail due to the following reasons:

- SAML Response parse errors
- SAML Response validation errors (for example, Wrong Issuer)
- SAML Assertion validation errors (for example, Wrong Audience)
- SAML Response signature validation errors (for example, Wrong Signature)
- IdP signing certificate errors (for example, Certificate Revoked)

Note Cisco ISE does not support SAML responses with encrypted assertions. If this is configured in the IdP, you will see the following error message in ISE: `FailureReason=24803 Unable to find 'username' attribute assertion`.

If the authentication fails, we recommend that you check the "DetailedInfo" attribute in the authentication log. This attribute provides additional information regarding the cause of failure.

Identity Source Sequences

Identity source sequences define the order in which Cisco ISE looks for user credentials in the different databases.

If you have user information in more than one of the databases that are connected to Cisco ISE, you can define the order in which you want Cisco ISE to look for information in these identity sources. Once a match is found, Cisco ISE does not look any further, but evaluates the credentials, and returns the result to the user. This policy is the first match policy.

Create Identity Source Sequences

Before you begin

Ensure that you have configured your external identity sources in Cisco ISE.

To perform the following task, you must be a Super Admin or System Admin.

For allowing guest users to authenticate through Local WebAuth, you must configure both the Guest portal authentication source and the identity source sequence to contain the same identity stores.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **Identity Source Sequences** > **Add**.

Step 2 Enter a name for the identity source sequence. You can also enter an optional description.

Step 3 Check the **Select Certificate Authentication Profile** check box and choose a certificate authentication profile for certificate-based authentication.

Step 4 Choose the database or databases that you want to include in the identity source sequence in the **Selected List** field.

Step 5 Rearrange the databases in the **Selected list** field in the order in which you want Cisco ISE to search the databases.

Step 6 If a selected identity store cannot be accessed for authentication, choose one of the following options in the **Advanced Search List** area:

- **Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError**
- **Treat as if the user was not found and proceed to the next store in the sequence**

  While processing a request, Cisco ISE searches these identity sources in sequence. Ensure that you have the identity sources in the Selected list field listed in the order in which you want Cisco ISE to search them.

Step 7 Click **Submit** to create the identity source sequence that you can then use in policies.

Delete Identity Source Sequences

You can delete identity source sequences that you no longer use in policies.

Before you begin

- Ensure that the identity source sequence that you are about to delete is not used in any authentication policy.
- To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration** > **Identity Management** > **Identity Source Sequences**.

Step 2 Check the check box next to the identity source sequence or sequences that you want to delete, then click **Delete**.

Step 3 Click **OK** to delete the identity source sequence or sequences.

Identity Source Details in Reports

Cisco ISE provides information about the identity sources through the Authentications dashlet and Identity Source reports.

Authentications Dashlet

From the Authentications dashlet, you can drill down to find more information including failure reasons.

Choose Operations > RADIUS Livelog to view real-time authentication summary. For more information about RADIUS Live Logs, see RADIUS Live Logs, on page 443.

Identity Source Reports

Cisco ISE provides various reports that include information about identity sources. See the Available Reports section for a description of these reports.

Profiled Endpoints on the Network

The Profiler service assists in identifying, locating, and determining the capabilities of all endpoints on your network (known as identities in Cisco ISE), regardless of their device types, to ensure and maintain appropriate access to your enterprise network. The Cisco ISE Profiler function uses a number of probes to collect attributes for all endpoints on your network, and pass them to the Profiler analyzer, where the known endpoints are classified according to their associated policies and identity groups.

The Profiler Feed service allows administrators to retrieve new and updated endpoint profiling policies and the updated OUI database as a feed from a designated Cisco feed server through a subscription in to Cisco ISE.

Profiler Condition Settings

The following table describes the fields in the Profiler Condition window. The navigation path for this window is **Policy** > **Policy Elements** > **Conditions** > **Profiling**.

Table 101: Profiler Condition Settings

Field Name	Usage Guidelines
Name	Name of the profiler condition.
Description	Description of the profiler condition.
Type	Choose any one of the predefined types.
Attribute Name	Choose an attribute on which to base the profiler condition.
Operator	Choose an operator.
Attribute Value	Enter the value for the attribute that you have chosen. For Attribute Names that contain pre-defined Attribute Values, this option displays a drop-down list with the pre-defined values, and you can choose a value.
System Type	Profiling conditions can be any one of the following types: • **Cisco Provided**: Profiling conditions that are provided by Cisco ISE when deployed are identified as Cisco Provided. You cannot edit or delete them from the system. • **Administrator Created**: Profiling conditions that you create as an administrator of Cisco ISE are identified as Administrator Created.

Related Topics

Cisco ISE Profiling Service, on page 775
Profiler Conditions, on page 800
Profiler Feed Service, on page 838
Create a Profiler Condition, on page 815

Profiled Endpoints on the Network

The Profiler service assists in identifying, locating, and determining the capabilities of all endpoints on your network (known as identities in Cisco ISE), regardless of their device types, to ensure and maintain appropriate access to your enterprise network. The Cisco ISE Profiler function uses a number of probes to collect attributes for all endpoints on your network, and pass them to the Profiler analyzer, where the known endpoints are classified according to their associated policies and identity groups.

The Profiler Feed service allows administrators to retrieve new and updated endpoint profiling policies and the updated OUI database as a feed from a designated Cisco feed server through a subscription in to Cisco ISE.

Profiler Condition Settings

The following table describes the fields in the Profiler Condition window. The navigation path for this window is **Policy** > **Policy Elements** > **Conditions** > **Profiling**.

Table 102: Profiler Condition Settings

Field Name	Usage Guidelines
Name	Name of the profiler condition.
Description	Description of the profiler condition.
Type	Choose any one of the predefined types.
Attribute Name	Choose an attribute on which to base the profiler condition.
Operator	Choose an operator.
Attribute Value	Enter the value for the attribute that you have chosen. For Attribute Names that contain pre-defined Attribute Values, this option displays a drop-down list with the pre-defined values, and you can choose a value.
System Type	Profiling conditions can be any one of the following types: • **Cisco Provided**: Profiling conditions that are provided by Cisco ISE when deployed are identified as Cisco Provided. You cannot edit or delete them from the system. • **Administrator Created**: Profiling conditions that you create as an administrator of Cisco ISE are identified as Administrator Created.

Related Topics

Cisco ISE Profiling Service, on page 775
Profiler Conditions, on page 800
Profiler Feed Service, on page 838
Create a Profiler Condition, on page 815

Cisco ISE Profiling Service

The profiling service in Cisco Identity Services Engine (ISE) identifies the devices that connect to your network and their location. The endpoints are profiled based on the endpoint profiling policies configured in Cisco ISE. Cisco ISE then grants permission to the endpoints to access the resources in your network based on the result of the policy evaluation.

The profiling service:

- Facilitates an efficient and effective deployment and ongoing management of authentication by using IEEE standard 802.1X port-based authentication access control, MAC Authentication Bypass (MAB) authentication, and Network Admission Control (NAC) for any enterprise network of varying scale and complexity.
- Identifies, locates, and determines the capabilities of all of the attached network endpoints regardless of endpoint types.
- Protects against inadvertently denying access to some endpoints.

ISE Community Resource

ISE Endpoint Profiles

How To: ISE Profiling Design Guide

Profiler Work Center

The Profiler Work Center menu (Work Centers > Profiler) contains all the profiler pages, which acts as a single start point for ISE administrators. The Profiler Work Center menu contains the following options: Overview, Ext ID Stores, Network Devices, Endpoint Classification, Node Config, Feeds, Manual Scans, Policy Elements, Profiling Policies, Authorization Policy, Troubleshoot, Reports, Settings, and Dictionaries.

Profiler Dashboard

The Profiler dashboard (Work Centers > Profiler > Endpoint Classification) is a centralized monitoring tool for the profiles, endpoints, and assets in your network. The dashboard represents data in both graphical and table formats. The Profiles dashlet displays the logical and endpoint profiles that are currently active in the network. The Endpoints dashlet displays the identity group, PSNs, OS types of the endpoints that connect to your network. The Assets dashlet displays flows such as Guest, BYOD, and Corporate. The table displays the various endpoints that are connected and you can also add new endpoints.

Endpoint Inventory Using Profiling Service

You can use the profiling service to discover, locate, and determine the capabilities of all the endpoints connected to your network. You can ensure and maintain appropriate access of endpoints to the enterprise network, regardless of their device types.

The profiling service collects attributes of endpoints from the network devices and the network, classifies endpoints into a specific group according to their profiles, and stores endpoints with their matched profiles in the Cisco ISE database. All the attributes that are handled by the profiling service need to be defined in the profiler dictionaries.

The profiling service identifies each endpoint on your network, and groups those endpoints according to their profiles to an existing endpoint identity group in the system, or to a new group that you can create in the system. By grouping endpoints, and applying endpoint profiling policies to the endpoint identity group, you can determine the mapping of endpoints to the corresponding endpoint profiling policies.

Cisco ISE Profiler Queue Limit Configuration

Cisco ISE profiler collects a significant amount of endpoint data from the network in a short period of time. It causes Java Virtual Machine (JVM) memory utilization to go up due to accumulated backlog when some of the slower Cisco ISE components process the data generated by the profiler, which results in performance degradation and stability issues.

To ensure that the profiler does not increase the JVM memory utilization and prevent JVM to go out of memory and restart, limits are applied to the following internal components of the profiler:

- Endpoint Cache: Internal cache is limited in size that has to be purged periodically (based on least recently used strategy) when the size exceeds the limit.
- Forwarder: The main ingress queue of endpoint information collected by the profiler.
- Event Handler: An internal queue that disconnects a fast component, which feeds data to a slower processing component (typically related to a database query).

Endpoint Cache

- maxEndPointsInLocalDb = 100000 (endpoint objects in cache)
- endPointsPurgeIntervalSec = 300 (endpoint cache purge thread interval in seconds)
- numberOfProfilingThreads = 8 (number of threads)

The limit is applicable to all profiler internal event handlers. A monitoring alarm is triggered when queue size limit is reached.

Cisco ISE Profiler Queue Size Limits

- forwarderQueueSize = 5000 (endpoint collection events)
- eventHandlerQueueSize = 10000 (events)

Event Handlers

- NetworkDeviceEventHandler: For network device events, in addition to filtering duplicate Network Access Device (NAD) IP addresses, which are already cached.
- ARPCacheEventHandler: For ARP Cache events.

Martian IP Addresses

Martian IP addresses are not displayed in **Context Visibility** > **Endpoints** and **Work Centers** > **Profiler** > **Endpoint Classification** windows as the RADIUS parser removes such addresses before they reach the profiling service. Martian IP addresses are a security concern as they are vulnerable to attacks. However, martian IP addresses are displayed in MnT logs for auditing purposes. This behaviour stands true in the case of multicast IP addresses as well. For more information on Martian IP addresses, see https://www.cisco.com/assets/sol/sb/Switches_Emulators_v2_3_5_xx/help/250/index.html#page/tesla_250_olh/martian_addresses.html

Profiler Forwarder Persistence Queue

The Profiler Forwarder Persistence queue stores events before they are sent to the profiler module for further processing. In addition, the queuing capacity has also been increased to support increased event handling. This reduces the number events that are lost because of a sudden increase in the number of events. This in turn reduces the alarms raised, when the queue reaches its maximum limit.

This feature is enabled by default. If required, you can disable this feature to fall back to the original mechanism, where events are sent directly to the profiler module. To enable or disable this feature, choose **Administration** > **System** > **Settings** > **Profiling** and check or uncheck the **Enable Profiler Forwarder Persistence Queue** check box.

Configure Profiling Service in Cisco ISE Nodes

You can configure the profiling service that provides you a contextual inventory of all the endpoints that are using your network resources in any Cisco ISE-enabled network.

You can configure the profiling service to run on a single Cisco ISE node that assumes all Administration, Monitoring, and Policy Service personas by default.

In a distributed deployment, the profiling service runs only on Cisco ISE nodes that assume the Policy Service persona and does not run on other Cisco ISE nodes that assume the Administration and Monitoring personas.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 2 Choose a Cisco ISE node that assumes the Policy Service persona.

Step 3 Click **Edit** in the Deployment Nodes page.

Step 4 On the **General Settings** tab, check the **Policy Service** check box. If the Policy Service check box is unchecked, both the session services and the profiling service check boxes are disabled.

Step 5 Perform the following tasks:

a) Check the **Enable Session Services** check box to run the Network Access, Posture, Guest, and Client Provisioning session services.
b) Check the **Enable Profiling Services** check box to run the profiling service.
c) Check the **Enable Device Admin Service** check box to run the device administration service to control and audit an enterprise's network devices.

Step 6 Click **Save** to save the node configuration.

Network Probes Used by Profiling Service

Network probe is a method used to collect an attribute or a set of attributes from an endpoint on your network. The probe allows you to create or update endpoints with their matched profile in the Cisco ISE database.

Cisco ISE can profile devices using a number of network probes that analyze the behavior of devices on the network and determine the type of the device. Network probes help you to gain more network visibility.

IP Address and MAC Address Binding

You can create or update endpoints only by using their MAC addresses in an enterprise network. If you do not find an entry in the ARP cache, then you can create or update endpoints by using the L2 MAC address of an HTTP packet and the IN_SRC_MAC of a NetFlow packet in Cisco ISE. The profiling service is dependent on L2 adjacency when endpoints are only a hop away. When endpoints are L2 adjacent, the IP addresses and MAC addresses of endpoints are already mapped, and there is no need for IP-MAC cache mapping.

If endpoints are not L2 adjacent and are multiple hops away, mapping may not be reliable. Some of the known attributes of NetFlow packets that you collect include PROTOCOL, L4_SRC_PORT, IPV4_SRC_ADDR, L4_DST_PORT, IPV4_DST_ADDR, IN_SRC_MAC, OUT_DST_MAC, IN_SRC_MAC, and OUT_SRC_MAC. When endpoints are not L2 adjacent and are multiple L3 hops away, the IN_SRC_MAC attributes carry only the MAC addresses of L3 network devices. When the HTTP probe is enabled in Cisco ISE, you can create endpoints only by using the MAC addresses of HTTP packets, because the HTTP request messages do not carry IP addresses and MAC addresses of endpoints in the payload data.

Cisco ISE implements an ARP cache in the profiling service, so that you can reliably map the IP addresses and the MAC addresses of endpoints. For the ARP cache to function, you must enable either the DHCP probe or the RADIUS probe. The DHCP and RADIUS probes carry the IP addresses and the MAC addresses of endpoints in the payload data. The dhcp-requested address attribute in the DHCP probe and the Framed-IP-address attribute in the RADIUS probe carry the IP addresses of endpoints, along with their MAC addresses, which can be mapped and stored in the ARP cache.

NetFlow Probe

Cisco ISE profiler implements Cisco IOS NetFlow Version 9. We recommend using NetFlow Version 9, which has additional functionality needed to enhance the profiler to support the Cisco ISE profiling service.

You can collect NetFlow Version 9 attributes from the NetFlow-enabled network access devices to create an endpoint, or update an existing endpoint in the Cisco ISE database. You can configure NetFlow Version 9 to attach the source and destination MAC addresses of endpoints and update them. You can also create a dictionary of NetFlow attributes to support NetFlow-based profiling.

For more information on the NetFlow Version 9 Record Format, see Table 6, “NetFlow Version 9 Field Type Definitions” of the NetFlow Version 9 Flow-Record Format document.

In addition, Cisco ISE supports NetFlow versions earlier than Version 5. If you use NetFlow Version 5 in your network, then you can use Version 5 only on the primary network access device (NAD) at the access layer because it will not work anywhere else.

Cisco IOS NetFlow Version 5 packets do not contain MAC addresses of endpoints. The attributes that are collected from NetFlow Version 5 cannot be directly added to the Cisco ISE database. You can discover endpoints by using their IP addresses, and append the NetFlow Version 5 attributes to endpoints, which can be done by combining IP addresses of the network access devices and IP addresses obtained from the NetFlow Version 5 attributes. However, these endpoints must have been previously discovered with the RADIUS or SNMP probe.

The MAC address is not a part of IP flows in earlier versions of NetFlow Version 5, which requires you to profile endpoints with their IP addresses by correlating the attributes information collected from the network access devices in the endpoints cache.

For more information on the NetFlow Version 5 Record Format, see Table 2, “Cisco IOS NetFlow Flow Record and Export Format Content Information” of the NetFlow Services Solutions Guide.

DHCP Probe

The Dynamic Host Configuration Protocol probe in your Cisco ISE deployment allows the Cisco ISE profiling service to reprofile endpoints based only on new requests of INIT-REBOOT and SELECTING message types. Though other DHCP message types such as RENEWING and REBINDING are processed, they are not used for profiling endpoints. Any attribute parsed out of DHCP packets is mapped to endpoint attributes.

DHCPREQUEST Message Generated During INIT-REBOOT State

If the DHCP client checks to verify a previously allocated and cached configuration, then the client must not fill in the Server identifier (server-ip) option. Instead it should fill in the Requested IP address (requested-ip) option with the previously assigned IP address, and fill in the Client IP Address (ciaddr) field with zero in its DHCPREQUEST message. The DHCP server will then send a DHCPNAK message to the client if the Requested IP address is incorrect or the client is located in the wrong network.

DHCPREQUEST Message Generated During SELECTING State

The DHCP client inserts the IP address of the selected DHCP server in the Server identifier (server-ip) option, fills in the Requested IP address (requested-ip) option with the value of the Your IP Address (yiaddr) field from the chosen DHCPOFFER by the client, and fills in the “ciaddr” field with zero.

Table 103: DHCP Client Messages from Different States

—	INIT-REBOOT	SELECTING	RENEWING	REBINDING
broadcast/unicast	broadcast	broadcast	unicast	broadcast
server-ip	MUST NOT	MUST	MUST NOT	MUST NOT
requested-ip	MUST	MUST	MUST NOT	MUST NOT
ciaddr	zero	zero	IP address	IP address

Wireless LAN Controller Configuration in DHCP Bridging Mode

We recommend that you configure wireless LAN controllers (WLCs) in Dynamic Host Configuration Protocol (DHCP) bridging mode, where you can forward all the DHCP packets from the wireless clients to Cisco ISE. You must uncheck the Enable DHCP Proxy check box available in the WLC web interface: **Controller** > **Advanced** > **DHCP Master Controller Mode** > **DHCP Parameters**. You must also ensure that the DHCP IP helper command points to the Cisco ISE Policy Service node.

DHCP SPAN Probe

The DHCP Switched Port Analyzer (SPAN) probe, when initialized in a Cisco ISE node, listens to network traffic, which are coming from network access devices on a specific interface. You need to configure network access devices to forward DHCP SPAN packets to the Cisco ISE profiler from the DHCP servers. The profiler receives these DHCP SPAN packets and parses them to capture the attributes of an endpoint, which can be used for profiling endpoints.

For example,

```
switch(config)# monitor session 1 source interface Gi1/0/4
switch(config)# monitor session 1 destination interface Gi1/0/2
```

HTTP Probe

In HTTP probe, the identification string is transmitted in an HTTP request-header field User-Agent, which is an attribute that can be used to create a profiling condition of IP type, and to check the web browser information. The profiler captures the web browser information from the User-Agent attribute along with other HTTP attributes from the request messages, and adds them to the list of endpoint attributes.

Cisco ISE listens to communication from the web browsers on both port 80 and port 8080. Cisco ISE provides many default profiles, which are built in to the system to identify endpoints based on the User-Agent attribute.

HTTP probe is enabled by default. Multiple ISE services such as CWA, Hotspot, BYOD, MDM, and Posture rely on URL-redirection of the client's web browser. The redirected traffic includes the RADIUS session ID of the connected endpoint. When a PSN terminates these URL-redirected flows, it has visibility into the decrypted HTTPS data. Even when the HTTP probe is disabled on the PSN, the node will parse the browser user agent string from the web traffic and correlate the data to the endpoint based on its associated session ID. When browser strings are collected through this method, the source of the data is listed as Guest Portal or CP (Client Provisioning) rather than HTTP Probe.

HTTP SPAN Probe

The HTTP probe in your Cisco ISE deployment, when enabled with the Switched Port Analyzer (SPAN) probe, allows the profiler to capture HTTP packets from the specified interfaces. You can use the SPAN capability on port 80, where the Cisco ISE server listens to communication from the web browsers.

HTTP SPAN collects HTTP attributes of an HTTP request-header message along with the IP addresses in the IP header (L3 header), which can be associated to an endpoint based on the MAC address of an endpoint in the L2 header. This information is useful for identifying different mobile and portable IP-enabled devices such as Apple devices, and computers with different operating systems. Identifying different mobile and portable IP-enabled devices is made more reliable because the Cisco ISE server redirects captures during a guest login or client provisioning download. This allows the profiler to collect the User-Agent attribute and other HTTP attributes, from the request messages and then identify devices such as Apple devices.

Unable to Collect HTTP Attributes in Cisco ISE Running on VMware

If you deploy Cisco ISE on an ESX server (VMware), the Cisco ISE profiler collects the Dynamic Host Configuration Protocol traffic but does not collect the HTTP traffic due to configuration issues on the vSphere client. To collect HTTP traffic on a VMware setup, configure the security settings by changing the Promiscuous Mode to Accept from Reject (by default) of the virtual switch that you create for the Cisco ISE profiler. When the Switched Port Analyzer (SPAN) probe for DHCP and HTTP is enabled, Cisco ISE profiler collects both the DHCP and HTTP traffic.

pxGrid Probe

The pxGrid probe leverages Cisco pxGrid for receiving endpoint context from external sources. Prior to Cisco ISE 2.4, Cisco ISE served only as a publisher and shared various context information such as session identity and group information as well as configuration elements to external subscribers. With the introduction of the pxGrid probe in Cisco ISE 2.4, other solutions serve as the publishers and Cisco ISE Policy Service nodes become the subscribers.

The pxGrid probe is based on pxGrid v2 specification using the Endpoint Asset topic */topic/com.cisco.endpoint.asset* with Service Name *com.cisco.endpoint.asset*. The following table displays the topic attributes all of which are preceded by the prefix *asset*.

Table 104: Endpoint Asset Topic

Attribute Name	Type	Description
assetId	Long	Asset ID
assetName	String	Asset name
assetIpAddress	String	IP address
assetMacAddress	String	MAC address
assetVendor	String	Manufacturer
assetProductId	String	Product Code
assetSerialNumber	String	Serial Number
assetDeviceType	String	Device Type
assetSwRevision	String	S/W Revision number
assetHwRevision	String	H/W Revision number
assetProtocol	String	Protocol
assetConnectedLinks	Array	Array of Network Link objects
assetCustomAttributes	Array	Array of Custom name-value pairs

In addition to the attributes commonly used to track networked assets such as device MAC address (assetMacAddress) and IP address (assetIpAddress), the topic allows vendors to publish unique endpoint information as Custom Attributes (assetCustomAttributes). The use of Endpoint Custom Attributes in Cisco ISE makes the topic extensible to a variety of use cases without requiring schema updates for each new set of unique vendor attributes shared over pxGrid.

RADIUS Probe

You can configure Cisco ISE for authentication with RADIUS, where you can define a shared secret that you can use in client-server transactions. With the RADIUS request and response messages that are received from the RADIUS servers, the profiler can collect RADIUS attributes, which can be used for profiling endpoints.

Cisco ISE can function as a RADIUS server, and a RADIUS proxy client to other RADIUS servers. When it acts as a proxy client, it uses external RADIUS servers to process RADIUS requests and response messages.

The RADIUS probe also collects attributes sent in RADIUS accounting packets by device sensors. For more information, see Attributes Collection from Cisco IOS Sensor-Embedded Switches, on page 795 and Configuration Checklist for Cisco IOS Sensor-Enabled Network Access Devices, on page 796.

The RADIUS probe is running by default, even for systems not configured for Profiling Service to ensure ISE can track endpoint authentication and authorization details for use in Context Visibility Services.

The RADIUS probe and Profiling Services are also used to track the creation and update times for registered endpoints for purposes of purge operations.

Table 105: Common Attributes Collected Using the RADIUS Probe

User Name	Calling Station ID	Called Station ID	Framed IP Address
NAS-IP-Address	NAS-Port-Type	NAS-Port-Id	NAS-Identifier
Device Type (NAD)	Location (NAD)	Authentication Policy	Authorization Policy

Note When an accounting stop is received, it triggers the Cisco ISE to reprofile the corresponding endpoint if it was originally profiled with an IP address. Therefore if you have custom profiles for endpoints profiled with IP addresses, the only way to meet the total certainty factor for these profiles is to match on the corresponding IP address.

Network Scan (NMAP) Probe

Cisco ISE enables you to detect devices in a subnet by using the NMAP security scanner. You enable the NMAP probe on the Policy Service node that is enabled to run the profiling service. You use the results from that probe in an endpoint profiling policy.

Each NMAP manual subnet scan has a unique numeric ID that is used to update an endpoint source information with that scan ID. Upon detection of endpoints, the endpoint source information can also be updated to indicate that it is discovered by the Network Scan probe.

The NMAP manual subnet scan is useful for detecting devices such as printers with a static IP address assigned to them that are connected constantly to the Cisco ISE network, and therefore these devices cannot be discovered by other probes.

NMAP Scan Limitations

Scanning a subnet is highly resource intensive. Scanning a subnet is lengthy process that depends on the size and density of the subnet. Number of active scans is always restricted to one scan, which means that you can scan only a single subnet at a time. You can cancel a subnet scan at any time while the subnet scan is in progress. You can use the **Click** to see latest scan results link to view the most recent network scan results that are stored in **Work Centers** > **Profiler** > **Manual Scans** > **Manual NMAP Scan Results**.

Manual NMAP Scan

The following NMAP command scans a subnet and sends the output to nmapSubnet.log:

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log
    --append-output -oX - <subnet>
```

Table 106: NMAP Commands for a Manual Subnet Scan

-O	Enables OS detection
-sU	UDP scan
-p <port ranges>	Scans only specified ports. For example, U:161, 162
oN	Normal output

oX	XML output

SNMP Read Only Community Strings for NMAP Manual Subnet Scan

The NMAP manual subnet scan is augmented with an SNMP Query whenever the scan discovers that UDP port 161 is open on an endpoint that results in more attributes being collected. During the NMAP manual subnet scan, the Network Scan probe detects whether SNMP port 161 is open on the device. If the port is open, an SNMP Query is triggered with a default community string (public) with SNMP version 2c.

If the device supports SNMP and the default Read Only community string is set to public, you can obtain the MAC address of the device from the MIB value “ifPhysAddress”.

In addition, you can configure additional SNMP Read Only community strings separated by a comma for the NMAP manual network scan in the **Profiler Configuration** window. You can also specify new Read Only community strings for an SNMP MIB walk with SNMP versions 1 and 2c. For information on configuring SNMP Read Only community strings, see Setup CoA, SNMP RO Community, and Endpoint Attribute Filter, on page 789.

Manual NMAP Scan Results

The most recent network scan results are stored in Work Centers > Profiler > Manual Scans > Manual NMAP Scan Results. The Manaul NMAP Scan Results page displays only the most recent endpoints that are detected, along with their associated endpoint profiles, their MAC addresses, and their static assignment status as the result of a manual network scan you perform on any subnet. This page allows you to edit points that are detected from the endpoint subnet for better classification, if required.

Cisco ISE allows you to perform the manual network scan from the Policy Service nodes that are enabled to run the profiling service. You must choose the Policy Service node from the primary Administration ISE node user interface in your deployment to run the manual network scan from the Policy Service node. During the manual network scan on any subnet, the Network Scan probe detects endpoints on the specified subnet, their operating systems, and check UDP ports 161 and 162 for an SNMP service.

Given below is additional information related to the manual NMAP scan results:

- To detect unknown endpoints, NMAP should be able to learn the IP/MAC binding via NMAP or a supporting SNMP scan.
- ISE learns IP/MAC binding of known endpoints via Radius authentication or DHCP profiling.
- The IP/MAC bindings are not replicated across PSN nodes in a deployment. Therefore, you must trigger the manual scan from the PSN, which has the IP/MAC binding in its local database (for example, the PSN against which a mac address was last authenticated with).
- The NMAP scan results do not display any information related to an endpoint that NMAP had previously scanned, manually or automatically.

DNS Probe

The Domain Name Service (DNS) probe in your Cisco ISE deployment allows the profiler to lookup an endpoint and get the fully qualified domain name (FQDN). After an endpoint is detected in your Cisco ISE-enabled network, a list of endpoint attributes is collected from the NetFlow, DHCP, DHCP SPAN, HTTP, RADIUS, or SNMP probes.

When you deploy Cisco ISE in a standalone or in a distributed environment for the first time, you are prompted to run the setup utility to configure the Cisco ISE appliance. When you run the setup utility, you will configure the Domain Name System (DNS) domain and the primary nameserver (primary DNS server), where you can configure one or more nameservers during setup. You can also change or add DNS nameservers later after deploying Cisco ISE using the CLI commands.

DNS FQDN Lookup

Before a DNS lookup can be performed, one of the following probes must be started along with the DNS probe: DHCP, DHCP SPAN, HTTP, RADIUS, or SNMP. This allows the DNS probe in the profiler to do a reverse DNS lookup (FQDN lookup) against specified name servers that you define in your Cisco ISE deployment. A new attribute is added to the attribute list for an endpoint, which can be used for an endpoint profiling policy evaluation. The FQDN is the new attribute that exists in the system IP dictionary. You can create an endpoint profiling condition to validate the FQDN attribute and its value for profiling. The following are the specific endpoint attributes that are required for a DNS lookup and the probe that collects these attributes:

- The dhcp-requested-address attribute—An attribute collected by the DHCP and DHCP SPAN probes.
- The SourceIP attribute—An attribute collected by the HTTP probe
- The Framed-IP-Address attribute—An attribute collected by the RADIUS probe
- The cdpCacheAddress attribute—An attribute collected by the SNMP probe

Configure Call Station ID Type in the WLC Web Interface

You can use the WLC web interface to configure Call Station ID Type information. You can go to the Security tab of the WLC web interface to configure the calling station ID in the RADIUS Authentication Servers page. The MAC Delimiter field is set to Colon by default in the WLC user interface.

For more information on how to configure in the WLC web interface, see Chapter 6, “Configuring Security Solutions” in the Cisco Wireless LAN Controller Configuration Guide, Release 7.2.

For more information on how to configure in the WLC CLI using the config radius callStationIdType command, see Chapter 2, “Controller Commands” in the Cisco Wireless LAN Controller Command Reference Guide, Release 7.2.

Step 1 Log in to your Wireless LAN Controller user interface.

Step 2 Click **Security**.

Step 3 Expand **AAA**, and then choose **RADIUS** > **Authentication**.

Step 4 Choose **System MAC Address** from the Call Station ID Type drop-down list.

Step 5 Check the **AES Key Wrap** check box when you run Cisco ISE in FIPS mode.

Step 6 Choose **Colon** from the MAC Delimeter drop-down list.

SNMP Query Probe

In addition to configuring the SNMP Query probe in the Edit Node page, you must configure other Simple Management Protocol settings in the following location: **Administration** > **Network Resources** > **Network Devices**.

You can configure SNMP settings in the new network access devices (NADs) in the Network Devices list page. The polling interval that you specify in the SNMP query probe or in the SNMP settings in the network access devices query NADs at regular intervals.

You can turn on and turn off SNMP querying for specific NADs based on the following configurations:

- SNMP query on Link up and New MAC notification turned on or turned off
- SNMP query on Link up and New MAC notification turned on or turned off for Cisco Discovery Protocol information
- SNMP query timer for once an hour for each switch by default

For an iDevice, and other mobile devices that do not support SNMP, the MAC address can be discovered by the ARP table, which can be queried from the network access device by an SNMP Query probe.

Cisco Discovery Protocol Support with SNMP Query

When you configure SNMP settings on the network devices, you must ensure that the Cisco Discovery Protocol is enabled (by default) on all the ports of the network devices. If you disable the Cisco Discovery Protocol on any of the ports on the network devices, then you may not be able to profile properly because you will miss the Cisco Discovery Protocol information of all the connected endpoints. You can enable the Cisco Discovery Protocol globally by using the cdp run command on a network device, and enable the Cisco Discovery Protocol by using the cdp enable command on any interface of the network access device. To disable the Cisco Discovery Protocol on the network device and on the interface, use the no keyword at the beginning of the commands.

Link Layer Discovery Protocol Support with SNMP Query

The Cisco ISE profiler uses an SNMP Query to collect LLDP attributes. You can also collect LLDP attributes from a Cisco IOS sensor, which is embedded in the network device, by using the RADIUS probe. The following are the default LLDP configuration settings that you can use to configure LLDP global configuration and LLDP interface configuration commands on the network access devices.

Table 107: Default LLDP Configuration

Attribute	Setting
LLDP global state	Disabled
LLDP holdtime (before discarding)	120 seconds
LLDP timer (packet update frequency)	30 seconds
LLDP reinitialization delay	2 seconds
LLDP tlv-select	Enabled to send and receive all TLVs.

Attribute	Setting
LLDP interface state	Enabled
LLDP receive	Enabled
LLDP transmit	Enabled
LLDP med-tlv-select	Enabled to send all LLDP-MED TLVs

CDP and LLDP Capability Codes Displayed in a Single Character

The Attribute List of an endpoint displays a single character value for the lldpCacheCapabilities and lldpCapabilitiesMapSupported attributes. The values are the Capability Codes that are displayed for the network access device that runs CDP and LLDP.

Example 1

```
lldpCacheCapabilities S
lldpCapabilitiesMapSupported S
```

Example 2

```
lldpCacheCapabilities B;T
lldpCapabilitiesMapSupported B;T
```

Example 3

```
Switch#show cdp neighbors
Capability Codes:
R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP,
r - Repeater, P - Phone, D - Remote, C - CVTA, M - Two-port Mac Relay
...
Switch#

Switch#show lldp neighbors
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
...
Switch#
```

SNMP Trap Probe

The SNMP Trap receives information from the specific network access devices that support MAC notification, linkup, linkdown, and informs. The SNMP Trap probe receives information from the specific network access devices when ports come up or go down and endpoints disconnect from or connect to your network.

For SNMP Trap to be fully functional and create endpoints, you must enable SNMP Query so that the SNMP Query probe triggers a poll event on the particular port of the network access device when a trap is received. To make this feature fully functional, you should configure the network access device and SNMP Trap.

Note Cisco ISE does not support SNMP Traps that are received from the Wireless LAN Controllers (WLCs) and Access Points (APs).

Active Directory Probe

The Active Directory (AD) probe:

- Improves the fidelity of OS information for Windows endpoints. Microsoft AD tracks detailed OS information for AD-joined computers including version and service pack levels. The AD probe retrieves this information directly using the AD Runtime connector to provide a highly reliable source of client OS information.
- Helps distinguish between corporate and non-corporate assets. A basic but important attribute available to the AD probe is whether an endpoint exists in AD. This information can be used to classify an endpoint contained in the AD as a managed device or corporate asset.

You can enable the AD probe under **Administration** > **System** > **Deployment** > **Profiling Configuration**. When this probe is enabled, Cisco ISE fetches the AD attributes for a new endpoint as soon as it receives a hostname. The hostname is typically learned from the DHCP or DNS probes. Once successfully retrieved, ISE does not attempt to query AD again for the same endpoint until a the rescan timer expires. This is to limit the load on AD for attribute queries. The rescan timer is configurable in the **Days Before Rescan** field (**Administration** > **System** > **Deployment** > **Profiling Configuration** > **Active Directory**). If there is additional profiling activity on the endpoint, the AD is queried again.

The following AD probe attributes can be matched in the **Policy** > **Policy Elements** > **Profiling** using the ACTIVEDIRECTORY condition. AD attributes collected using the AD Probe appear with the prefix “AD” in the endpoint details on the **Context Visibility** > **Endpoints** window.

- AD-Host-Exists
- AD-Join-Point
- AD-Operating-System
- AD-OS-Version
- AD-Service-Pack

Configure Probes for Each Cisco ISE Node

You can configure one or more probes on the Profiling Configuration tab per Cisco ISE node in your deployment that assumes the Policy Service persona, which could be:

- A standalone node: If you have deployed Cisco ISE on a single node that assumes all Administration, Monitoring, and Policy Service personas by default.

- Multiple nodes: If you have registered more than one node in your deployment that assume Policy Service persona.

Note Not all probes are enabled by default. Some probes are partially enabled even when they are not explicitly enabled by a check mark. The profiling configuration is currently unique to each PSN. We recommend that each PSN in the deployment should be configured with identical profiler configuration settings.

Before you begin

You can configure the probes per Cisco ISE node only from the Administration node, which is unavailable on the secondary Administration node in a distributed deployment.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 2 Choose a Cisco ISE node that assumes the Policy Service persona.

Step 3 Click **Edit** in the Deployment Nodes page.

Step 4 On the **General Settings** tab, check the **Policy Service** check box. If the Policy Service check box is unchecked, both the session services and the profiling service check boxes are disabled.

Step 5 Check the **Enable Profiling Services** check box.

Step 6 Click the **Profiling Configuration** tab.

Step 7 Configure the values for each probe.

Step 8 Click **Save** to save the probe configuration.

Setup CoA, SNMP RO Community, and Endpoint Attribute Filter

Cisco ISE allows a global configuration to issue a Change of Authorization (CoA) in the Profiler Configuration page that enables the profiling service with more control over endpoints that are already authenticated.

In addition, you can configure additional SNMP Read Only community strings separated by a comma for the NMAP manual network scan in the Profiler Configuration page. The SNMP RO community strings are used in the same order as they appear in the Current custom SNMP community strings field.

You can also configure endpoint attribute filtering in the Profiler Configuration page.

Step 1 Choose **Administration** > **System** > **Settings** > **Profiling**.

Step 2 Choose one of the following settings to configure the CoA type:

- **No CoA** (default)—You can use this option to disable the global configuration of CoA. This setting overrides any configured CoA per endpoint profiling policy. If the goal is only visibilibility, retain the default value as **No CoA**.
- **Port Bounce**—You can use this option, if the switch port exists with only one session. If the port exists with multiple sessions, then use the Reauth option. If the goal is to immediately update the access policy based on profile changes, select the **Port Bounce** option, this will ensure that any clientless endpoints is reauthorized, and IP address is refreshed, if required.

- **Reauth**—You can use this option to enforce reauthentication of an already authenticated endpoint when it is profiled. Select the **Reauth** option, if no VLAN or address change is expected following the reauthorization of the current session.

  Note If you have multiple active sessions on a single port, the profiling service issues a CoA with the **Reauth** option even though you have configured CoA with the **Port Bounce** option. This function avoids disconnecting other sessions, a situation that might occur with the **Port Bounce** option.

Step 3 Enter new SNMP community strings separated by a comma for the NMAP manual network scan in the **Change Custom SNMP Community Strings** field, and re-enter the strings in the **Confirm Custom SNMP Community Strings** field for confirmation.

The default SNMP community string used is *public*. Click **Show** in the **Current Custom SNMP Community Strings** section to verify this.

Step 4 Check the **Endpoint Attribute Filter** check box to enable endpoint attribute filtering.

On enabling the **EndPoint Attribute Filter**, the Cisco ISE profiler only keeps allowed attributes and discards all other attributes. For more information, see Global Setting to Filter Endpoint Attributes, on page 793 and Attribute Filters for ISE Database Persistence and Performance, on page 793 sections. As a best practice, we recommend you to enable **Endpoint Attribute Filter** in production deployments.

Step 5 Check the **Enable Probe Data Publisher** check box if you want Cisco ISE to publish endpoint probe data to pxGrid subscribers that need this data to classify endpoints onboarding on ISE. The pxGrid subscriber can pull the endpoint records from Cisco ISE using bulk download during initial deployment phase. Cisco ISE sends the endpoint records to the pxGrid subscriber whenever they are updated in PAN. This option is disabled by default.

When you enable this option, ensure that the pxGrid persona is enabled in your deployment.

Step 6 Click **Save**.

Global Configuration of Change of Authorization for Authenticated Endpoints

You can use the global configuration feature to disable change of authorization (CoA) by using the default No CoA option or enable CoA by using port bounce and reauthentication options. If you have configured Port Bounce for CoA in Cisco ISE, the profiling service may still issue other CoAs as described in the “CoA Exemptions” section.

The global configuration chosen dictates the default CoA behavior only in the absense of more specific settings. See Change of Authorization Configuration for Each Endpoint Profiling Policy, on page 820.

You can use the RADIUS probe or the Monitoring persona REST API to authenticate the endpoints. You can enable the RADIUS probe, which allows faster performance. If you have enabled CoA, then we recommend that you enable the RADIUS probe in conjunction with your CoA configuration in the Cisco ISE application for faster performance. The profiling service can then issue an appropriate CoA for endpoints by using the RADIUS attributes that are collected.

If you have disabled the RADIUS probe in the Cisco ISE application, then you can rely on the Monitoring persona REST API to issue CoAs. This allows the profiling service to support a wider range of endpoints. In a distributed deployment, your network must have at least one Cisco ISE node that assumes the Monitoring persona to rely on the Monitoring persona REST API to issue a CoA.

Cisco ISE arbitrarily will designate either the primary or secondary Monitoring node as the default destination for REST queries in your distributed deployment, because both the primary and secondary Monitoring nodes have identical session directory information.

Use Cases for Issuing Change of Authorization

The profiling service issues the change of authorization in the following cases:

- Endpoint deleted: When an endpoint is deleted from the Endpoints page and the endpoint is disconnected or removed from the network.
- An exception action is configured: If you have an exception action configured per profile that leads to an unusual or an unacceptable event from that endpoint. The profiling service moves the endpoint to the corresponding static profile by issuing a CoA.
- An endpoint is profiled for the first time: When an endpoint is not statically assigned and profiled for the first time; for example, the profile changes from an unknown to a known profile.
    - An endpoint identity group has changed: When an endpoint is added or removed from an endpoint identity group that is used by an authorization policy.

      The profiling service issues a CoA when there is any change in an endpoint identity group, and the endpoint identity group is used in the authorization policy for the following:

        - The endpoint identity group changes for endpoints when they are dynamically profiled
        - The endpoint identity group changes when the static assignment flag is set to true for a dynamic endpoint
- An endpoint profiling policy has changed and the policy is used in an authorization policy: When an endpoint profiling policy changes, and the policy is included in a logical profile that is used in an authorization policy. The endpoint profiling policy may change due to the profiling policy match or when an endpoint is statically assigned to an endpoint profiling policy, which is associated to a logical profile. In both the cases, the profiling service issues a CoA, only when the endpoint profiling policy is used in an authorization policy.

Exemptions for Issuing a Change of Authorization

The profiling service does not issue a CoA when there is a change in an endpoint identity group and the static assignment is already true.

Cisco ISE does not issue a CoA for the following reasons:

- An Endpoint disconnected from the network—When an endpoint disconnected from your network is discovered.
- Authenticated wired (Extensible Authentication Protocol) EAP-capable endpoint—When an authenticated wired EAP-capable endpoint is discovered.
- Multiple active sessions per port—When you have multiple active sessions on a single port, the profiling service issues a CoA with the Reauth option even though you have configured CoA with the Port Bounce option.

- Packet-of-Disconnect CoA (Terminate Session) when a wireless endpoint is detected—If an endpoint is discovered as wireless, then a Packet-of-Disconnect CoA (Terminate-Session) is issued instead of the Port Bounce CoA. The benefit of this change is to support the Wireless LAN Controller (WLC) CoA.
- Profiler CoA is suppressed when the **Suppress Profiler CoA for endpoints in Logical Profile** option is used for the configured logical profile in the Authorization Profile. Profiler CoA will be triggered for all other endpoints by default.
- Global No CoA Setting overrides Policy CoA—Global No CoA overrides all configuration settings in endpoint profiling policies as there is no CoA issued in Cisco ISE irrespective of CoA configured per endpoint profiling policy.

Note No CoA and Reauth CoA configurations are not affected, and the profiler service applies the same CoA configuration for wired and wireless endpoints.

Change of Authorization Issued for Each Type of CoA Configuration

Table 108: Change of Authorization Issued for Each Type of CoA Configuration

Scenarios	No CoA Configuration	Port Bounce Configuration	Reauth Configuration	Additional Information
Global CoA configuration in Cisco ISE (typical configuration)	No CoA	Port Bounce	Reauthentication	—
An endpoint is disconnected on your network	No CoA	No CoA	No CoA	Change of authorization is determined by the RADIUS attribute Acct-Status -Type value Stop.
Wired with multiple active sessions on the same switch port	No CoA	Reauthentication	Reauthentication	Reauthentication avoids disconnecting other sessions.
Wireless endpoint	No CoA	Packet-of-Disconnect CoA (Terminate Session)	Reauthentication	Support to Wireless LAN Controller.
Incomplete CoA data	No CoA	No CoA	No CoA	Due to missing RADIUS attributes.

Attribute Filters for ISE Database Persistence and Performance

Cisco ISE implements filters for Dynamic Host Configuration Protocol (both DHCP Helper and DHCP SPAN), HTTP, RADIUS, and Simple Network Management Protocol probes except for the NetFlow probe to address performance degradation. Each probe filter contains the list of attributes that are temporal and irrelevant for endpoint profiling and removes those attributes from the attributes collected by the probes.

The isebootstrap log (isebootstrap-yyyymmdd-xxxxxx.log) contains messages that handles the creation of dictionaries and with filtering of attributes from the dictionaries. You can also configure to log a debug message when endpoints go through the filtering phase to indicate that filtering has occurred.

The Cisco ISE profiler invokes the following endpoint attribute filters:

- A DHCP filter for both the DHCP Helper and DHCP SPAN contains all the attributes that are not necessary and they are removed after parsing DHCP packets. The attributes after filtering are merged with existing attributes in the endpoint cache for an endpoint.
- An HTTP filter is used for filtering attributes from HTTP packets, where there is no significant change in the set of attributes after filtering.
- A RADIUS filter is used once the syslog parsing is complete and endpoint attributes are merged into the endpoint cache for profiling.
- SNMP filter for SNMP Query includes separate CDP and LLDP filters, which are all used for SNMP-Query probe.

Global Setting to Filter Endpoint Attributes

You can reduce the number of persistence events and replication events by reducing the number of endpoint attributes that do not change frequently at the collection point. Enabling the **EndPoint Attribute Filter** will have the Cisco ISE profiler only to keep allowed attributes and discard all other attributes.

To enable the **Endpoint Attribute Filter**), see the Setup CoA, SNMP RO Community, and Endpoint Attribute Filter, on page 789 section.

An allowed list is a set of attributes that are used in custom endpoint profiling policies for profiling endpoints, and that are essential for Change of Authorization (CoA), Bring Your Own Device (BYOD), Device Registration WebAuth (DRW), and so on to function in Cisco ISE as expected. The allowed list is always used as a criteria when ownership changes for the endpoint (when attributes are collected by multiple Policy Service nodes) even when disabled.

By default, the allowed list is disabled and the attributes are dropped only when the attribute filter is enabled. The allowed list is dynamically updated when endpoint profiling policies change including from the feed to include new attributes in the profiling policies. Any attribute that is not present in the allowed list is dropped immediately at the time of collection, and the attribute is not used for profiling endpoints. When combined with the buffering, the number of persistence events can be reduced.

You must ensure that the allowed list contains a set of attributes determined from the following two sources:

- A set of attributes that are used in the default profiles so that you can match endpoints to the profiles.
- A set of attributes that are essential for Change of Authorization (CoA), Bring Your Own Device (BYOD), Device Registration WebAuth (DRW), and so on to function as expected.

Note To add an new attribute to the allowed list, the administrator needs to create a new profiler condiion and policy that uses the attribute. This new attribute will be automatically added to the allowed list of stored and replicated attributes.

Table 109: Allowed Attributes

AAA-Server	BYODRegistration
Calling-Station-ID	Certificate Expiration Date
Certificate Issue Date	Certificate Issuer Name
Certificate Serial Number	Description
DestinationIPAddress	Device Identifier
Device Name	DeviceRegistrationStatus
EndPointPolicy	EndPointPolicyID
EndPointProfilerServer	EndPointSource
FQDN	FirstCollection
Framed-IP-Address	IdentityGroup
IdentityGroupID	IdentityStoreGUID
IdentityStoreName	L4_DST_PORT
LastNmapScanTime	MACAddress
MatchedPolicy	MatchedPolicyID
NADAddress	NAS-IP-Address
NAS-Port-Id	NAS-Port-Type
NmapScanCount	NmapSubnetScanID
OS Version	OUI
PolicyVersion	PortalUser
PostureApplicable	Product
RegistrationTimeStamp	—
StaticAssignment	StaticGroupAssignment
TimeToProfile	Total Certainty Factor
User-Agent	cdpCacheAddress

cdpCacheCapabilities	cdpCacheDeviceId
cdpCachePlatform	cdpCacheVersion
ciaddr	dhcp-class-identifier
dhcp-requested-address	host-name
hrDeviceDescr	ifIndex
ip	lldpCacheCapabilities
lldpCapabilitiesMapSupported	lldpSystemDescription
operating-system	sysDescr
161-udp	—

Attributes Collection from Cisco IOS Sensor-Embedded Switches

An Cisco IOS sensor integration allows Cisco ISE run time and the Cisco ISE profiler to collect any or all of the attributes that are sent from the switch. You can collect DHCP, CDP, and LLDP attributes directly from the switch by using the RADIUS protocol. The attributes that are collected for DHCP, CDP, and LLDP are then parsed and mapped to attributes in the profiler dictionaries in the following location: **Policy** > **Policy Elements** > **Dictionaries**.

For information about the supported Catalyst platforms for Device sensors, see https://communities.cisco.com/docs/DOC-72932.

Cisco IOS Sensor-Embedded Network Access Devices

Integrating Cisco IOS sensor embedded network access devices with Cisco ISE involves the following components:

- A Cisco IOS sensor
- Data collector that is embedded in the network access device (switch) for gathering DHCP, CDP, and LLDP data
- Analyzers for processing the data and determining the device-type of endpoints

  There are two ways of deploying an analyzer, but they are not expected to be used in conjunction with each other:

  - An analyzer can be deployed in Cisco ISE
  - Analyzers can be embedded in the switch as the sensor

Configuration Checklist for Cisco IOS Sensor-Enabled Network Access Devices

This section summarizes a list of tasks that you must configure in the Cisco IOS sensor-enabled switches and Cisco ISE to collect DHCP, CDP, and LLDP attributes directly from the switch:

- Ensure that the RADIUS probe is enabled in Cisco ISE.
- Ensure that network access devices support an IOS sensor for collecting DHCP, CDP, and LLDP information.
- Ensure that network access devices run the following CDP and LLDP commands to capture CDP and LLDP information from endpoints:

  ```
  cdp enable
  lldp run
  ```

- Ensure that session accounting is enabled separately by using the standard AAA and RADIUS commands.

  For example, use the following commands:

  ```
  aaa new-model
  aaa accounting dot1x default start-stop group radius

  radius-server host <ip> auth-port <port> acct-port <port> key <shared-secret>
  radius-server vsa send accounting
  ```

- Ensure that you run IOS sensor-specific commands.
  - Enabling Accounting Augmentation

    You must enable the network access devices to add Cisco IOS sensor protocol data to the RADIUS accounting messages and to generate additional accounting events when it detects new sensor protocol data. This means that any RADIUS accounting message should include all CDP, LLDP, and DHCP attributes.

    Enter the following global command:

    device-sensor accounting

  - Disabling Accounting Augmentation

    To disable (accounting) network access devices and add Cisco IOS sensor protocol data to the RADIUS accounting messages for sessions that are hosted on a given port (if the accounting feature is globally enabled), enter the following command at the appropriate port:

    no device-sensor accounting

  - TLV Change Tracking

    By default, for each supported peer protocol, client notifications and accounting events are generated only when an incoming packet includes a type, length, and value (TLV) that has not been received previously in the context of a given session.

    You must enable client notifications and accounting events for all TLV changes where there are either new TLVs, or where previously received TLVs have different values. Enter the following command:

    device-sensor notify all-changes

- Be sure that you disable the Cisco IOS Device Classifier (local analyzer) in the network access devices.

Enter the following command:

```
no macro auto monitor
```

Note This command prevents network access devices from sending two identical RADIUS accounting messages per change.

Support for Cisco IND Controllers by ISE Profiler

Cisco ISE can profile and display the status of devices attached to a Cisco Industrial Network Device (IND). PxGrid connects Cisco ISE and the Cisco Industrial Network Director to communicate endpoint (IoT) data. pxGrid on Cisco ISE consumes Cisco IND events, and queries Cisco IND to update endpoint type.

Cisco ISE profiler has dictionary attributes for IoT devices. Choose **Policy** > **Policy Elements** > **Dictionaries**, and select *IOTASSET* from the list of System Dictionaries to see the dictionary attributes.

Guidelines and Recommendations

If you have several ISE nodes configured for profiling, we recommend that you enable pxGrid for Cisco IND on only one node.

Multiple Cisco IND devices can connect to a single ISE.

If the same endpoint is received from two or more publishers (Cisco IND), Cisco ISE only keeps the last publisher's data for that endpoint.

Cisco ISE gets Cisco IND data from the service names *com.cisco.endpoint.asset* and */topic/com.cisco.endpoint.asset*in pxGrid.

Cisco IND Profiling Process Flow

Cisco IND Asset discovery finds an IoT device and publishes the endpoint data for that device to pxGrid. Cisco ISE sees the event on pxGrid, and gets the endpoint data. Profiler policies in Cisco ISE assign the device data to attributes in the ISE profiler dictionary, and applies those attributes to the endpoint in Cisco ISE.

IoT endpoint data which does not meet the existing attributes in Cisco ISE are not saved. But you can create more attributes in Cisco ISE, and register them with Cisco IND.

Cisco ISE does a bulk download of endpoints when the connection to Cisco IND through pxGrid is first established. If there is a network failure, Cisco ISE does another bulk download of accumulated endpoint changes.

Configure Cisco ISE and Cisco IND for IND Profiling

Note You must install the Cisco ISE certificate in Cisco IND, and install the Cisco IND certificate in ISE, before you activate pxGrid in Cisco IND.

1. Choose **Administration** > **Deployment**. Edit the PSN that you plan to use as pxGrid consumer, and enable pxGrid. This PSN is the one that creates endpoints from pxGrid data published by Cisco IND and profiling.

2. Choose **Administration** > **pxGrid Services** to verify that pxGrid is running. Then click the **Certificates** tab, and fill in the certificate fields. Click **Create** to issue the certificate and download the certificate.

   - For **I want to**, select "**Generate a single certificate (without a certificate signing request), Common Name**, and enter a name for the Cisco IND you are connecting with.
   - For **Certificate Download Format**, choose `PKS12 format`.
   - For **Certificate Password**, create a password.

Note The ISE internal CA must be enabled. If your browser blocks popups, you won't be able to download the certificate. Unzip the certificate to make the PEM file available for the next step.

3. In Cisco IND, choose **Settings** > **pxGrid**, and click `Download .pem IND certificate`. Keep this window open.

4. In Cisco ISE, choose **Administration** > **pxGrid Services** > **All Clients**. When you see the Cisco IND pxGrid client, approve it.

5. In Cisco IND, move the slider to enable pxGrid. Another screen opens, where you define the location of the ISE node, the name of the certificate that you entered for this pxGrid server in ISE, and the password you provided. Click **Upload Certificate**, and locate the ISE pxGrid PEM file.

6. In ISE, choose **Administration** > **Certificates** > **Trusted Certificates**. Click **Import** and enter the path to the certificate you got from Cisco IND.

7. In Cisco IND, click **Activate**.

8. In Cisco ISE, choose **Adminstration > Deployment**. Select the PSN you are using for the Cisco IND connection, select the Profiling window, and enable the pxGrid probe.

9. The pxGrid connection between ISE and Cisco IND is now active. Verify that by displaying the IoT endpoints that Cisco IND has found.

Add an Attribute for IND Profiling

Cisco IND may return attributes that are not in the ISE dictionary. You can add more attributes to Cisco ISE, so you can more accurately profile that IoT device. To add a new attribute, you create a custom attribute in Cisco ISE, and send that attribute to Cisco IND over pxGrid.

1. Choose **Administration** > **Identity Management** > **Settings**, and select **Endpoint Custom Attributes**. Create an attribute endpoint attribute.

2. You can now use this attribute in a profiler policy to identify assets with the new attribute. Choose **Policy** > **Profiling**, and create a new profiler policy. In the **Rules** section, create a new rule. When you add an **attribute/value**, select the **CUSTOMATTRIBUTE** folder, and the custom attribute you created.

Cisco ISE Support for MUD

Manufacturer Usage Descriptor (MUD) is an IETF standard, which defines a way to on-board IoT devices. It provides seamless visibility and segmentation automation of IoT devices. MUD has been approved in IETF process, and released as RFC8520. For more information, see https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/.

Cisco ISE, Release 2.6 and later supports identification of IoT devices. Cisco ISE automatically creates profiling policies and Endpoint Identity Groups. MUD supports profiling IoT devices, creating profiling policies dynamically, and automating the entire process of creating policies and Endpoint Identity Groups. Administrators can use these profiling policies to create manually Authorization Policies and Profiles. IoT devices sending MUD URL in DHCP and LLDP packets are on board, using those profiles and policies.

Cisco ISE performs unsigned classification of IoT devices. Cisco ISE does not store the MUD attributes; the attributes are only used in the current session. In the **Context and Visibility > Endpoints** window, you can filter IoT devices by the **Endpoint Profile** field.

The following devices support sending MUD data to Cisco ISE:

- Cisco Catalyst 3850 Series Switches running Cisco IOS XE Version 16.9.1 & 16.9.2
- Cisco Catalyst Digital Building Series Switches running Cisco IOS Version 15.2(6)E2
- Cisco Industrial Ethernet 4000 Series Switches running Cisco IOS Version 15.2(6)E2
- Internet of Things (IoT) devices with embedded MUD functionality

Cisco ISE supports the following profiling protocols and profiling probes:

- LLDP and Radius - TLV 127
- DHCP - Option 161

Both fields can be sent to Cisco ISE by IOS Device Sensor.

Configuring ISE for MUD

1. Choose **Work Centers** > **Profiler** > **Profiler Settings** , and check the **Enable profiling for MUD** check box.
2. Add the Network Access Device that can send MUD URIs to ISE. To add network devices, choose **Administration** > **Network Resources** > **Network Devices**.
3. Verify that the MUD-URL connection is working.
    a. Choose **Context Visibility** > **Endpoints**, and find IoT endpoints that ISE successfully classified. You can filter IoT devices by the Endpoint profile name, which starts with **`IOT-MUD`**.
    b. Click the endpoint MAC address of one of the IoT devices, and select the attribute tag. Verify that there is a mud-url in the list of attributes.
    c. Choose **Policy** > **Profiling** and filter the list by selecting **`IOT Created`** for **System Type**.
4. Optionally configure debug logging for the new IoT devices.

  a. Choose **System** > **Logging** > **Debug Log Configuration**, and select the ISE node that has the MUD configuration.
  b. Select **Debug Log Configuration** in the left menu, and then select **profiler**.

As more IoT devices are classified, all devices of the same category or group with same MUD-URL are assigned to the same endpoint group. For example, if a Molex light connects, and is classified, a profiler group is created for that Molex light. As more Molex lights of the same type (with the same MUD-URL) are classified, they inherit the same classification or endpoint identity group.

Verify MUD Traffic Flow in ISE and the Switch

1. Before turning on the IoT device, either **connect port** or **unshut** the interface:
    a. Start packet capture at ISE.
    b. Start packet capture at switch ports.
2. View the following output on the switch:
    a. **show device-sensor cache all**
    b. **show access-session**
    c. **show radius statistics**
3. Turn on the IoT devices.
4. Repeat the following every minute:
    a. **show device-sensor cache all**
    b. **show access-session**
    c. **show radius statistics**
5. Wait for 3 to 5 minutes for all the devices show up on ISE.
6. Stop both the ISE and switch packet captures.
7. Repeat the following every minute:
    a. **show device-sensor cache all**
    b. **show access-session**
    c. **show radius statistics**

Profiler Conditions

Profiling conditions are policy elements and are similar to other conditions. However unlike authentication, authorization, and guest conditions, the profiling conditions can be based on a limited number of attributes. The Profiler Conditions page lists the attributes that are available in Cisco ISE and their description.

Profiler conditions can be one of the following:

- Cisco Provided: Cisco ISE includes predefined profiling conditions when deployed and they are identified as Cisco Provided in the Profiler Conditions window. You cannot delete Cisco Provided profiling conditions.

  You can also find Cisco Provided conditions in the System profiler dictionaries in the following location: **Policy** > **Policy Elements** > **Dictionaries** > **System**.

  For example, MAC dictionary. For some products, the OUI (Organizationally Unique Identifier) is an unique attribute that you can use it first for identifying the manufacturing organization of devices. It is a component of the device MAC address. The MAC dictionary contains the MACAddress and OUI attributes.

- Administrator Created: Profiler conditions that you create as an administrator of Cisco ISE or predefined profiling conditions that are duplicated are identified as Administrator Created. You can create a profiler condition of DHCP, MAC, SNMP, IP, RADIUS, NetFlow, CDP, LLDP, and NMAP types using the profiler dictionaries in the **Profiler Conditions** window.

Although, the recommended upper limit for the number of profiling policies is 1000, you can stretch up to 2000 profiling policies.

Profiling Network Scan Actions

An endpoint scan action is a configurable action that can be referred to in an endpoint profiling policy, and that is triggered when the conditions that are associated with the network scan action are met.

An endpoint scan is used to scan endpoints in order to limit resources usage in the Cisco ISE system. A network scan action scans a single endpoint, unlike resource-intensive network scans. It improves the overall classification of endpoints, and redefines an endpoint profile for an endpoint. Endpoint scans can be processed only one at a time.

You can associate a single network scan action to an endpoint profiling policy. Cisco ISE predefines three scanning types for a network scan action, which can include one or all three scanning types: for instance, an OS-scan, an SNMPPortsAndOS-scan, and a CommonPortsAndOS-scan. You cannot edit or delete OS-scan, SNMPPortsAndOS-scan, and CommonPortsAndOS-scans, which are predefined network scan actions in Cisco ISE. You can also create a new network scan action of your own.

Once an endpoint is appropriately profiled, the configured network scan action cannot be used against that endpoint. For example, scanning an Apple-Device allows you to classify the scanned endpoint to an Apple device. Once an OS-scan determines the operating system that an endpoint is running, it is no longer matched to an Apple-Device profile, but it is matched to an appropriate profile for an Apple device.

Create a New Network Scan Action

A network scan action that is associated with an endpoint profiling policy scans an endpoint for an operating system, Simple Network Management Protocol (SNMP) ports, and common ports. Cisco provides network scan actions for the most common NMAP scans, but you can also create one of your own.

When you create a new network scan, you define the type of information that the NMAP probe will scan for.

Before you begin

The Network Scan (NMAP) probe must be enabled before you can define a rule to trigger a network scan action. The procedure for that is described in Configure Probes for Each Cisco ISE Node.

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **Profiling** > **Network Scan (NMAP) Actions**. Alternatively, you can choose **Work Centers** > **Profiler** > **Policy Elements** > **NMAP Scan Actions**.

Step 2 Click **Add**.

Step 3 Enter a name and description for the network scan action that you want to create.

Step 4 Check one or more check boxes when you want to scan an endpoint for the following:

- Scan OS: To scan for an operating system
- Scan SNMP Port: To scan SNMP ports (161, 162)
- Scan Common Port: To scan common ports.
- Scan Custom Ports: To scan custom ports.
- Scan Include Service Version Information: To scan the version information, which may contain detailed description of the device.
- Run SMB Discovery Script: To scan SMB ports (445 and 139) to retrieve information such as the OS and computer name.
- Skip NMAP Host Discovery: To skip the initial host discovery stage of the NMAP scan.

Note The Skip NMAP Host Discovery option is selected by default for automatic NMAP scan, however, you must select it to run manual NMAP scan.

Step 5 Click **Submit**.

NMAP Operating System Scan

The operating system scan (OS-scan) type scans for an operating system (and OS version) that an endpoint is running. This is a resource intensive scan.

The NMAP tool has limitations on OS-scan which may cause unreliable results. For example, when scanning an operating system of network devices such as switches and routers, the NMAP OS-scan may provide an incorrect operating-system attribute for those devices. Cisco ISE displays the operating-system attribute, even if the accuracy is not 100%.

You should configure endpoint profiling policies that use the NMAP operating-system attribute in their rules to have low certainty value conditions (Certainty Factor values). We recommend that whenever you create an endpoint profiling policy based on the NMAP:operating-system attribute, include an AND condition to help filter out false results from NMAP.

The following NMAP command scans the operating system when you associate Scan OS with an endpoint profiling policy:

```
nmap -sS -O -F -oN /opt/CSCOcpm/logs/nmap.log -append-output -oX - <IP-address>
```

The following NMAP command scans a subnet and sends the output to nmapSubnet.log:

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log
    --append-output -oX - <subnet>
```

Table 110: NMAP Commands for a Manual Subnet Scan

-O	Enables OS detection
-sU	UDP scan
-p <port ranges>	Scans only specified ports. For example, U:161, 162
oN	Normal output
oX	XML output

Operating System Ports

The following table lists the TCP ports that NMAP uses for OS scanning. In addition, NMAP uses ICMP and UDP port 51824.

1	3	4	6	7	9	13	17	19
20	21	22	23	24	25	26	30	32
33	37	42	43	49	53	70	79	80
81	82	83	84	85	88	89	90	99
100	106	109	110	111	113	119	125	135
139	143	144	146	161	163	179	199	211
212	222	254	255	256	259	264	280	301
306	311	340	366	389	406	407	416	417
425	427	443	444	445	458	464	465	481
497	500	512	513	514	515	524	541	543
544	545	548	554	555	563	587	593	616
617	625	631	636	646	648	666	667	668
683	687	691	700	705	711	714	720	722
726	749	765	777	783	787	800	801	808
843	873	880	888	898	900	901	902	903
911	912	981	987	990	992	993	995	999
1000	1001	1002	1007	1009	1010	1011	1021	1022
1023	1024	1025	1026	1027	1028	1029	1030	1031
1032	1033	1034	1035	1036	1037	1038	1039	1040-1100
1102	1104	1105	1106	1107	1108	1110	1111	1112

1113	1114	1117	1119	1121	1122	1123	1124	1126
1130	1131	1132	1137	1138	1141	1145	1147	1148
1149	1151	1152	1154	1163	1164	1165	1166	1169
1174	1175	1183	1185	1186	1187	1192	1198	1199
1201	1213	1216	1217	1218	1233	1234	1236	1244
1247	1248	1259	1271	1272	1277	1287	1296	1300
1301	1309	1310	1311	1322	1328	1334	1352	1417
1433	1434	1443	1455	1461	1494	1500	1501	1503
1521	1524	1533	1556	1580	1583	1594	1600	1641
1658	1666	1687	1688	1700	1717	1718	1719	1720
1721	1723	1755	1761	1782	1783	1801	1805	1812
1839	1840	1862	1863	1864	1875	1900	1914	1935
1947	1971	1972	1974	1984	1998-2010	2013	2020	2021
2022	2030	2033	2034	2035	2038	2040-2043	2045-2049	2065
2068	2099	2100	2103	2105-2107	2111	2119	2121	2126
2135	2144	2160	2161	2170	2179	2190	2191	2196
2200	2222	2251	2260	2288	2301	2323	2366	2381-2383
2393	2394	2399	2401	2492	2500	2522	2525	2557
2601	2602	2604	2605	2607	2608	2638	2701	2702
2710	2717	2718	2725	2800	2809	2811	2869	2875
2909	2910	2920	2967	2968	2998	3000	3001	3003
3005	3006	3007	3011	3013	3017	3030	3031	3052
3071	3077	3128	3168	3211	3221	3260	3261	3268
3269	3283	3300	3301	3306	3322	3323	3324	3325
3333	3351	3367	3369	3370	3371	3372	3389	3390
3404	3476	3493	3517	3527	3546	3551	3580	3659
3689	3690	3703	3737	3766	3784	3800	3801	3809
3814	3826	3827	3828	3851	3869	3871	3878	3880
3889	3905	3914	3918	3920	3945	3971	3986	3995

3998	4000-4006	4045	4111	4125	4126	4129	4224	4242
4279	4321	4343	4443	4444	4445	4446	4449	4550
4567	4662	4848	4899	4900	4998	5000-5004	5009	5030
5033	5050	5051	5054	5060	5061	5080	5087	5100
5101	5102	5120	5190	5200	5214	5221	5222	5225
5226	5269	5280	5298	5357	5405	5414	5431	5432
5440	5500	5510	5544	5550	5555	5560	5566	5631
5633	5666	5678	5679	5718	5730	5800	5801	5802
5810	5811	5815	5822	5825	5850	5859	5862	5877
5900-5907	5910	5911	5915	5922	5925	5950	5952	5959
5960-5963	5987-5989	5998-6007	6009	6025	6059	6100	6101	6106
6112	6123	6129	6156	6346	6389	6502	6510	6543
6547	6565-6567	6580	6646	6666	6667	6668	6669	6689
6692	6699	6779	6788	6789	6792	6839	6881	6901
6969	7000	7001	7002	7004	7007	7019	7025	7070
7100	7103	7106	7200	7201	7402	7435	7443	7496
7512	7625	7627	7676	7741	7777	7778	7800	7911
7920	7921	7937	7938	7999	8000	8001	8002	8007
8008	8009	8010	8011	8021	8022	8031	8042	8045
8080-8090	8093	8099	8100	8180	8181	8192	8193	8194
8200	8222	8254	8290	8291	8292	8300	8333	8383
8400	8402	8443	8500	8600	8649	8651	8652	8654
8701	8800	8873	8888	8899	8994	9000	9001	9002
9003	9009	9010	9011	9040	9050	9071	9080	9081
9090	9091	9099	9100	9101	9102	9103	9110	9111
9200	9207	9220	9290	9415	9418	9485	9500	9502
9503	9535	9575	9593	9594	9595	9618	9666	9876
9877	9878	9898	9900	9917	9929	9943	9944	9968
9998	9999	10000	10001	10002	10003	10004	10009	10010

10012	10024	10025	10082	10180	10215	10243	10566	10616
10617	10621	10626	10628	10629	10778	11110	11111	11967
12000	12174	12265	12345	13456	13722	13782	13783	14000
14238	14441	14442	15000	15002	15003	15004	15660	15742
16000	16001	16012	16016	16018	16080	16113	16992	16993
17877	17988	18040	18101	18988	19101	19283	19315	19350
19780	19801	19842	20000	20005	20031	20221	20222	20828
21571	22939	23502	24444	24800	25734	25735	26214	27000
27352	27353	27355	27356	27715	28201	30000	30718	30951
31038	31337	32768	32769	32770	32771	32772	32773	32774
32775	32776	32777	32778	32779	32780	32781	32782	32783
32784	32785	33354	33899	34571	34572	34573	34601	35500
36869	38292	40193	40911	41511	42510	44176	44442	44443
44501	45100	48080	49152	49153	49154	49155	49156	49157
49158	49159	49160	49161	49163	49165	49167	49175	49176
49400	49999	50000	50001	50002	50003	50006	50300	50389
50500	50636	50800	51103	51493	52673	52822	52848	52869
54045	54328	55055	55056	55555	55600	56737	56738	57294
57797	58080	60020	60443	61532	61900	62078	63331	64623
64680	65000	65129	65389					

NMAP SNMP Port Scan

The SNMPPortsAndOS-scan type scans an operating system (and OS version) that an endpoint is running and triggers an SNMP Query when SNMP ports (161 and 162) are open. It can be used for endpoints that are identified and matched initially with an Unknown profile for better classification.

The following NMAP command scans SNMP ports (UDP 161 and 162) when you associate the Scan SNMP Port with an endpoint profiling policy:

```
nmap -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP-address>
```

Table 111: NMAP Commands for an Endpoint SNMP Port Scan

-sU	UDP scan.
-p <port-ranges>	Scans only specified ports. For example, scans UDP ports 161 and 16.2

oN	Normal output.
oX	XML output.
IP-address	IP-address of an endpoint that is scanned.

NMAP Common Ports Scan

The CommonPortsAndOS-scan type scans an operating system (and OS version) that an endpoint is running and common ports (TCP and UDP), but not SNMP ports. The following NMAP command scans common ports when you associate Scan Common Port with an endpoint profiling policy:nmap -sTU -p T:21,22,23,25,53,80,110,135,139,143,443,445,3306,3389,8080,U:53,67,68,123,135,137,138,139,161,445,500,520,631,1434,1900 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP address>

Table 112: NMAP Commands for an Endpoint Common Ports Scan

-sTU	Both TCP connect scan and UDP scan.
-p <port ranges>	Scans TCP ports: 21,22,23,25,53,80,110,135,139,143, 443,445,3306,3389,8080 and UDP ports: 53,67,68,123,135,137, 138,139,161,445,500,520,631,1434,1900
oN	Normal output.
oX	XML output.
IP address	IP address of an endpoint that is scanned.

Common Ports

The following table lists the common ports that NMAP uses for scanning.

Table 113: Common Ports

TCP Ports		**UDP Ports**	
Ports	**Service**	**Ports**	**Service**
21/tcp	ftp	53/udp	domain
22/tcp	ssh	67/udp	dhcps
23/tcp	telnet	68/udp	dhcpc
25/tcp	smtp	123/udp	ntp
53/tcp	domain	135/udp	msrpc
80/tcp	http	137/udp	netbios-ns
110/tcp	pop3	138/udp	netbios-dgm
135/tcp	msrpc	139/udp	netbios-ssn
139/tcp	netbios-ssn	161/udp	snmp
143/tcp	imap	445/udp	microsoft-ds
443/tcp	https	500/udp	isakmp
445/tcp	microsoft-ds	520/udp	route

TCP Ports		**UDP Ports**	
Ports	**Service**	**Ports**	**Service**
3389/tcp	ms-term-serv	1434/udp	ms-sql-m
8080/tcp	http-proxy	1900/udp	upnp

NMAP Custom Ports Scan

In addition to the common ports, you can use custom ports (**Work Centers** > **Profiler** > **Policy Elements** > **NMAP Scan Actions** or **Policy** > **Policy Elements** > **Results** > **Profiling** > **Network Scan (NMAP) Actions**) to specify automatic and manual NMAP scan actions. NMAP probes collect the attributes from endpoints via the specified custom ports that are open. These attributes are updated in the endpoint's attribute list in the ISE Identities page (**Work Centers** > **Network Access** > **Identities** > **Endpoints**). You can specify up to 10 UDP and 10 TCP ports for each scan action. You cannot use the same port numbers that you have specified as common ports. See Configure Profiler Policies Using the McAfee ePolicy Orchestrator for more information.

NMAP Include Service Version Information Scan

The Include Service Version Information NMAP probe automatically scans the endpoints to better classify them, by collecting information about services running on the device. The service version option can be combined with common ports or custom ports.

Example:

CLI Command: nmap -sV -p T:8083 172.21.75.217

Output:

Port	**State**	**Service**	**Version**
8083/tcp	open	http	McAfee ePolicy Orchestrator Agent 4.8.0.1500 (ePOServerName: WIN2008EPO, AgentGuid: {1F5ED719-0A22-4F3B-BABA-00FAE756C2FE})

NMAP SMB Discovery Scan

NMAP SMB Discovery scan helps differentiate the Windows versions, and results in a better endpoint profiling. You can configure the NMAP scan action to run the SMB discovery script that is provided by NMAP.

The NMAP scan action is incorporated within the windows default policies and when the endpoint matches the policy and the scanning rule, the endpoint is scanned and the result helps to determine the exact windows version. The policy will be then configured on the feed service and new pre-defined NMAP scan is created with the SMB discovery option.

The NMAP scan action is invoked by the Microsoft-Workstation policies and the result of the scan is saved on the endpoint under the operating system attribute and leveraged to the Windows policies. You can also find the SMB Discovery script option in the manual scan on the subnet.

Note For SMB discovery, be sure to enable the Windows file sharing option in the endpoint.

SMB Discovery Attributes

When the SMB discovery script is executed on the endpoint, new SMB discovery attributes, such as SMB.Operating-system, are added to the endpoint. These attributes are considered for updating the Windows endpoint profiling policies on the feed service. When a SMB discovery script is run, the SMB discovery attribute is prefixed with SMB, such as SMB.operating-system, SMB.lanmanager, SMB.server, SMB.fqdn, SMB.domain, SMB.workgroup, and SMB.cpe.

Skip NMAP Host Discovery

Scanning every port of every single IP address is a time-consuming process. Depending on the purpose of the scan, you can skip the NMAP host discovery of active endpoints.

If a NMAP scan is triggered after the classification of an endpoint, the profiler always skips the host discovery of the endpoint. However, if a manual scan action is triggered after enabling the Skip NMAP Host Discovery Scan, then host discovery is skipped.

NMAP Scan Workflow

Steps to be followed to perform a NMAP scan:

Before you begin

In order to run NMAP SMB discovery script, you must enable the file sharing in your system. Refer to the Enable File Sharing to Run NMAP SMB Discovery Script topic for an example.

Step 1 Create an SMB Scan Action.

Step 2 Configure the Profiler Policy Using the SMB Scan Action.

Step 3 Add a New Condition Using the SMB Attribute.

Create an SMB Scan Action

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Profiling** > **Network Scan (NMAP) Actions**.

Step 2 Enter the **Action Name** and **Description**.

Step 3 Check the **Run SMB Discovery Script** checkbox.

Step 4 Click **Add** to create the network access users.

What to do next

You should configure the profiler policy using the SMB scan action.

Configure the Profiler Policy Using the SMB Scan Action

Before you begin

You must create a new profiler policy to scan an endpoint with the SMB scan action. For example, you can scan a Microsoft Workstation by specifying a rule that if the DHCP class identifier contains the MSFT attribute, then a network action should be taken.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Profiling** > **Add**.

Step 2 Enter the **Name** and **Description**.

Step 3 In the drop-down, select the scan action (for example, SMBScanAction) that you had created.

What to do next

You should add a new condition using the SMB attribute.

Add a New Condition Using the SMB Attribute

Before you begin

You should create a new profiler policy to scan the version of an endpoint. For example, you can scan for Windows 7 under the Microsoft Workstation parent policy.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Profiling** > **Add**.

Step 2 Enter the **Name** (for example, Windows-7Workstation) and **Description**.

Step 3 In the **Network Scan (NMAP) Action** drop-down, select **None**.

Step 4 In the **Parent Policy** drop-down choose the Microsoft-Workstation policy.

Enable File Sharing to Run NMAP SMB Discovery Script

Given below is an example to enable file sharing in Windows OS version 7, to run the NMAP SMB discovery script.

Step 1 Choose **Control Panel** > **Network and Internet**.

Step 2 Click **Network and Sharing Center**.

Step 3 Click **Change Advanced Sharing Settings**.

Step 4 Click **Turn on File and Printer Sharing**.

Step 5 Enable the following options: **Enable File Sharing for Devices That Use 40- or 56-bit Encryption** and **Turn on Password Protected Sharing**.

Step 6 Click **Save Changes**.

Step 7 Configure the Firewall settings.

a) In the Control Panel, navigate to **System and Security** > **Windows Firewall** > **Allow a Program Through Windows Firewall**.

b) Check the **File and Printer Sharing** check box.
c) Click **OK**.

Step 8 Configure the shared folder.

a) Right-click the destination folder, and select **Properties**.
b) Click the **Sharing** tab, and click **Share**.
c) In the **File Sharing** dialog box, add the required names and click **Share**.
d) Click **Done** after the selected folder is shared.
e) Click **Advanced Sharing** and select the **Share This Folder** check box.
f) Click **Permissions**.
g) In the **Permissions for Scans** dialog box, choose **Everyone** and check the **Full Control** check box.
h) Click **OK**.

Exclude Subnets from NMAP Scan

You can perform an NMAP scan to identify an endpoint's OS or SNMP port.

When performing the NMAP scan, you can exclude a whole subnet or IP range that should not be scanned by NMAP. You can configure the subnet or IP range in the **NMAP Scan Subnet Exclusions** window (**Work Centers > Profiler > Settings > NMAP Scan Subnet Exclusions**). This helps limit the load on your network and saves a considerable amount of time.

For Manual NMAP scan, you can use the **Run Manual NMAP Scan** window (**Work Centers > Profiler > Manual Scans > Manual NMAP Scan > Configure NMAP Scan Subnet Exclusions At**) to specify the subnet or IP range.

Manual NMAP Scan Settings

You can perform a manual NMAP scan (**Work Centers** > **Profiler** > **Manual Scans** > **Manual NMAP Scan**) using the scan options that are available for automatic NMAP scan. You can choose either the scan options or the predefined ones.

Table 114: Manual NMAP Scan Settings

Field Name	Usage Guidelines
Node	Choose the ISE node from which the NMAP scan is run.
Manual Scan Subnet	Enter the range of subnet IP addresses of endpoints for which you want to run the NMAP scan.
Configure NMAP Scan Subnet Exclusions At	You will be directed to the **Work Centers** > **Profiler** > **Settings** > **NMAP Scan Subnet Exclusions** window. Specify the IP address and subnet mask that should be excluded. If there is a match, the NMAP scan is not run.
NMAP Scan Subnet	You can do one of the following: • Specify Scan Options • Select an Existing NMAP Scan

Field Name	Usage Guidelines
Specify Scan Options	Select the required scan options: OS, SNMP Port, Common Ports, Custom Ports, Include Service Version Information, Run SMB Discovery Script, Skip NMAP Host Discovery. See Create a New Network Scan Action for more information.
Select an Existing NMAP Scan	Displays the **Existing NMAP Scan Actions** drop-down list that displays the default profiler NMAP scan actions.
Reset to Default Scan Options	Click this option to restore default settings (all scan options are checked).
Save as NMAP Scan Action	Enter an action name and a description.

Run a Manual NMAP Scan

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Profiler** > **Manual Scans** > **Manual NMAP Scan**.

Step 2 In the **Node** drop-down list, select the ISE node from which you intend to run the NMAP scan.

Step 3 In the **Manual Scan Subnet** text box, enter the subnet address whose endpoints you intend to check for open ports.

Step 4 Select one of the following:

a) Choose **Specify Scan Options**, and on the right side of the page, choose the required scan options. Refer to the Create a New Network Scan Action page for more information.

b) Choose **Select An Existing NMAP Scan Action** to select the default NMAP scan action, such as MCAFeeEPOOrchestratorClientScan.

Step 5 Click **Run Scan**.

Configure Profiler Policies Using the McAfee ePolicy Orchestrator

Cisco ISE profiling services can detect if the McAfee ePolicy Orchestrator (McAfee ePO) client is present on the endpoint. This helps in determining if a given endpoint belongs to your organization.

The entities involved in the process are:

- ISE Server
- McAfee ePO Server
- McAfee ePO Agent

Cisco ISE provides an in-built NMAP scan action (MCAFeeEPOOrchestratorClientscan) to check if the McAfee agent is running on an endpoint using NMAP McAfee script on the configured port. You can also create new NMAP scan options using the custom ports (for example, 8082). You can configure a new NMAP scan action using the McAfee ePO software by following the steps below:

Step 1 Configure the McAfee ePo NMAP Scan Action.

Step 2 Configure the McAfee ePO Agent.

Step 3 Configure Profiler Policies Using the McAfee ePO NMAP Scan Action.

Configure the McAfee ePo NMAP Scan Action

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Profiler** > **Policy Elements** > **Network Scan (NMAP) Actions**.

Step 2 Click **Add**.

Step 3 Enter the **Action Name** and **Description**.

Step 4 In the **Scan Options**, select **Custom Ports**.

Step 5 In the **Custom Ports** dialog box, add the required TCP port. The 8080 TCP port is enabled by default for McAfee ePO.

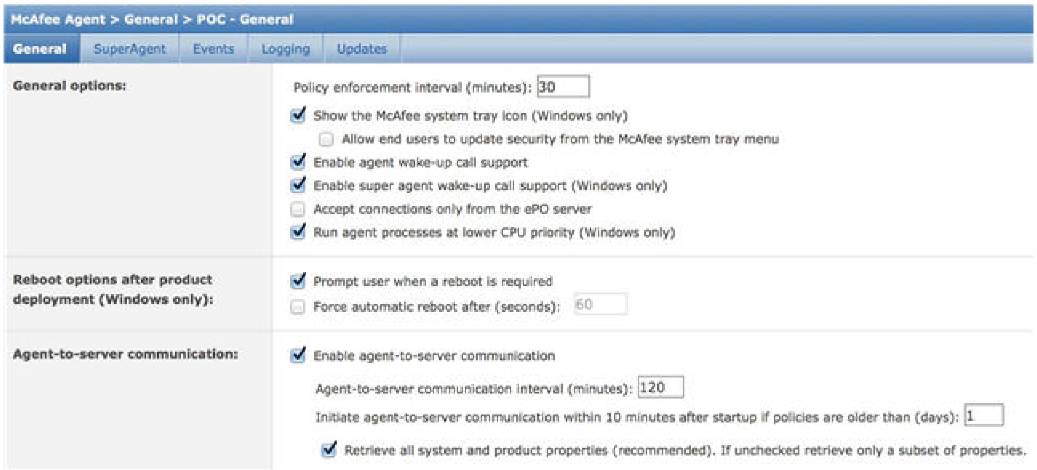
Step 6 Check the **Include Service Version Information** checkbox.

Step 7 Click **Submit**.

Configure the McAfee ePO Agent

Step 1 In your McAfee ePO server, check the recommended settings to facilitate the communication between the McAfee ePO agent and the ISE server.

Figure 26: McAfee ePO Agent Recommended Options



General options:

Policy enforcement interval (minutes): 30

☑ Show the McAfee system tray icon (Windows only)

  ☐ Allow end users to update security from the McAfee system tray menu

☑ Enable agent wake-up call support

☑ Enable super agent wake-up call support (Windows only)

☐ Accept connections only from the ePO server

☑ Run agent processes at lower CPU priority (Windows only)

Reboot options after product deployment (Windows only):

☑ Prompt user when a reboot is required

☐ Force automatic reboot after (seconds): 60

Agent-to-server communication:

☑ Enable agent-to-server communication

Agent-to-server communication interval (minutes): 120

Initiate agent-to-server communication within 10 minutes after startup if policies are older than (days): 1

☑ Retrieve all system and product properties (recommended). If unchecked retrieve only a subset of properties.

Step 2 Verify that the **Accept Connections Only From The ePO Server** is unchecked.

Configure Profiler Policies Using the McAfee ePO NMAP Scan Action

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Profiling** > **Add**.

Step 2 Enter the **Name** and **Description**.

Step 3 In the **Network Scan (NMAP) Action** drop-down list, select the required action (for example, MCAFeeEPOOrchestratorClientscan).

Step 4 Create the parent profiler policy (for example, Microsoft-Workstation containing a rule to check if the DHCP class identifier contains the MSFT attribute).

Step 5 Create a new policy (for example CorporateDevice) within the parent NMAP McAfee ePO policy (for example, Microsoft-Workstation) to check if the McAfee ePO agent is installed on the endpoint.

Endpoints that meet the condition are profiled as corporate devices. You can use the policy to move endpoints profiled with McAfee ePO agent to a new VLAN.

Profiler Endpoint Custom Attributes

Choose **Administration** > **Identity Management** > **Settings** > **Endpoint Custom Attributes** to assign attributes to endpoints, besides the attributes that the endpoint gathers from the probe. The endpoint custom attributes can be used in authorization policies to profile endpoints.

You can create a maximum of 100 endpoint custom attributes. The types of endpoint custom attributes supported are: Int, String, Long, Boolean, and Float.

You can add values for the endpoint custom attributes in the **Context Directory** > **Endpoints** > **Endpoint Classification** window.

Use cases for endpoint custom attributes include, to allow or block devices based on certain attributes or to assign certain privileges based on the authorization.

Using Endpoint Custom Attributes in Authorization Policy

The endpoint custom attributes section allows you to configure extra attributes. Each definition consists of the attribute and type (String, Int, Boolean, Float, Long). You can profile devices using endpoint custom attributes.

Note You must have a Cisco ISE Advantage license to add custom attributes to the endpoints.

The following steps show how to create an authorization policy using endpoint custom attributes.

Step 1 Create the endpoint custom attributes and assign values.

a) Choose **Administration** > **Identity Management** > **Settings** > **Endpoint Custom Attributes** page.
b) In the **Endpoint Custom Attributes** area, enter the **Attribute Name** (for example, deviceType), Data Type (for example, String) and Parameters.
c) Click **Save**.
d) Choose **Context Visibility** > **Endpoints** > **Summary**.
e) Assign the custom attribute values.
    - Check the required MAC address check box, and click **Edit**.
    - Or, click the required MAC address, and on the Endpoints page, click **Edit**.
f) In the **Edit Endpoint** dialog box, in the **Custom Attribute** area enter the required attribute values (for example, deviceType = Apple-iPhone).
g) Click **Save**.

Step 2 Create an authorization policy using the custom attributes and values.

a) Choose **Policy** > **Policy Sets**.

b) Create the authorization policy by selecting the custom attributes from the Endpoints dictionary (for example, Rule Name: Corporate Devices, Conditions:EndPoints:deviceType Contains Apple-iPhone, Permissions: then PermitAccess).

c) Click **Save**.

Related Topics

Profiler Endpoint Custom Attributes, on page 814

Create a Profiler Condition

Endpoint profiling policies in Cisco ISE allow you to categorize discovered endpoints on your network, and assign them to specific endpoint identity groups. These endpoint profiling policies are made up of profiling conditions that Cisco ISE evaluates to categorize and group endpoints.

Before you begin

To perform the following task, you must be a Super Admin or Policy Admin.

Step 1 Choose **Policy** > **Policy Elements** > **Conditions** > **Profiling** > **Add**.

Step 2 Enter values for the fields as described in the Endpoint Profiling Policies Settings, on page 816.

Step 3 Click **Submit** to save the profiler condition.

Step 4 Repeat this procedure to create more conditions.

Endpoint Profiling Policy Rules

You can define a rule that allows you to choose one or more profiling conditions from the library that are previously created and saved in the policy elements library, and to associate an integer value for the certainty factor for each condition, or associate either an exception action or a network scan action for that condition. The exception action or the network scan action is used to trigger the configurable action while Cisco ISE is evaluating the profiling policies with respect to the overall classification of endpoints.

When the rules in a given policy are evaluated separately with an OR operator, the certainty metric for each rule contributes to the overall matching of the endpoint profiles into a specific category of endpoints. If the rules of an endpoint profiling policy match, then the profiling policy and the matched policy are the same for that endpoint when they are dynamically discovered on your network.

Logically Grouped Conditions in Rules

An endpoint profiling policy (profile) contains a single condition or a combination of multiple single conditions that are logically combined using an AND or OR operator, against which you can check, categorize, and group endpoints for a given rule in a policy.

A condition is used to check the collected endpoint attribute value against the value specified in the condition for an endpoint. If you map more than one attribute, you can logically group the conditions, which helps you to categorize endpoints on your network. You can check endpoints against one or more such conditions with a corresponding certainty metric (an integer value that you define) associated with it in a rule or trigger an exception action that is associated to the condition or a network scan action that is associated to the condition.

Certainty Factor

The minimum certainty metric in the profiling policy evaluates the matching profile for an endpoint. Each rule in an endpoint profiling policy has a minimum certainty metric (an integer value) associated to the profiling conditions. The certainty metric is a measure that is added for all the valid rules in an endpoint profiling policy, which measures how each condition in an endpoint profiling policy contributes to improve the overall classification of endpoints.

The certainty metric for each rule contributes to the overall matching of the endpoint profiles into a specific category of endpoints. The certainty metric for all the valid rules are added together to form the matching certainty. It must exceed the minimum certainty factor that is defined in an endpoint profiling policy. By default, the minimum certainty factor for all new profiling policy rules and predefined profiling policies is 10.

Endpoint Profiling Policies Settings

The following table describes the fields in the **Endpoint Policies** window. To view this window, click the **Menu** icon (☰) and choose **Policy** > **Profiling** > **Profiling Policies**.

Table 115: Endpoint Profiling Policies Settings

Field Name	Usage Guidelines
Name	Enter the name of the endpoint profiling policy that you want to create.
Description	Enter the description of the endpoint profiling policy that you want to create.
Policy Enabled	By default, the **Policy Enabled** check box is checked to associate a matching profiling policy when you profile an endpoint. When unchecked, the endpoint profiling policy is excluded when you profile an endpoint.
Minimum Certainty Factor	Enter the minimum value that you want to associate with the profiling policy. The default value is 10.
Exception Action	Choose an exception action, which you want to associate with the conditions when defining a rule in the profiling policy. The default is NONE. The exception actions are defined in the following location: **Policy** > **Policy Elements** > **Results** > **Profiling** > **Exception Actions**.
Network Scan (NMAP) Action	Choose a network scan action from the list, which you want to associate with the conditions when defining a rule in the profiling policy, if required. The default is NONE. The exception actions are defined in the following location: **Policy** > **Policy Elements** > **Results** > **Profiling** > **Network Scan (NMAP) Actions**.

Field Name	Usage Guidelines
Create an Identity Group for the policy	Check one of the following options to create an endpoint identity group: • **Yes, create matching Identity Group** • **No, use existing Identity Group hierarchy**
Yes, create matching Identity Group	Choose this option to use an existing profiling policy. This option creates a matching identity group for those endpoints and the identity group will be the child of the Profiled endpoint identity group when an endpoint profile matches an existing profiling policy. For example, the Xerox-Device endpoint identity group is created in the Endpoints Identity Groups page when endpoints discovered on your network match the Xerox-Device profile.
No, use existing Identity Group hierarchy	Check this check box to assign endpoints to the matching parent endpoint identity group using hierarchical construction of profiling policies and identity groups. This option allows you to make use of the endpoint profiling policies hierarchy to assign endpoints to one of the matching parent endpoint identity groups, as well as to the associated endpoint identity groups to the parent identity group. For example, endpoints that match an existing profile are grouped under the appropriate parent endpoint identity group. Here, endpoints that match the Unknown profile are grouped under Unknown, and endpoints that match an existing profile are grouped under the Profiled endpoint identity group. For example, • If endpoints match the Cisco-IP-Phone profile, then they are grouped under the Cisco-IP-Phone endpoint identity group. • If endpoints match the Workstation profile, then they are grouped under the Workstation endpoint identity group. The Cisco-IP-Phone and Workstation endpoint identity groups are associated to the Profiled endpoint identity group in the system.
Parent Policy	Choose a parent profiling policy that are defined in the system to which you want to associate the new endpoint profiling policy. You can choose a parent profiling policy from which you can inherit rules and conditions to its child.
Associated CoA Type	Choose one of the following CoA types that you want to associate with the endpoint profiling policy: • No CoA • Port Bounce • Reauth • Global Settings that is applied from the profiler configuration set in Administration > System > Settings > Profiling

Field Name	Usage Guidelines
Rules	One or more rules that are defined in endpoint profiling policies determine the matching profiling policy for endpoints, which allows you to group endpoints according to their profiles. One or more profiling conditions from the policy elements library are used in rules for validating endpoint attributes and their values for the overall classification.
Conditions	Click the plus [+] sign to expand the Conditions anchored overlay, and click the minus [-] sign, or click outside the anchored overlay to close it. Click **Select Existing Condition from Library** or **Create New Condition (Advanced Option)** . **Select Existing Condition from Library**: You can define an expression by selecting Cisco predefined conditions from the policy elements library. **Create New Condition (Advanced Option)**: You can define an expression by selecting attributes from various system or user-defined dictionaries. You can associate one of the following with the profiling conditions: • An integer value for the certainty factor for each condition • Either an exception action or a network scan action for that condition Choose one of the following predefined settings to associate with the profiling condition: • Certainty Factor Increases: Enter the certainty value for each rule, which can be added for all the matching rules with respect to the overall classification. • Take Exception Action: Triggers an exception action that is configured in the Exception Action field for this endpoint profiling policy. • Take Network Scan Action: Triggers a network scan action that is configured in the Network Scan (NMAP) Action field for this endpoint profiling policy.

Select Existing Condition from Library	You can do the following:
	• You can choose Cisco predefined conditions that are available in the policy elements library, and then use an AND or OR operator to add multiple conditions.
	• Click the Action icon to do the following in the subsequent steps:
	    • **Add Attribute or Value**: You can add ad-hoc attribute or value pairs
	    • **Add Condition from Library**: You can add Cisco predefined conditions
	    • **Duplicate**: Create a copy of the selected condition
	    • **Add Condition to Library**: You can save ad-hoc attribute/value pairs that you create to the policy elements library
	    • **Delete**: Delete the selected condition.

Field Name	Usage Guidelines

Create New Condition (Advance Option)	You can do the following:
	• You can add ad-hoc attribute/value pairs to your expression, and then use an AND or OR operator to add multiple conditions.
	• Click the Action icon to do the following in the subsequent steps:
	  • **Add Attribute or Value**: You can add ad-hoc attribute or value pairs
	  • **Add Condition from Library**: You can add Cisco predefined conditions
	  • **Duplicate**: Create a copy of the selected condition
	  • **Add Condition to Library**: You can save ad-hoc attribute/value pairs that you create to the policy elements library
	  • **Delete**: Delete the selected condition. You can use the AND or OR operator

Related Topics

Cisco ISE Profiling Service, on page 775
Create Endpoint Profiling Policies, on page 819
Endpoint Context Visibility Using UDID Attribute, on page 851

Create Endpoint Profiling Policies

You can create new profiling policies to profile endpoints by using the following options in the New Profiler Policy page:

- Policy Enabled
- Create an Identity Group for the policy to create a matching endpoint identity group or use the endpoint identity group hierarchy
- Parent Policy
- Associated CoA Type

Note When you choose to create an endpoint policy in the **Profiling Policies** window, do not use the Stop button on your web browsers. This action leads to the following: stops loading the **New Profiler Policy** window, loads other list pages and the menus within the list pages when you access them, and prevents you from performing operations on all the menus within the list pages except the Filter menus. You might need to log out of Cisco ISE, and then log in again to perform operations on all the menus within the list pages.

You can create a similar characteristic profiling policy by duplicating an endpoint profiling policy through which you can modify an existing profiling policy instead of creating a new profiling policy by redefining all conditions.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Profiling** > **Profiling Policies**.

Step 2 Click **Add**.

Step 3 Enter a name and description for the new endpoint policy that you want to create. The **Policy Enabled** check box is checked by default to include the endpoint profiling policy for validation when you profile an endpoint.

Step 4 Enter a value for the minimum certainty factor within the valid range 1 to 65535.

Note The following considerations must be taken into account when you create custom profiling policies:

- If the same attributes configured in the custom policy are already configured to be evaluated by a default profiling policy, and if the default profiling policy has a greater certainty factor (CF) than the custom policy, then the custom profiling policy will never be asigned to any endpoint. This is because a profiling policy that has higher increases of CF will take precedence over any other with lower increases of the CF.
- Many default profiling policies are configured for incremental CF increases by 10, 20 and 30.

Step 5 Click the arrow next to the **Exception Action** drop-down list to associate an exception action or click the arrow next to the **Network Scan (NMAP) Action** drop-down list to associate a network scan action.

Step 6 Choose one of the following options for **Create an Identity Group for the policy**:

- **Yes, create matching Identity Group**
- **No, use existing Identity Group hierarchy**

Step 7 Click the arrow next to the **Parent Policy** drop-down list to associate a parent policy to the new endpoint policy.

Step 8 Choose a CoA type to be associated in the **Associated CoA Type** drop-down list.

Step 9 Click in the rule to add conditions and associate an integer value for the certainty factor for each condition or associate either an exception action or a network scan action for that condition for the overall classification of an endpoint.

Step 10 Click **Submit** to add an endpoint policy or click the **Profiler Policy List** link from the New Profiler Policy page to return to the Profiling Policies page.

Change of Authorization Configuration for Each Endpoint Profiling Policy

In addition to the global configuration of change of authorization (CoA) types in Cisco ISE, you can also configure to issue a specific type of CoA associated for each endpoint profiling policy.

The global No CoA type configuration overrides each CoA type configured in an endpoint profiling policy. If the global CoA type is set other than the No CoA type, then each endpoint profiling policy is allowed to override the global CoA configuration.

When a CoA is triggered, each endpoint profiling policy can determine the actual CoA type, as follows:

- General Setting—This is the default setting for all the endpoint profiling policies that issues a CoA per global configuration.
- No CoA—This setting overrides any global configuration and disables CoA for the profile.
- Port Bounce—This setting overrides the global Port Bounce and Reauth configuration types, and issues port bounce CoA.

- Reauth—This setting overrides the global Port Bounce and Reauth configuration types, and issues reauthentication CoA.

Note If the profiler global CoA configuration is set to Port Bounce (or Reauth), ensure that you configure corresponding endpoint profiling policies with No CoA, the per-policy CoA option so that the BYOD flow does not break for your mobile devices.

See the summary of configuration below combined for all the CoA types and the actual CoA type issued in each case based on the global and endpoint profiling policy settings.

Table 116: CoA Type Issued for Various Combination of Configuration

Global CoA Type	Default CoA Type set per Policy	No coA Type per Policy	Port Bounce Type per Policy	Reauth Type per Policy
No CoA	No CoA	No CoA	No CoA	No CoA
Port Bounce	Port Bounce	No CoA	Port Bounce	Re-Auth
Reauth	Reauth	No CoA	Port Bounce	Re-Auth

Import Endpoint Profiling Policies

You can import endpoint profiling policies from a file in XML by using the same format that you can create in the export function. If you import newly created profiling policies that have parent policies associated, then you must have defined parent policies before you define child policies.

The imported file contains the hierarchy of endpoint profiling policies that contain the parent policy first, then the profile that you imported next along with the rules and checks that are defined in the policy.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Profiling** > **Profiling** > **Profiling Policies**.

Step 2 Click **Import**.

Step 3 Click **Browse** to locate the file that you previously exported and want to import.

Step 4 Click **Submit**.

Step 5 Click the **Profiler Policy List** link to return to the **Profiling Policies** window.

Export Endpoint Profiling Policies

You can export endpoint profiling policies to other Cisco ISE deployments. Or, you can use the XML file as a template for creating your own policies to import. You can also download the file to your system in the default location, which can be used for importing later.

A dialog appears when you want to export endpoint profiling policies, which prompts you to open the profiler_policies.xml with an appropriate application or save it. This is a file in XML format that you can open in a web browser, or in other appropriate applications.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Profiling** > **Profiling** > **Profiling Policies**.

Step 2 Choose **Export**, and choose one of the following:

- **Export Selected**: You can export only the selected endpoint profiling policies in the **Profiling Policies** window.
- **Export Selected with Endpoints**: You can export the selected endpoint profiling policies, and the endpoints that are profiled with the selected endpoint profiling policies.
- **Export All**: By default, you can export all the profiling policies in the **Profiling Policies** window.

Step 3 Click **OK** to export the endpoint profiling policies in the profiler_policies.xml file.

Predefined Endpoint Profiling Policies

Cisco ISE includes predefined default profiling policies when Cisco ISE is deployed, and their hierarchical construction allows you to categorize identified endpoints on your network, and assign them to a matching endpoint identity groups. Because endpoint profiling policies are hierarchical, you can find that the **Profiling Policies** window displays the list of generic (parent) policies for devices and child policies to which their parent policies are associated in the Profiling Policies listing window.

The **Profiling Policies** window displays endpoint profiling policies with their names, type, description and the status, if enabled or not for validation.

The endpoint profiling policy types are classified as follows:

- Cisco Provided: Endpoint profiling policies that are predefined in Cisco ISE are identified as the Cisco Provided type.
  - Administrator Modified: Endpoint profiling policies are identified as the Administrator Modified type when you modify predefined endpoint profiling policies. Cisco ISE overwrites changes that you have made in the predefined endpoint profiling policies during upgrade.
- Administrator Created: Endpoint profiling policies that you create or when you duplicate Cisco-provided endpoint profiling policies are identified as the Administrator Created type.

We recommend that you create a generic policy (a parent) for a set of endpoints from which its children can inherit the rules and conditions. If an endpoint has to be classified, then the endpoint profile has to first match the parent, and then its descendant (child) policies when you are profiling an endpoint.

For example, Cisco-Device is a generic endpoint profiling policy for all Cisco devices, and other policies for Cisco devices are children of Cisco-Device. If an endpoint has to be classified as a Cisco-IP-Phone 7960, then the endpoint profile for this endpoint has to first match the parent Cisco-Device policy, its child Cisco-IP-Phone policy, and then the Cisco-IP-Phone 7960 profiling policy for better classification.

Note Cisco ISE will not overwrite the Administrator Modified policies nor their children policies even if they are still labeled as Cisco Provided. If an Administrator Modified policy is deleted, it reverts back to the previous Cisco Provided policy. Next time when Feed Update happens, all children policies are updated.

Predefined Endpoint Profiling Policies Overwritten During Upgrade

You can edit existing endpoint profiling policies in the Profiling Policies page. You must also save all your configurations in a copy of the predefined endpoint profiles when you want to modify the predefined endpoint profiling policies.

During an upgrade, Cisco ISE overwrites any configuration that you have saved in the predefined endpoint profiles.

Unable to Delete Endpoint Profiling Policies

You can delete selected or all the endpoint profiling policies in the **Profiling Policies** window. By default, you can delete all the endpoint profiling policies from the **Profiling Policies** window. When you select all the endpoint profiling policies and try to delete them in the **Profiling Policies** window, some of them may not be deleted, if the endpoint profiling policies are mapped to other endpoint profiling policies or mapped to an authorization policy.

- You cannot delete Cisco Provided endpoint profiling policies.
- You cannot delete a parent profile in the **Profiling Policies** window when an endpoint profile is defined as a parent to other endpoint profiles. For example, Cisco-Device is a parent to other endpoint profiling policies for Cisco devices.
- You cannot delete an endpoint profile when it is mapped to an authorization policy. For example, Cisco-IP-Phone is mapped to the Profiled Cisco IP Phones authorization policy, and it is a parent to other endpoint profiling policies for Cisco IP Phones.

Predefined Profiling Policies for Draeger Medical Devices

Cisco ISE contains default endpoint profiling policies that include a generic policy for Draeger medical devices, a policy for Draeger-Delta medical device, and a policy for Draeger-M300 medical device. Both the medical devices share ports 2050 and 2150, and therefore you cannot classify the Draeger-Delta and Draeger-M300 medical devices when you are using the default Draeger endpoint profiling policies.

If these Draeger devices share ports 2050 and 2150 in your environment, you must add a rule in addition to checking for the device destination IP address in the default Draeger-Delta and Draeger-M300 endpoint profiling policies so that you can distinquish these medical devices.

Cisco ISE includes the following profiling conditions that are used in the endpoint profiling policies for the Draeger medical devices:

- Draeger-Delta-PortCheck1 that contains port 2000
- Draeger-Delta-PortCheck2 that contains port 2050
- Draeger-Delta-PortCheck3 that contains port 2100

- Draeger-Delta-PortCheck4 that contains port 2150
- Draeger-M300PortCheck1 that contains port 1950
- Draeger-M300PortCheck2 that contains port 2050
- Draeger-M300PortCheck3 that contains port 2150

Endpoint Profiling Policy for Unknown Endpoints

An endpoint that does not match existing profiles and cannot be profiled in Cisco ISE is an unknown endpoint. An unknown profile is the default system profiling policy that is assigned to an endpoint, where an attribute or a set of attributes collected for that endpoint do not match with existing profiles in Cisco ISE.

An Unknown profile is assigned in the following scenarios:

- When an endpoint is dynamically discovered in Cisco ISE, and there is no matching endpoint profiling policy for that endpoint, it is assigned to the unknown profile.
- When an endpoint is statically added in Cisco ISE, and there is no matching endpoint profiling policy for a statically added endpoint, it is assigned to the unknown profile.

  If you have statically added an endpoint to your network, the statically added endpoint is not profiled by the profiling service in Cisco ISE. You can change the unknown profile later to an appropriate profile and Cisco ISE will not reassign the profiling policy that you have assigned.

Endpoint Profiling Policy for Statically Added Endpoints

For the endpoint that is statically added to be profiled, the profiling service computes a profile for the endpoint by adding a new MATCHEDPROFILE attribute to the endpoint. The computed profile is the actual profile of an endpoint if that endpoint is dynamically profiled. This allows you to find the mismatch between the computed profile for statically added endpoints and the matching profile for dynamically profiled endpoints.

Endpoint Profiling Policy for Static IP Devices

If you have an endpoint with a statically assigned IP address, you can create a profile for such static IP devices.

You must enable the RADIUS probe or SNMP Query and SNMP Trap probes to profile an endpoint that has a static IP address.

Endpoint Profiling Policy Matching

Cisco ISE always considers a chosen policy for an endpoint that is the matched policy rather than an evaluated policy when the profiling conditions that are defined in one or more rules are met in a profiling policy. Here, the status of static assignment for that endpoint is set to false in the system. But, this can be set to true after it is statically reassigned to an existing profiling policy in the system, by using the static assignment feature during an endpoint editing.

The following apply to the matched policies of endpoints:

- For statically assigned endpoint, the profiling service computes the MATCHEDPROFILE.

- For dynamically assigned endpoints, the MATCHEDPROFILEs are identical to the matching endpoint profiles.

You can determine a matching profiling policy for dynamic endpoints using one or more rules that are defined in a profiling policy and assign appropriately an endpoint identity group for categorization.

When an endpoint is mapped to an existing policy, the profiling service searches the hierarchy of profiling policies for the closest parent profile that has a matching group of policies and assigns the endpoint to the appropriate endpoint policy.

Endpoint Profiling Policies Used for Authorization

You can use an endpoint profiling policy in authorization rules, where you can create a new condition to include a check for an endpoint profiling policy as an attribute, and the attribute value assumes the name of the endpoint profiling policy. You can select an endpoint profiling policy from the endpoints dictionary, which includes the following attributes: PostureApplicable, EndPointPolicy, LogicalProfile, and BYODRegistration.

The attribute value for PostureApplicable is auto set based on the operating system. It is set to *No* for IOS and Android devices because AnyConnect support is not available on those platforms to perform Posture. The value is set as *Yes* for Mac OSX and Windows devices.

You can define an authorization rule that includes a combination of EndPointPolicy, BYODRegistration, and identity groups.

Wi-Fi Device Analytics Data from Cisco Catalyst 9800 Wireless LAN Controller

From Cisco ISE Release 3.1 Patch 8, you can create profiling policies, authorization conditions, and authentication conditions and policies for Apple, Intel, and Samsung endpoints, using device analytics data from the Cisco Wireless LAN Controllers integrated with your Cisco ISE. The controller learns about endpoint attributes such as model number, operating system version, and other information from a set of endpoints using device analytics. The collected data is then shared with Cisco ISE.

In Cisco ISE, the received data is added to a new dictionary named Wi-Fi Device Analytics.

You must ensure that the following conditions are met to allow device attribute data exchange between the two systems.

For Cisco Wireless LAN Controllers:

- The network device is a Cisco Catalyst 9800 Series Wireless Controller running Cisco IOS XE 17.10.1 or later versions, with 802.11ac Wave2 and 802.11ax (Wi-Fi 6/6E) access points.
- In the Cisco Catalyst 9800 Wireless Controller:
  1. Configure a policy profile to enable:
     - RADIUS Profiling
     - HTTP TLV Caching
     - DHCP TLV Caching
     - Dot11-tlv-accounting (configured only through the CLI).

2. Apple iOS analytics requires a secure WLAN with either PSK or 802.1X.
3. Samsung analytics requires a secure WLAN with WPA, WPA2, or WPA3 policy.
4. Intel analytics requires a secure WLAN with Protected Management Frame (PMF) set to either optional or required.

- RADIUS accounting must be enabled in the controller.

For information on how to configure the Cisco Catalyst 9800 Series Wireless Controllers devices, see the configuration guide for your device.

To receive device analytics data from the Cisco Wireless LAN Controllers, carry out the following steps in the Cisco ISE administration portal:

1. Choose **Administration** > **System** > **Deployment** > **Node** .
2. Click the hostname of a node.
3. In the **Edit Node** window, in the **Profiling Configuration** tab, ensure that the **RADIUS** option is enabled.
4. Choose **Work Centers** > **Device Administration** > **Network Resources** > **Network Devices**. Ensure that the required Cisco Catalyst 9800 Series Wireless Controller devices are integrated with your Cisco ISE. For information on how to add these devices to Cisco ISE, see Add a Network Device in Cisco ISE, on page 358.

After the Cisco Catalyst 9800 Series Wireless Controller devices and Cisco ISE are configured to allow the sharing of device attributes between the two systems, you can view the device attributes in the **Context Visibility** > **Endpoints** window. When you click the endpoint's MAC address, the details include new attributes whose names are in the format DEVICE_INFO_<*ATTRIBUTE NAME*>.

Seven device Information attributes are available from Cisco Wireless LAN Controllers:

- Model Number
- Firmware Version
- OS version
- Manufacturer Name
- Model Name
- Hardware Model
- Vendor Type

Endpoint Profiling Policies Grouped into Logical Profiles

A logical profile is a container for a category of profiles or associated profiles, irrespective of Cisco-provided or administrator-created endpoint profiling policies. An endpoint profiling policy can be associated with multiple logical profiles.

You can use the logical profile in an authorization policy condition to help create an overall network access policy for a category of profiles. You can create a simple condition for authorization, which can be included in the authorization rule. The attribute-value pair that you can use in the authorization condition is the logical profile (attribute) and the name of the logical profile (value), which can be found in the EndPoints systems dictionary.

For example, you can create a logical profile for all mobile devices like Android, Apple iPhone, or Blackberry by assigning matching endpoint profiling policies for that category to the logical profile. Cisco ISE contains IP-Phone, a default logical profile for all the IP phones, which includes IP-Phone, Cisco-IP-Phone, Nortel-IP-Phone-2000-Series, and Avaya-IP-Phone profiles.

From Cisco ISE Release 3.1 Patch 5 when an endpoint goes through Cisco ISE profiling workflows, if the endpoint matches an endpoint profiling policy with an associated logical profile, the endpoint is automatically assigned the logical profile. You can view the logical profiles assigned to endpoints in the **Context Visibility** > **Endpoints** > **Endpoint Classification** window.

Create Logical Profiles

You can create a logical profile that you can use to group a category of endpoint profiling policies, which allows you to create an overall category of profiles or associated profiles. You can also remove the endpoint profiling policies from the assigned set moving them back to the available set.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Profiling** > **Profiling** > **Logical Profiles**.

Step 2 Click **Add**.

Step 3 Enter a name and description for the new logical profile in the text boxes for **Name** and **Description**.

Step 4 Choose endpoint profiling policies from the **Available Policies** to assign them in a logical profile.

Step 5 Click the right arrow to move the selected endpoint profiling policies to the **Assigned Policies**.

Step 6 Click **Submit**.

Profiling Exception Actions

An exception action is a single configurable action that can be referred to in an endpoint profiling policy, and that is triggered when the exception conditions that are associated with the action are met.

Exception Actions can be any one of the following types:

- Cisco-provided—You can not delete Cisco-provided exception actions. Cisco ISE triggers the following noneditable profiling exception actions from the system when you want to profile endpoints in Cisco ISE:
  - Authorization Change—The profiling service issues a change of authorization when an endpoint is added or removed from an endpoint identity group that is used by an authorization policy.
  - Endpoint Delete—An exception action is triggered in Cisco ISE and a CoA is issued when an endpoint is deleted from the system in the Endpoints page, or reassigned to the unknown profile from the edit page on a Cisco ISE network.
  - FirstTimeProfiled—An exception action is triggered in Cisco ISE and a CoA is issued when an endpoint is profiled in Cisco ISE for the first time, where the profile of that endpoint changes from an unknown profile to an existing profile but that endpoint is not successfully authenticated on a Cisco ISE network.

- Administrator-created—Cisco ISE triggers profiling exception actions that you create.

Create Exception Actions

You can define and associate one or more exception rules to a single profiling policy. This association triggers an exception action (a single configurable action) when the profiling policy matches and at least one of the exception rules matches in the profiling endpoints in Cisco ISE.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Profiling** > **Exception Actions**.

Step 2 Click **Add**.

Step 3 Enter a name and description for the exception action in the text boxes for **Name** and **Description**.

Step 4 Check the **CoA Action** check box.

Step 5 Click the **Policy Assignment** drop-down list to choose an endpoint policy.

Step 6 Click **Submit**.

Create Endpoints with Static Assignments of Policies and Identity Groups

You can create a new endpoint statically by using the MAC address of an endpoint in the Endpoints page. You can also choose an endpoint profiling policy and an identity group in the Endpoints page for static assignment.

The regular and mobile device (MDM) endpoints are displayed in the Endpoints Identities list. In the listing page, columns for attributes like Hostname, Device Type, Device Identifier for MDM endpoints are displayed. Other columns like Static Assignment and Static Group Assignment are not displayed by default.

Note You cannot add, edit, delete, import, or export MDM Endpoints using this page.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Identities** > **Endpoints**.

Step 2 Click **Add**.

Step 3 Enter the MAC address of an endpoint in hexadecimal format and separated by a colon.

Step 4 Choose a matching endpoint policy from the **Policy Assignment** drop-down list to change the static assignment status from dynamic to static.

Step 5 Check the **Static Assignment** check box to change the status of static assignment that is assigned to the endpoint from dynamic to static.

Step 6 Choose an endpoint identity group to which you want to assign the newly created endpoint from the **Identity Group Assignment** drop-down list.

Step 7 Check the **Static Group Assignment** check box to change the dynamic assignment of an endpoint identity group to static.

Step 8 Click **Submit**.

Import Endpoints Using a CSV File

You can import endpoints from a CSV file that you have created from a Cisco ISE template and update it with endpoint details. Endpoints exported from Cisco ISE contains around 90 attributes and therefore cannot be imported directly into another ISE deployment. If columns that are not allowed for import are present in the CSV file, a message with the list of attributes that cannot be imported is displayed. You must delete the specified columns before trying to import the file again.

In the **Export Endpoints** dialog box, check the **Importable Only** check box if you want to export only the attributes that can be imported to Cisco ISE without any modification to the CSV file. Using this option removes the need to modify the column or metadata in the exported CSV file before importing it to Cisco ISE.

There are about 31 attributes that can be imported. The list includes MACAddress, EndPointPolicy, and IdentityGroup. Optional attributes are:

Description	PortalUser	LastName
PortalUser.GuestType	PortalUser.FirstName	EmailAddress
PortalUser.Location	Device Type	host-name
PortalUser.GuestStatus	StaticAssignment	Location
PortalUser.CreationType	StaticGroupAssignment	MDMEnrolled
PortalUser.EmailAddress	User-Name	MDMOSVersion
PortalUser.PhoneNumber	DeviceRegistrationStatus	MDMServerName
PortalUser.LastName	AUPAccepted	MDMServerID
PortalUser.GuestSponsor	FirstName	BYODRegistration
CUSTOM.<custom attribute name>	—	—

The file header has to be in the format as specified in the default import template so that the list of endpoints appear in this order: MACAddress, EndpointPolicy, IdentityGroup <List of attributes listed above as optional attributes>. You can create the following file templates:

- MACAddress
- MACAddress, EndPointPolicy
- MACAddress, EndPointPolicy, IdentityGroup
- MACAddress, EndPointPolicy, IdentityGroup, <List of attributes listed above as optional attributes>

All attribute values, except MAC address, are optional for importing endpoints from a CSV file. If you want to import endpoints without certain values, the values are still separated by a comma. For example,

- MAC1, Endpoint Policy1, Endpoint Identity Group1
- MAC2
- MAC3, Endpoint Policy3
- MAC4, , Endpoint Identity Group4
- MAC5, , Endpoint Identity Group5, MyDescription, MyPortalUser, and so on

To import the endpoints using a CSV file:

Step 1 Choose **Context Visibility** > **Endpoints** > **Import** .

Step 2 Click **Import From File**.

Step 3 Click **Browse** to locate the CSV file that you have already created.

Step 4 Click **Submit**.

To import endpoint custom attributes, you have to create the same custom attributes as in the CSV file in the **Administration** > **Identity Management** > **Settings** > **Endpoint Custom Attributes** window using the correct data types. These attributes have to be prefixed with CUSTOM to differentiate them from endpoint attributes.

Default Import Template Available for Endpoints

You can generate a template in which you can update endpoints that can be used to import endpoints. By default, you can use the Generate a Template link to create a CSV file in the Microsoft Office Excel application and save the file locally on your system. The file can be found in **Context Visibility** > **Endpoints** > **Import** > **Import From File**. You can use the Generate a Template link to create a template, and the Cisco ISE server will display the Opening template.csv dialog. This dialog allows you to open the default template.csv file, or save the template.csv file locally on your system. If you choose to open the template.csv file from the dialog, the file opens in the Microsoft Office Excel application. The default template.csv file contains a header row that displays the MAC address, Endpoint Policy, and Endpoint Identity Group, and other optional attributes.

You must update the MAC addresses of endpoints, endpoint profiling policies, endpoint identity groups along with any of the optional attribute values you wish to import, and save the file with a new file name. This file can be used to import endpoints. See the header row in the template.csv file that is created when you use the Generate a Template link.

Table 117: CSV Template File

MAC	EndpointPolicy	IdentityGroup	Other Optional Attributes
11:11:11:11:11:11	Android	Profiled	<Empty>/<Value>

Unknown Endpoints Reprofiled During Import

If the file used for import contains endpoints that have their MAC addresses, and their assigned endpoint profiling policies is the Unknown profile, then those endpoints are immediately reprofiled in Cisco ISE to the matching endpoint profiling policies during import. However, they are not statically assigned to the Unknown profile. If endpoints do not have endpoint profiling policies assigned to them in the CSV file, then they are assigned to the Unknown profile, and then reprofiled to the matching endpoint profiling policies. See below how Cisco ISE reprofiles Unknown profiles that match the Xerox_Device profile during import and also how Cisco ISE reprofiles an endpoint that is unassigned.

Table 118: Unknown Profiles: Import from a File

MAC Address	Endpoint Profiling Policy Assigned Before Import in Cisco ISE	Endpoint Profiling Policy Assigned After Import in Cisco ISE
00:00:00:00:01:02	Unknown	Xerox-Device
00:00:00:00:01:03	Unknown	Xerox-Device
00:00:00:00:01:04	Unknown	Xerox-Device
00:00:00:00:01:05	If no profile is assigned to an endpoint, then it is assigned to the Unknown profile, and also reprofiled to the matching profile.	Xerox-Device

Endpoints with Invalid Attributes Not Imported

If any of the endpoints present in the CSV file have invalid attributes, then the endpoints are not imported and an error message is displayed.

For example, if endpoints are assigned to invalid profiles in the file used for import, then they are not imported because there are no matching profiles in Cisco ISE. See below how endpoints are not imported when they are assigned to invalid profiles in the CSV file.

Table 119: Invalid Profiles: Import from a File

MAC Address	Endpoint Profiling Policy Assigned Before Import in Cisco ISE	Endpoint Profiling Policy Assigned After Import in Cisco ISE
00:00:00:00:01:02	Unknown	Xerox-Device
00:00:00:00:01:05	If an endpoint such as 00:00:00:00:01:05 is assigned to an invalid profile other than the profiles that are available in Cisco ISE, then Cisco ISE displays a warning message that the policy name is invalid and the endpoint will not be imported.	The endpoint is not imported because there is no matching profile in Cisco ISE.

Import Endpoints from LDAP Server

You can import the MAC addresses, the associated profiles, and the endpoint identity groups of endpoints securely from an LDAP server.

Before you begin

Before you begin to import endpoints, ensure that you have installed the LDAP server.

You have to configure the connection settings and query settings before you can import from an LDAP server. If the connection settings or query settings are configured incorrectly in Cisco ISE, then the "LDAP import failed:" error message appears.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Context Visibility** > **Endpoints** > **Import** > **Import from LDAP**.

Step 2 Enter the values for the connection settings.

Step 3 Enter the values for the query settings.

Step 4 Click **Submit**.

Export Endpoints Using CSV File

You can export all the endpoints or only the selected endpoints using a CSV file. The endpoints are listed with around 90 attributes along with their MAC addresses, endpoint profiling policies, and endpoint identity groups. The custom attributes are also exported to the CSV file and are prefixed with CUSTOM to differentiate them from other endpoint attributes.

Note To import endpoint custom attributes that are exported from one deployment to another, you must create the same custom attributes in the **Administration** > **Identity Management** > **Settings** > **Endpoint Custom Attributes** window and use the same data type as specified in the original deployment.

To export the endpoints using a CSV file:

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Context Visibility** > **Endpoints**.

Step 2 From the **Export** drop-down list, choose one of the following options:

- **Export All**: Choose this option to export all the endpoints listed in the **Endpoints** window.
- **Export Selected**: Choose this option to export only the selected endpoints.
- **Export Filtered**: Choose this option while using the **Quick Filter** or the **Advanced Filter** option to export only the filtered endpoints.

Step 3 In the **Export Endpoints** dialog box, check the **Importable Only** check box if you want to export only the attributes that can be imported to Cisco ISE without any modification to the CSV file. Using this option prevents the need to modify the columns or metadata in the exported CSV file before importing it to Cisco ISE.

Step 4 Click **OK** to save the CSV file.

Most of the attributes in the exported spreadsheet are simple. The following attributes require an explanation:

- *UpdateTime*: The last time that the profiler updated the endpoint, due to a change to an endpoint attribute. The value is 0 if there have been no updates since the endpoint session started. It will be blank briefly, during an update

- *InactivityTime*: Time since the endpoint was active.

Identified Endpoints

Cisco ISE displays identified endpoints that connect to your network and use resources on your network in the **Endpoints** window. An endpoint is typically a network-capable device that connect to your network through wired and wireless network access devices and VPN. Endpoints can be personal computers, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, and so on.

The MAC address of an endpoint, expressed in hexadecimal form, is always the unique representation of an endpoint, but you can also identify an endpoint with a varying set of attributes and the values associated to them, called an attribute-value pair. You can collect a varying set of attributes for endpoints based on the endpoint capability, the capability and configuration of the network access devices and the methods (probes) that you use to collect these attributes.

Dynamically Profiled Endpoints

When endpoints are discovered on your network, they can be profiled dynamically based on the configured profiling endpoint profiling policies, and assigned to the matching endpoint identity groups depending on their profiles.

Statically Profiled Endpoints

An endpoint can be profiled statically when you create an endpoint with its MAC address and associate a profile to it along with an endpoint identity group in Cisco ISE. Cisco ISE does not reassign the profiling policy and the identity group for statically assigned endpoints.

Unknown Endpoints

If you do not have a matching profiling policy for an endpoint, you can assign an unknown profiling policy (Unknown) and the endpoint therefore will be profiled as Unknown. The endpoint profiled to the Unknown endpoint policy requires that you create a profile with an attribute or a set of attributes collected for that endpoint. The endpoint that does not match any profile is grouped within the Unknown endpoint identity group.

Identified Endpoints Locally Stored in Policy Service Nodes Database

Cisco ISE writes identified endpoints locally in the Policy Service node database. After storing endpoints locally in the database, these endpoints are then made available (remote write) in the Administration node database only when significant attributes change in the endpoints, and replicated to the other Policy Service nodes database. Significant attributes are those used by the Cisco ISE system or those used specifically in an endpoint profiling policy or rule.

The following are the significant attributes:

- ip
- EndPointPolicy
- MatchedValue

- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

When you change endpoint profile definitions in Cisco ISE, all endpoints have to be reprofiled. A Policy Service node that collects the attributes of endpoints is responsible for reprofiling of those endpoints.

When a Policy Service node starts collecting attributes about an endpoint for which attributes were initially collected by a different Policy Service node, then the endpoint ownership changes to the current Policy Service node. The new Policy Service node will retrieve the latest attributes from the previous Policy Service node and reconcile the collected attributes with those attributes that were already collected.

When a significant attribute changes in the endpoint, attributes of the endpoint are automatically saved in the Administration node database so that you have the latest significant change in the endpoint. If the Policy Service node that owns an endpoint is not available for some reasons, then the Administrator ISE node will reprofile an endpoint that lost the owner and you have to configure a new Policy Service node for such endpoints.

Policy Service Nodes in Cluster

Cisco ISE uses Policy Service node group as a cluster that allows to exchange endpoint attributes when two or more nodes in the cluster collect attributes for the same endpoint. We recommend to create clusters for all Policy Service nodes that reside behind a load balancer.

If a different node other than the current owner receives attributes for the same endpoint, it sends a message across the cluster requesting the latest attributes from the current owner to merge attributes and determine if a change of ownership is needed. If you have not defined a node group in Cisco ISE, it is assumed that all nodes are within one cluster.

There are no changes made to endpoint creation and replication in Cisco ISE. Only the change of ownership for endpoints is decided based on an allowed list of attributes used for profiling that are built from static attributes and dynamic attributes.

Upon subsequent attributes collection, the endpoint is updated on the Administration node, if anyone of the following attributes changes:

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID

- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

When an endpoint is edited and saved in the Administration node, the attributes are retrieved from the current owner of the endpoint.

Create Endpoint Identity Groups

Cisco ISE groups endpoints that it discovers in to the corresponding endpoint identity groups. Cisco ISE comes with several system-defined endpoint identity groups. You can also create additional endpoint identity groups from the **Endpoint Identity Groups** window. You can edit or delete the endpoint identity groups that you have created. You can only edit the description of the system-defined endpoint identity groups. You cannot edit the name of these groups or delete them.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **Groups** > **Endpoint Identity Groups**.

Step 2 Click **Add**.

Step 3 Enter the **Name** for the endpoint identity group that you want to create (do not include spaces in the name of the endpoint identity group).

Step 4 Enter the **Description** for the endpoint identity group that you want to create.

Step 5 Click the **Parent Group** drop-down list to choose an endpoint identity group to which you want to associate the newly created endpoint identity group.

Step 6 Click **Submit**.

Identified Endpoints Grouped in Endpoint Identity Groups

Cisco ISE groups discovered endpoints into their corresponding endpoint identity groups based on the endpoint profiling policies. Profiling policies are hierarchical, and they are applied at the endpoint identify groups level in Cisco ISE. By grouping endpoints to endpoint identity groups, and applying profiling policies to endpoint identity groups, Cisco ISE enables you to determine the mapping of endpoints to the endpoint profiles by checking corresponding endpoint profiling policies.

Cisco ISE creates a set of endpoint identity groups by default, and allows you to create your own identity groups to which endpoints can be assigned dynamically or statically. You can create an endpoint identity group and associate the identity group to one of the system-created identity groups. You can also assign an endpoint that you create statically to any one of the identity groups that exists in the system, and the profiling service cannot reassign the identity group.

Default Endpoint Identity Groups Created for Endpoints

Cisco ISE creates the following endpoint identity groups:

- Blocked List: This endpoint identity group includes endpoints that are statically assigned to this group in Cisco ISE and endpoints that are blocked in the device registration portal. An authorization profile can be defined in Cisco ISE to permit, or deny network access to endpoints in this group.
- GuestEndpoints: This endpoint identity group includes endpoints that are used by guest users.
- Profiled: This endpoint identity group includes endpoints that match endpoint profiling policies except Cisco IP phones and workstations in Cisco ISE.
- RegisteredDevices: This endpoint identity group includes endpoints, which are registered devices that are added by an employee through the devices registration portal. The profiling service continues to profile these devices normally when they are assigned to this group. Endpoints are statically assigned to this group in Cisco ISE, and the profiling service cannot reassign them to any other identity group. These devices will appear like any other endpoint in the endpoints list. You can edit, delete, and block these devices that you added through the device registration portal from the endpoints list in the Endpoints window in Cisco ISE. Devices that you have blocked in the device registration portal are assigned to the Blocked List endpoint identity group, and an authorization profile that exists in Cisco ISE redirects blocked devices to a URL, which displays “Unauthorised Network Access”, a default portal page to the blocked devices.
- Unknown: This endpoint identity group includes endpoints that do not match any profile in Cisco ISE.

In addition to the above system created endpoint identity groups, Cisco ISE creates the following endpoint identity groups, which are associated to the Profiled (parent) identity group. A parent group is the default identity group that exists in the system:

- Cisco-IP-Phone: An identity group that contains all the profiled Cisco IP phones on your network.
- Workstation: An identity group that contains all the profiled workstations on your network.

Endpoint Identity Groups Created for Matched Endpoint Profiling Policies

If you have an endpoint policy that matches an existing policy, then the profiling service can create a matching endpoint identity group. This identity group becomes the child of the Profiled endpoint identity group. When you create an endpoint policy, you can check the Create Matching Identity Group check box in the Profiling Policies page to create a matching endpoint identity group. You cannot delete the matching identity group unless the mapping of the profile is removed.

Add Static Endpoints in Endpoint Identity Groups

You can add or remove statically added endpoints in any endpoint identity group.

You can add endpoints from the Endpoints widget only to a specific identity group. If you add an endpoint to the specific endpoint identity group, then the endpoint is moved from the endpoint identity group where it was dynamically grouped earlier.

Upon removal from the endpoint identity group where you recently added an endpoint, the endpoint is reprofiled back to the appropriate identity group. You do not delete endpoints from the system but only remove them from the endpoint identity group.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **Groups** > **Endpoint Identity Groups**.

Step 2 Choose an endpoint identity group, and click **Edit**.

Step 3 Click **Add**.

Step 4 Choose an endpoint in the Endpoints widget to add the selected endpoint in the endpoint identity group.

Step 5 Click the **Endpoint Group List** link to return to the Endpoint Identity Groups page.

Dynamic Endpoints Reprofiled After Adding or Removing in Identity Groups

If an endpoint identity group assignment is not static, then endpoints are reprofiled after you add or remove them from an endpoint identity group. Endpoints that are identified dynamically by the ISE profiler appear in appropriate endpoint identity groups. If you remove dynamically added endpoints from an endpoint identity group, Cisco ISE displays a message that you have successfully removed endpoints from the identity group but reprofiles them back in the endpoint identity group.

Endpoint Identity Groups Used in Authorization Rules

You can effectively use endpoint identity groups in the authorization policies to provide appropriate network access privileges to the discovered endpoints. For example, an authorization rule for all types of Cisco IP Phones is available by default in Cisco ISE in the following location: **Policy** > **Policy Sets** > **Default** > **Authorization Policy** .

You must ensure that the endpoint profiling policies are either standalone policies (not a parent to other endpoint profiling policies), or their parent policies of the endpoint profiling policies are not disabled.

Anycast and Profiler Services

Anycast is a networking technique where the same IP address is assigned to two or more hosts and routing is allowed to determine the most appropriate target to receive the data. Similar to the load balancer use cases to provide a single target for profiling data (RADIUS, DHCP relay, SNMP traps, and NetFlow), Anycast allows the sources to be configured with a single IP target to avoid sending the same data to multiple destinations.

The Anycast IP address can be assigned to a real PSN interface IP address or a load balancer virtual IP address to support redundancy across data centers. You must not assign the Anycast IP address to ISE Gigabit Ethernet 0 management interface.

The interface used for Anycast must be a dedicated interface used by the Profiler probe. The same requirement does not apply when the Anycast IP address is assigned to a load balancer virtual IP address.

When using Anycast, it is critical that any node failure be automatically detected and the corresponding route to the failed node be removed from the routing table. If an Anycast target is the only host on the link or VLAN, then failure may result in route being automatically removed.

When IP Anycast is deployed, it is very important to ensure that the route metrics to each target have significant weighting or bias. If the routes to Anycast targets flap or result in an Equal-Cost Multi-Path Routing (ECMP) scenario, then traffic for a given service (RADIUS AAA, DHCP or SNMP Trap Profiling, HTTPS portals) may be distributed to each target resulting in excessive traffic and service failures (RADIUS AAA and HTTPS portals) or suboptimal profiling and database replication (profiling services).

The key advantage of IP Anycast is that it greatly simplifies the configuration on access devices, profile data sources, and DNS. It can also optimize ISE profiling by ensuring that the data for a given endpoint is sent only to a single PSN. Additional route configuration must be carefully planned and managed with appropriate monitors. However, troubleshooting might be difficult because distinct subnetworks and IP addresses are not used.

Profiler Feed Service

Profiler conditions, exception actions, and NMAP scan actions are classified as Cisco-provided or administrator-created, as shown in the System Type attribute. Endpoint profiling policies are classified as Cisco-provided, administrator-created, or administrator- modified. These classifications are shown in the System Type attribute.

You can perform different operations on the profiler conditions, exception actions, NMAP scan actions, and endpoint profiling policies depending on the System Type attribute. You cannot edit or delete Cisco-provided conditions, exception actions, and nmap scan actions. You can not delete Endpoint policies that are provided by Cisco. When you edit policies, they are called administrator-modified. When the feed service updates policies, the administrator-modified policies are replaced by the up-to-date version of the Cisco-provided policy that it was based on.

You can retrieve new and updated endpoint profiling policies and the updated OUI database from the Cisco feed server. You must have a subscription to Cisco ISE. You can also receive e-mail notifications about applied, success, and failure messages. You can send the anonymous information back to Cisco about feed service actions, which helps Cisco improve the feed service.

The OUI database contains the MAC OUIs assigned to vendors. The OUI list is available here: http://standards.ieee.org/develop/regauth/oui/oui.txt

Cisco ISE downloads policies and OUI database updates every day at 1:00 A.M of the local Cisco ISE server time zone. Cisco ISE automatically applies these downloaded feed server policies, and stores the the changes so that you can revert to the previous state. When you revert to a previous state, the new endpoint profiling policies are removed and updated endpoint profiling policies are reverted to the previous state. In addition, the profiler feed service is automatically disabled.

You can also update the feed services manually in offline mode. You can download the updates manually by using this option if you cannot connect your ISE deployments to Cisco feed service.

Note Updates from the Feed Service are not allowed after the license goes Out of Compliance (OOC) for 45 days within a 60-day window period. The license is out of compliance when it has expired, or when the usage exceeds the allowed number of sessions.

Configure Profiler Feed Service

The Profiler Feed Service retrieves new and updated endpoint profiling policies and MAC OUI database updates from the Cisco Feed server. If the Feed Service is unavailable or other errors have occurred, it is reported in the Operations Audit report.

You can configure Cisco ISE to send anonymous feed service usage report back to Cisco, which sends the following information to Cisco:

- Hostname: Cisco ISE hostname
- MaxCount: Total number of endpoints

- ProfiledCount: Profiled endpoints count
- UnknownCount: Unknown endpoints count
- MatchSystemProfilesCount: Cisco Provided profiles count
- UserCreatedProfiles: User created profiles count

You can change the CoA type in a Cisco-provided profiling policy. When the feed service updates that policy, the CoA type will not be changed, but the rest of that policy's attributes will be still be updated.

Cisco ISE, Release 2.7 and later allow you to manually download OUI updates without downloading policy updates. If you customized some of your profiler conditions to change more than just the CoA type, you may not want the profiler feed to replace those conditions. You may still want the OUI updates, so the profiler can identify new devices as manufacturers add them. The option to download only OUI is available on the Feed Service portal.

Before you begin

The Profiler feed service can only be configured from the Cisco ISE Admin portal in a distributed deployment or in a standalone ISE node.

Set up a Simple Mail Transfer Protocol (SMTP) server if you plan to send e-mail notifications from the Admin portal about feed updates (**Administration** > **System** > **Settings**).

To update the Feed Services online:

Step 1 Choose **Administration** > **System** > **Certificates** > **Trusted Certificates**, and check if **QuoVadis Root CA 2** is enabled.

Step 2 Choose **Work Centers** > **Profiler** > **Feeds**.
You can also access the option in the **Administration** > **FeedService** > **Profiler** page.

Step 3 Click the **Online Subscription Update** tab.

Step 4 Click the **Test Feed Service Connection** button to verify that there is a connection to the Cisco Feed Service, and that the certificate is valid.

Step 5 Check the **Enable Online Subscription Update** check box.

Step 6 Enter time in HH:MM format (local time zone of the Cisco ISE server). By default, Cisco ISE feed service is scheduled at 1.00 AM every day.

Step 7 Check the **Notify administrator when download occurs** check box and enter your e-mail address in the **Administrator email address** text box. Check the **Provide Cisco anonymous information to help improve profiling accuracy** check box, if you want to allow Cisco ISE to collect non-sensitive information (that will be used to provide better services and additional features in forthcoming releases).

Step 8 Click **Save**.

Step 9 Click **Update Now**.

Instructs Cisco ISE to contact Cisco feed server for new and updated profiles created since the last feed service update. This re-profiles all endpoints in the system, which may cause an increase the load on the system. Due to updated endpoint profiling policies, there may be changes in the authorization policy for some endpoints that are currently connected to Cisco ISE.

The **Update Now** button is disabled when you update new and updated profiles created since the last feed service and enabled only after the download is completed. You must navigate away from the profiler feed service configuration window and return to this window.

Related Topics

Configure Profiler Feed Services Offline, on page 840

Configure Profiler Feed Services Offline

You can update the feed services offline when Cisco ISE is not directly connected to the Cisco feed server. You can download the offline update package from the Cisco feed server and upload it to Cisco ISE using the offline feed update. You can also set email notifications about new policies that are added to the feed server.

Configuring the profiler feed services offline involves the following tasks:

1. Download Offline Update Package
2. Apply Offline Feed Updates

Download Offline Update Package

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Profiler** > **Feeds**.
You can also access the option in the **Administration** > **FeedService** > **Profiler** page.

Step 2 Click the **Offline Manual Update** tab.

Step 3 Click **Download Updated Profile Policies** link. You will be redirected to Feed Service Partner Portal.
You can also go to https://ise.cisco.com/partner/ from your browser, to go to the feed service partner portal directly.

Step 4 If you are a first time user, accept the terms and agreements.
An email will be triggered to Feed Services administrator to approve your request. Upon approval, you will receive a confirmation email.

Step 5 Login to the partner portal using your Cisco.com credentials.

Step 6 Choose **Offline Feed** > **Download Package** .

Step 7 Click **Generate Package** .

Step 8 Click the **Click to View the Offline Update Package contents** link to view all the profiles and OUIs that are included in the generated package.

- The policies under Feed Profiler 1 and Feed OUI will be downloaded to all versions of Cisco ISE.
- The policies under Feed Profiler 2 will be downloaded only to Cisco ISE Release 1.3 and later.
- The policies under Feed Profiler 3 will be downloaded only to Cisco ISE Release 2.1 and later.

Step 9 Click **Download Package** and save the file to your local system.
You can upload the saved file to Cisco ISE server to apply the feed updates in the downloaded package.

Apply Offline Feed Updates

Before you begin

You must have downloaded the offline update package before applying the feed updates.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Profiler** > **Feeds** .
You can also access the option in the **Administration** > **FeedService** > **Profiler** window.

Step 2 Click the **Offline Manual Update** tab.

Step 3 Click **Browse** and choose the downloaded profiler feed package.

Step 4 Click **Apply Update** .

Configure Email Notifications for Profile and OUI Updates

You can configure your email address to receive notifications on profile and OUI updates.

Step 1 Perform **Step 1** through **Step 5** in the Download Offline Update Package section to go to the Feed Service Partner Portal.

Step 2 Choose **Offline Feed** > **Email Preferences**.

Step 3 Check the **Enable Notifications** checkbox to receive notifications.

Step 4 Choose the number of days from the **days** drop-down list to set the frequency in which you want to receive the notifications on new updates.

Step 5 Enter the e-mail address/addresses and click **Save** .

Undo Feed Updates

You can revert endpoint profiling policies that were updated in the previous update and remove endpoint profiling policies and OUIs that are newly added through the previous update of the profiler feed service .

An endpoint profiling policy, if modified after an update from the feed server is not changed in the system.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Profiler** > **Feeds**.

Step 2 Click **Go to Update Report Page** if you want to view the configuration changes made in the Change Configuration Audit report.

Step 3 Click **Undo Latest**.

Profiler Reports

Cisco ISE provides you with various reports on endpoint profiling, and troubleshooting tools that you can use to manage your network. You can generate reports for historical as well as current data. You may be able to drill down on a part of the report to view more details. For large reports, you can also schedule reports and download them in various formats.

You can run the following reports for endpoints from **Operations > Reports > Endpoints and Users**:

- Endpoint Session History
- Profiled Endpoint Summary
- Endpoint Profile Changes
- Top Authorizations by Endpoint
- Registered Endpoints

Detect Anomalous Behavior of Endpoints

Cisco ISE protects your network from the illegitimate use of a MAC address. Cisco ISE detects the endpoints involved in MAC address spoofing and allows you to restrict the permission of the suspicious endpoints.

The following are the two options in the profiler configuration page for Anomalous Behavior:

- Enable Anomalous Behavior Detection
- Enable Anomalous Behavior Enforcement

If you enable Anomalous Behavior detection, Cisco ISE probes for data, and checks for any contradiction to the existing data with respect to changes in attributes related to NAS-Port-Type, DHCP Class Identifier, and Endpoint Policy. If so, an attribute called **AnomalousBehavior** set to true is added to the endpoint which helps you to filter and view the endpoints in the Visibility Context page. Audit logs are also generated for the respective MAC address.

When anomalous behavior detection is enabled, Cisco ISE checks if the following attributes of existing endpoints have changed:

1. Port-Type—Determines if the access method of an endpoint has changed. This only applies when the same MAC address that is connected via Wired Dot1x has been used for Wireless Dot1x and visa-versa.
2. DHCP Class Identifier—Determines whether the type of client or vendor of an endpoint has changed. This only applies when DHCP Class identifier attribute is populated with a certain value and is then changed to another value. If an endpoint is configured with a static IP, the DHCP Class Identifier attribute is empty in Cisco ISE. Later on, if another device spoofs the MAC address of this endpoint and uses DHCP, the Class Identifier changes from an empty value to a specific string. This will not trigger anomalous behavior detection.
3. Endpoint Policy—Determines if there are significant profile changes. This only applies when the profile of an endpoint changes from a “Phone” or “Printer” to a “Workstation”.

If you enable Anomalous Behavior Enforcement, a CoA is issued upon detection of the anomalous Behavior, which can be used to re-authorize the suspicious endpoints, based on the authorization rules configured in the **Profiler Configuration** window.

Set Authorization Policy Rules for Endpoints with Anomalous Behavior

You can choose the action to be taken against any endpoint with anomalous Behavior by setting the corresponding rules on the Authorization Policy page.

Step 1 Choose **Policy** > **Policy Sets**.

Step 2 Click the arrow icon › from the **View** column corresponding to the Default Policy to open the Set view screen and view and manage the default authorization policy.

Step 3 From the **Actions** column on any row, click the cog icon and then from the drop-down list, insert a new authorization rule by selecting any of the insert or duplicate options, as necessary.
A new row appears in the Policy Sets table.

Step 4 Enter the Rule Name.

Step 5 From the **Conditions** column, click the (+) symbol.

Step 6 Create the required conditions in the **Conditions Studio Page**. In the **Editor** section, click the **Click To Add an Attribute** text box, and select the required Dictionary and Attribute (for example, Endpoints.AnomalousBehaviorEqualsTrue).

You can also drag and drop a Library condition to the **Click To Add An Attribute** text box.

Step 7 Click **Use** to set the authorization policy rules for endpoints with anomalous behavior.

Step 8 Click **Done**.

View Endpoints with Anomalous Behavior

You can view the endpoints with anomalous behavior by using any of the following options:

- Click Anomalous Behavior from **Home** > **Summary** > **Metrics**. This action opens a new tab with Anomalous Behaviour column in the lower pane of the window.
- Choose **Context Visibility** > **Endpoints** > **Endpoint Classification**. You can view the Anomalous Behaviour column in the lower pane of the window.
- You can create a new Anomalous Behavior column in Authentication view or Compromised Endpoints view in the Context Visibility window as explained in the following steps:

Step 1 Choose **Context Visibility** > **Endpoints** > **Authentication** or **Context Visibility** > **Endpoints** > **Compromised Endpoints**.

Step 2 Click the Settings icon in the lower pane of the window and check **Anomalous Behavior** check box..

Step 3 Click **Go**.
You can view the Anomalous Behavior column in the Authentication or Compromised Endpoints View.

Agent Download Issues on Client Machine

Problem

The client machine browser displays a “no policy matched” error message after user authentication and authorization. This issue applies to user sessions during the client provisioning phase of authentication.

Possible Causes

The client provisioning policy is missing required settings.

Posture Agent Download Issues

Remember that downloading the posture agent installer requires the following:

- The user must allow the ActiveX installer in the browser session the first time an agent is installed on the client machine. The client provisioning download page prompts for this.
- The client machine must have Internet access.

Resolution

- Ensure that a client provisioning policy exists in Cisco ISE. If yes, verify the policy identity group, conditions, and type of agent defined in the policy. Also ensure whether or not there is any agent profile configured under **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources** > **Add** > **AnyConnect Posture Profile**, even a profile with all default values.
- Try re-authenticating the client machine by bouncing the port on the access switch.

Endpoints

These windows enable you to configure and manage endpoints that connect to your network.

Endpoint Settings

The following table describes the fields on the **Endpoints** window, which you can use to create endpoints and assign policies for endpoints. To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Identities** > **Endpoints**.

Table 120: Endpoint Settings

Field Name	Usage Guidelines
MAC Address	Enter the MAC address in hexadecimal format to create an endpoint statically. The MAC address is the device identifier for the interface that is connected to the Cisco ISE enabled network.

Field Name	Usage Guidelines
Static Assignment	Check this check box when you want to create an endpoint statically in the Endpoints window and the status of static assignment is set to static. You can toggle the status of static assignment of an endpoint from static to dynamic or from dynamic to static.
Policy Assignment	(Disabled by default unless the **Static Assignment** is checked) Choose a matching endpoint policy from the **Policy Assignment** drop-down list. You can do one of the following: • If you do not choose a matching endpoint policy, but use the default endpoint policy Unknown, then the static assignment status is set to dynamic for the endpoint that allows dynamic profiling of an endpoint. • If you choose a matching endpoint policy other than Unknown, then the static assignment status is set to static for that endpoint and the **Static Assignment** check box is automatically checked.
Static Group Assignment	Check this check box when you want to assign an endpoint to an identity group statically. In you check this check box, the profiling service does not change the endpoint identity group the next time during evaluation of the endpoint policy for these endpoints, which were previously assigned dynamically to other endpoint identity groups. If you uncheck this check box, then the endpoint identity group is dynamic as assigned by the ISE profiler based on policy configuration. If you do not choose the Static Group Assignment option, then the endpoint is automatically assigned to the matching identity group the next time during evaluation of the endpoint policy.

Identity Group Assignment	Choose an endpoint identity group to which you want to assign the endpoint.
	You can assign an endpoint to an identity group when you create an endpoint statically, or when you do not want to use the **Create Matching Identity Group** option during evaluation of the endpoint policy for an endpoint.
	Cisco ISE includes the following system created endpoint identity groups:
	• Blocked List
	• GuestEndpoints
	• Profiled
	  • Cisco IP-Phone
	  • Workstation
	• RegisteredDevices
	• Unknown

Active Directory user endpoints that repeatedly fail RADIUS authentication for the same reason will be automatically rejected for a certain period, to avoid unnecessary processing by Cisco ISE and to protect against potential denial of service attacks.

To view a list of rejected endpoints, choose **Operations** > **Reports** > **Rejected Endpoints**. The data for this report will be available and displayed only when Advantage License is installed.

Note AD user endpoints that fail RADIUS authentication with the following two error messages are not rejected:

22063 - WRONG_PASSWORD

24408 - ACTIVE_DIRECTORY_USER_WRONG_PASSWORD

Related Topics

Identified Endpoints, on page 833
Create Endpoints with Static Assignments of Policies and Identity Groups, on page 828

Endpoint Import from LDAP Settings

The following table describes the fields on the Import from LDAP window, which you can use to import endpoints from an LDAP server. To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Identities** > **Endpoints**.

Table 121: Endpoint Import from LDAP Settings

Field Name	Usage Guidelines
Connection Settings	
Host	Enter the hostname, or the IP address of the LDAP server.
Port	Enter the port number of the LDAP server. You can use the default port 389 to import from an LDAP server, and the default port 636 to import from an LDAP server over SSL. **Note** Cisco ISE supports any configured port number. The configured value should match the LDAP server connection details.
Enable Secure Connection	Check the **Enable Secure Connection** check box to import from an LDAP server over SSL.
Root CA Certificate Name	Click the drop-down arrow to view the trusted CA certificates. The Root CA Certificate Name refers to the trusted CA certificate that is required to connect to an LDAP server. You can add (import), edit, delete, and export trusted CA certificates in Cisco ISE.
Anonymous Bind	You must enable either the **Anonymous Bind** check box, or enter the LDAP administrator credentials from the slapd.conf configuration file.

Field Name	Usage Guidelines
Admin DN	Enter the distinguished name (DN) configured for the LDAP administrator in the slapd.conf configuration file. Admin DN format example: cn=Admin, dc=cisco.com, dc=com
Password	Enter the password configured for the LDAP administrator in the slapd.conf configuration file.
Base DN	Enter the distinguished name of the parent entry. Base DN format example: dc=cisco.com, dc=com.
Query Settings	
MAC Address objectClass	Enter the query filter, which is used for importing the MAC address, for example, ieee802Device.
MAC Address Attribute Name	Enter the returned attribute name for import, for example, macAddress.
Profile Attribute Name	Enter the name of the LDAP attribute. This attribute holds the policy name for each endpoint entry that is defined in the LDAP server. When you configure the **Profile Attribute Name** field, consider the following: • If you do not specify this LDAP attribute in the **Profile Attribute Name** field or configure this attribute incorrectly, then endpoints are marked “Unknown” during an import operation, and these endpoints are profiled separately to the matching endpoint profiling policies. • If you configure this LDAP attribute in the **Profile Attribute Name** field, the attribute values are validated to ensure that the endpoint policy matches with an existing policy in Cisco ISE, and endpoints are imported. If the endpoint policy does not match with an existing policy, then those endpoints will not be imported.
Time Out	Enter the time in seconds. The valid range is from 1 to 60 seconds.

Related Topics

Identified Endpoints, on page 833
Import Endpoints from LDAP Server, on page 831

Endpoint Profiling Policies Settings

The following table describes the fields in the **Endpoint Policies** window. To view this window, click the **Menu** icon (☰) and choose **Policy** > **Profiling** > **Profiling Policies**.

Table 122: Endpoint Profiling Policies Settings

Field Name	Usage Guidelines
Name	Enter the name of the endpoint profiling policy that you want to create.

Field Name	Usage Guidelines
Description	Enter the description of the endpoint profiling policy that you want to create.
Policy Enabled	By default, the **Policy Enabled** check box is checked to associate a matching profiling policy when you profile an endpoint. When unchecked, the endpoint profiling policy is excluded when you profile an endpoint.
Minimum Certainty Factor	Enter the minimum value that you want to associate with the profiling policy. The default value is 10.
Exception Action	Choose an exception action, which you want to associate with the conditions when defining a rule in the profiling policy. The default is NONE. The exception actions are defined in the following location: **Policy** > **Policy Elements** > **Results** > **Profiling** > **Exception Actions**.
Network Scan (NMAP) Action	Choose a network scan action from the list, which you want to associate with the conditions when defining a rule in the profiling policy, if required. The default is NONE. The exception actions are defined in the following location: **Policy** > **Policy Elements** > **Results** > **Profiling** > **Network Scan (NMAP) Actions**.
Create an Identity Group for the policy	Check one of the following options to create an endpoint identity group: • **Yes, create matching Identity Group** • **No, use existing Identity Group hierarchy**
Yes, create matching Identity Group	Choose this option to use an existing profiling policy. This option creates a matching identity group for those endpoints and the identity group will be the child of the Profiled endpoint identity group when an endpoint profile matches an existing profiling policy. For example, the Xerox-Device endpoint identity group is created in the Endpoints Identity Groups page when endpoints discovered on your network match the Xerox-Device profile.

Field Name	Usage Guidelines
No, use existing Identity Group hierarchy	Check this check box to assign endpoints to the matching parent endpoint identity group using hierarchical construction of profiling policies and identity groups. This option allows you to make use of the endpoint profiling policies hierarchy to assign endpoints to one of the matching parent endpoint identity groups, as well as to the associated endpoint identity groups to the parent identity group. For example, endpoints that match an existing profile are grouped under the appropriate parent endpoint identity group. Here, endpoints that match the Unknown profile are grouped under Unknown, and endpoints that match an existing profile are grouped under the Profiled endpoint identity group. For example, • If endpoints match the Cisco-IP-Phone profile, then they are grouped under the Cisco-IP-Phone endpoint identity group. • If endpoints match the Workstation profile, then they are grouped under the Workstation endpoint identity group. The Cisco-IP-Phone and Workstation endpoint identity groups are associated to the Profiled endpoint identity group in the system.
Parent Policy	Choose a parent profiling policy that are defined in the system to which you want to associate the new endpoint profiling policy. You can choose a parent profiling policy from which you can inherit rules and conditions to its child.
Associated CoA Type	Choose one of the following CoA types that you want to associate with the endpoint profiling policy: • No CoA • Port Bounce • Reauth • Global Settings that is applied from the profiler configuration set in Administration > System > Settings > Profiling
Rules	One or more rules that are defined in endpoint profiling policies determine the matching profiling policy for endpoints, which allows you to group endpoints according to their profiles. One or more profiling conditions from the policy elements library are used in rules for validating endpoint attributes and their values for the overall classification.

Field Name	Usage Guidelines
Conditions	Click the plus [+] sign to expand the Conditions anchored overlay, and click the minus [-] sign, or click outside the anchored overlay to close it. Click **Select Existing Condition from Library** or **Create New Condition (Advanced Option)** . **Select Existing Condition from Library**: You can define an expression by selecting Cisco predefined conditions from the policy elements library. **Create New Condition (Advanced Option)**: You can define an expression by selecting attributes from various system or user-defined dictionaries. You can associate one of the following with the profiling conditions: • An integer value for the certainty factor for each condition • Either an exception action or a network scan action for that condition Choose one of the following predefined settings to associate with the profiling condition: • Certainty Factor Increases: Enter the certainty value for each rule, which can be added for all the matching rules with respect to the overall classification. • Take Exception Action: Triggers an exception action that is configured in the Exception Action field for this endpoint profiling policy. • Take Network Scan Action: Triggers a network scan action that is configured in the Network Scan (NMAP) Action field for this endpoint profiling policy.

Select Existing Condition from Library	You can do the following:
	• You can choose Cisco predefined conditions that are available in the policy elements library, and then use an AND or OR operator to add multiple conditions.
	• Click the Action icon to do the following in the subsequent steps:
	  • **Add Attribute or Value**: You can add ad-hoc attribute or value pairs
	  • **Add Condition from Library**: You can add Cisco predefined conditions
	  • **Duplicate**: Create a copy of the selected condition
	  • **Add Condition to Library**: You can save ad-hoc attribute/value pairs that you create to the policy elements library
	  • **Delete**: Delete the selected condition.

Field Name	Usage Guidelines

Create New Condition (Advance Option)	You can do the following:
	• You can add ad-hoc attribute/value pairs to your expression, and then use an AND or OR operator to add multiple conditions.
	• Click the Action icon to do the following in the subsequent steps:
	  • **Add Attribute or Value**: You can add ad-hoc attribute or value pairs
	  • **Add Condition from Library**: You can add Cisco predefined conditions
	  • **Duplicate**: Create a copy of the selected condition
	  • **Add Condition to Library**: You can save ad-hoc attribute/value pairs that you create to the policy elements library
	  • **Delete**: Delete the selected condition. You can use the AND or OR operator

Related Topics

Cisco ISE Profiling Service, on page 775
Create Endpoint Profiling Policies, on page 819
Endpoint Context Visibility Using UDID Attribute, on page 851

Endpoint Context Visibility Using UDID Attribute

The Unique Identifier (UDID) is an endpoint attribute that identifies MAC addresses of a particular endpoint. An endpoint can have multiple MAC addresses. For example, one MAC address for the wired interface and another for the wireless interface. The AnyConnect agent generates a UDID for that endpoint, and saves it as an endpoint attribute. You can use the UDID in authorization query. The UDID remains constant for an endpoint; the UDID does not change with the AnyConnect installation or uninstallation. When using UDID, **Context Visibility** window (**Context Visibility** > **Endpoints** > **Compliance**) displays one entry instead of multiple entries for endpoints with multiple NICs. You can ensure posture control on a specific endpoint rather than on a Mac address.

Note The endpoint must have AnyConnect 4.7 or higher to create the UDID.

Endpoint Scripts Wizard for Windows and MacOS Endpoints

The Endpoint Scripts Wizard allows you to run scripts on connected endpoints to carry out administrative tasks that comply with your organization's requirements. This includes tasks like uninstalling obsolete software, starting or terminating processes or applications, and enabling or disabling specific services.

Endpoint scripts can be run on Windows and MacOS endpoints through the Endpoint Scripts Wizard.

Before you begin

- You must have the user role of Super Admin.

- Configure login credentials for Cisco ISE to access MacOS and Windows endpoints with administrative privileges.

  In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Protocols** > **Endpoint Login Configuration**, and configure the following:

  - Domain credentials with which Cisco ISE can log into endpoints.
  - Local user credentials for Windows and MacOS with which Cisco ISE can log into the endpoints as a local user.

    Domain user has precedence over local user. If you have configured both, and need to run a script with local user credentials, you must remove domain credentials.

- Windows endpoints must have Windows PowerShell version 5.1 or later installed. PowerShell remoting must be enabled.
- MacOS endpoints must have Bash installed.
- Both Windows and MacOS endpoints must have cURL version 7.34 or later installed.
- The Windows and MacOS endpoints must be connected to a network and have active sessions in Cisco ISE.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Context Visibility** > **Endpoints**

Step 2 Click the link icon in the top-right corner of the window, and choose **Run Endpoint Scripts** from the drop-down list.

The **Welcome** tab contains a link to the **Endpoint Login Configuration** window to configure login credentials, if this is not already done. You can click the **Start** button at the bottom-right corner of this tab only when login credentials are configured.

Step 3 In the **Select Category** tab, you can select endpoints based either on their operating systems, or the applications available on them. Click the radio button for **By OS** or **By Application** to make your choice. Click **Next** to continue.

Step 4 In the **Select Endpoints** window, a dashlet displays the filters available for OS type, or application, as applicable. In the dashlet, click the filter you wish to apply, and all the endpoints for that filter are listed in a table.

- To select all the endpoints for the chosen filter, check the checkbox in the title row of the table.
- To select specific endpoints, check the check box for that entry in the table. To find a specific endpoint from the table, click the **Filter** button above the table and choose **Quick Filter**. You can filter by any of the parameters displayed to find the required endpoints.

Note If you chose **By Application** in the **Select Categories** step, remember to select endpoints belonging to the same OS type in this step. In the case of application-based scripts, create a script for each OS type and set up a separate job for each OS type on the Endpoints Scripts Wizard.

Step 5 Click **Next** after choosing the endpoints on which to run a script.

Step 6 In the **Select Scripts** tab, click **Add**.

Step 7 Click **Add Script** to choose the script from your system. Click **Start Upload** to add the script to the **Select Scripts** tab.

Step 8 Check the check box for the script you wish to run and click **Next**.

Step 9 The **Summary** tab displays the endpoints selected and the script chosen. Review the selection here and click **Back** to change any details. Click **Finish** to initiate running the scripts.

A pop-up window named **Endpoints Script Report** is displayed, with the **Job ID** of this task. Click **Endpoint Scripts provisioning report** to be redirected to the window with the details of this task.

To view the reports of jobs run through the Endpoints Scripts Wizard, choose **Operations** > **Reports** > **Reports** > **Endpoints and Users** > **Endpoint Scripts Provisioning Summary**.

Endpoint Scripts Provisioning Summary Report

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Reports** > **Endpoints and Users** > **Endpoint Scripts Provisioning Summary**

The Endpoint Scripts Provisioning Summary window displays details of jobs run through the Endpoint Scripts Wizard, over the last 30 days. Click **Schedule** in the top-right corner of the window to schedule exporting reports and keep track of older reports.

Click **Export To** and choose an option from the drop-down list to save a CSV or PDF version of the report to a repository or a local destination.

The **Endpoint Scripts Provisioning Summary** window displays a table with the following columns by default:

Name of Column	**Information Displayed**
Logged At	Time stamp of submission of job.
Job ID	Click the Job ID entry to view details of this entry. A new tab open with **Endpoint Scripts Provisioning Details**, with timestamp, MAC addresses of the endpoints selected, script status and provisioning status of the script for each of the endpoints, name of PSN provisioning the job, and the Job ID. **Note** **Note**: Click the MAC address for granular step-by-step details of the script run.
Admin Name	Name of administrator who submitted the job.
Operating System	Operating system for which the selected script was run.
Total/ Success /Failed/In-Progress Endpoints	• Total number of endpoints selected. • Number of endpoints on which the script ran successfully. • Number of endpoints on which the script failed to run. • Number of endpoints on which the script is still running.
Script Name	Name of the script included in the job.

Agent Download Issues on Client Machine

Problem

The client machine browser displays a “no policy matched” error message after user authentication and authorization. This issue applies to user sessions during the client provisioning phase of authentication.

Possible Causes

The client provisioning policy is missing required settings.

Posture Agent Download Issues

Remember that downloading the posture agent installer requires the following:

- The user must allow the ActiveX installer in the browser session the first time an agent is installed on the client machine. The client provisioning download page prompts for this.
- The client machine must have Internet access.

Resolution

- Ensure that a client provisioning policy exists in Cisco ISE. If yes, verify the policy identity group, conditions, and type of agent defined in the policy. Also ensure whether or not there is any agent profile configured under **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources** > **Add** > **AnyConnect Posture Profile**, even a profile with all default values.
- Try re-authenticating the client machine by bouncing the port on the access switch.

Endpoints

These windows enable you to configure and manage endpoints that connect to your network.

Endpoint Settings

The following table describes the fields on the **Endpoints** window, which you can use to create endpoints and assign policies for endpoints. To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Identities** > **Endpoints**.

Table 123: Endpoint Settings

Field Name	Usage Guidelines
MAC Address	Enter the MAC address in hexadecimal format to create an endpoint statically. The MAC address is the device identifier for the interface that is connected to the Cisco ISE enabled network.

Field Name	Usage Guidelines
Static Assignment	Check this check box when you want to create an endpoint statically in the Endpoints window and the status of static assignment is set to static. You can toggle the status of static assignment of an endpoint from static to dynamic or from dynamic to static.
Policy Assignment	(Disabled by default unless the **Static Assignment** is checked) Choose a matching endpoint policy from the **Policy Assignment** drop-down list. You can do one of the following: • If you do not choose a matching endpoint policy, but use the default endpoint policy Unknown, then the static assignment status is set to dynamic for the endpoint that allows dynamic profiling of an endpoint. • If you choose a matching endpoint policy other than Unknown, then the static assignment status is set to static for that endpoint and the **Static Assignment** check box is automatically checked.
Static Group Assignment	Check this check box when you want to assign an endpoint to an identity group statically. In you check this check box, the profiling service does not change the endpoint identity group the next time during evaluation of the endpoint policy for these endpoints, which were previously assigned dynamically to other endpoint identity groups. If you uncheck this check box, then the endpoint identity group is dynamic as assigned by the ISE profiler based on policy configuration. If you do not choose the Static Group Assignment option, then the endpoint is automatically assigned to the matching identity group the next time during evaluation of the endpoint policy.

Identity Group Assignment	Choose an endpoint identity group to which you want to assign the endpoint.
	You can assign an endpoint to an identity group when you create an endpoint statically, or when you do not want to use the **Create Matching Identity Group** option during evaluation of the endpoint policy for an endpoint.
	Cisco ISE includes the following system created endpoint identity groups:
	• Blocked List
	• GuestEndpoints
	• Profiled
	  • Cisco IP-Phone
	  • Workstation
	• RegisteredDevices
	• Unknown

Active Directory user endpoints that repeatedly fail RADIUS authentication for the same reason will be automatically rejected for a certain period, to avoid unnecessary processing by Cisco ISE and to protect against potential denial of service attacks.

To view a list of rejected endpoints, choose **Operations** > **Reports** > **Rejected Endpoints**. The data for this report will be available and displayed only when Advantage License is installed.

Note AD user endpoints that fail RADIUS authentication with the following two error messages are not rejected:

22063 - WRONG_PASSWORD

24408 - ACTIVE_DIRECTORY_USER_WRONG_PASSWORD

Related Topics

Identified Endpoints, on page 833
Create Endpoints with Static Assignments of Policies and Identity Groups, on page 828

Endpoint Import from LDAP Settings

The following table describes the fields on the Import from LDAP window, which you can use to import endpoints from an LDAP server. To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Identities** > **Endpoints**.

Table 124: Endpoint Import from LDAP Settings

Field Name	Usage Guidelines
Connection Settings	
Host	Enter the hostname, or the IP address of the LDAP server.
Port	Enter the port number of the LDAP server. You can use the default port 389 to import from an LDAP server, and the default port 636 to import from an LDAP server over SSL. **Note** Cisco ISE supports any configured port number. The configured value should match the LDAP server connection details.
Enable Secure Connection	Check the **Enable Secure Connection** check box to import from an LDAP server over SSL.
Root CA Certificate Name	Click the drop-down arrow to view the trusted CA certificates. The Root CA Certificate Name refers to the trusted CA certificate that is required to connect to an LDAP server. You can add (import), edit, delete, and export trusted CA certificates in Cisco ISE.
Anonymous Bind	You must enable either the **Anonymous Bind** check box, or enter the LDAP administrator credentials from the slapd.conf configuration file.

Field Name	Usage Guidelines
Admin DN	Enter the distinguished name (DN) configured for the LDAP administrator in the slapd.conf configuration file. Admin DN format example: cn=Admin, dc=cisco.com, dc=com
Password	Enter the password configured for the LDAP administrator in the slapd.conf configuration file.
Base DN	Enter the distinguished name of the parent entry. Base DN format example: dc=cisco.com, dc=com.
Query Settings	
MAC Address objectClass	Enter the query filter, which is used for importing the MAC address, for example, ieee802Device.
MAC Address Attribute Name	Enter the returned attribute name for import, for example, macAddress.
Profile Attribute Name	Enter the name of the LDAP attribute. This attribute holds the policy name for each endpoint entry that is defined in the LDAP server. When you configure the **Profile Attribute Name** field, consider the following: • If you do not specify this LDAP attribute in the **Profile Attribute Name** field or configure this attribute incorrectly, then endpoints are marked “Unknown” during an import operation, and these endpoints are profiled separately to the matching endpoint profiling policies. • If you configure this LDAP attribute in the **Profile Attribute Name** field, the attribute values are validated to ensure that the endpoint policy matches with an existing policy in Cisco ISE, and endpoints are imported. If the endpoint policy does not match with an existing policy, then those endpoints will not be imported.
Time Out	Enter the time in seconds. The valid range is from 1 to 60 seconds.

Related Topics

Identified Endpoints, on page 833

Import Endpoints from LDAP Server, on page 831

Endpoint Profiling Policies Settings

The following table describes the fields in the **Endpoint Policies** window. To view this window, click the **Menu** icon (☰) and choose **Policy** > **Profiling** > **Profiling Policies**.

Table 125: Endpoint Profiling Policies Settings

Field Name	Usage Guidelines
Name	Enter the name of the endpoint profiling policy that you want to create.

Field Name	Usage Guidelines
Description	Enter the description of the endpoint profiling policy that you want to create.
Policy Enabled	By default, the **Policy Enabled** check box is checked to associate a matching profiling policy when you profile an endpoint. When unchecked, the endpoint profiling policy is excluded when you profile an endpoint.
Minimum Certainty Factor	Enter the minimum value that you want to associate with the profiling policy. The default value is 10.
Exception Action	Choose an exception action, which you want to associate with the conditions when defining a rule in the profiling policy. The default is NONE. The exception actions are defined in the following location: **Policy** > **Policy Elements** > **Results** > **Profiling** > **Exception Actions**.
Network Scan (NMAP) Action	Choose a network scan action from the list, which you want to associate with the conditions when defining a rule in the profiling policy, if required. The default is NONE. The exception actions are defined in the following location: **Policy** > **Policy Elements** > **Results** > **Profiling** > **Network Scan (NMAP) Actions**.
Create an Identity Group for the policy	Check one of the following options to create an endpoint identity group: • **Yes, create matching Identity Group** • **No, use existing Identity Group hierarchy**
Yes, create matching Identity Group	Choose this option to use an existing profiling policy. This option creates a matching identity group for those endpoints and the identity group will be the child of the Profiled endpoint identity group when an endpoint profile matches an existing profiling policy. For example, the Xerox-Device endpoint identity group is created in the Endpoints Identity Groups page when endpoints discovered on your network match the Xerox-Device profile.

Field Name	Usage Guidelines
No, use existing Identity Group hierarchy	Check this check box to assign endpoints to the matching parent endpoint identity group using hierarchical construction of profiling policies and identity groups. This option allows you to make use of the endpoint profiling policies hierarchy to assign endpoints to one of the matching parent endpoint identity groups, as well as to the associated endpoint identity groups to the parent identity group. For example, endpoints that match an existing profile are grouped under the appropriate parent endpoint identity group. Here, endpoints that match the Unknown profile are grouped under Unknown, and endpoints that match an existing profile are grouped under the Profiled endpoint identity group. For example, • If endpoints match the Cisco-IP-Phone profile, then they are grouped under the Cisco-IP-Phone endpoint identity group. • If endpoints match the Workstation profile, then they are grouped under the Workstation endpoint identity group. The Cisco-IP-Phone and Workstation endpoint identity groups are associated to the Profiled endpoint identity group in the system.
Parent Policy	Choose a parent profiling policy that are defined in the system to which you want to associate the new endpoint profiling policy. You can choose a parent profiling policy from which you can inherit rules and conditions to its child.
Associated CoA Type	Choose one of the following CoA types that you want to associate with the endpoint profiling policy: • No CoA • Port Bounce • Reauth • Global Settings that is applied from the profiler configuration set in Administration > System > Settings > Profiling
Rules	One or more rules that are defined in endpoint profiling policies determine the matching profiling policy for endpoints, which allows you to group endpoints according to their profiles. One or more profiling conditions from the policy elements library are used in rules for validating endpoint attributes and their values for the overall classification.

Field Name	Usage Guidelines
Conditions	Click the plus [+] sign to expand the Conditions anchored overlay, and click the minus [-] sign, or click outside the anchored overlay to close it. Click **Select Existing Condition from Library** or **Create New Condition (Advanced Option)** . **Select Existing Condition from Library**: You can define an expression by selecting Cisco predefined conditions from the policy elements library. **Create New Condition (Advanced Option)**: You can define an expression by selecting attributes from various system or user-defined dictionaries. You can associate one of the following with the profiling conditions: • An integer value for the certainty factor for each condition • Either an exception action or a network scan action for that condition Choose one of the following predefined settings to associate with the profiling condition: • Certainty Factor Increases: Enter the certainty value for each rule, which can be added for all the matching rules with respect to the overall classification. • Take Exception Action: Triggers an exception action that is configured in the Exception Action field for this endpoint profiling policy. • Take Network Scan Action: Triggers a network scan action that is configured in the Network Scan (NMAP) Action field for this endpoint profiling policy.

Select Existing Condition from Library	You can do the following:
	• You can choose Cisco predefined conditions that are available in the policy elements library, and then use an AND or OR operator to add multiple conditions.
	• Click the Action icon to do the following in the subsequent steps:
	  • **Add Attribute or Value**: You can add ad-hoc attribute or value pairs
	  • **Add Condition from Library**: You can add Cisco predefined conditions
	  • **Duplicate**: Create a copy of the selected condition
	  • **Add Condition to Library**: You can save ad-hoc attribute/value pairs that you create to the policy elements library
	  • **Delete**: Delete the selected condition.

Field Name	Usage Guidelines

Create New Condition (Advance Option)	You can do the following:
	• You can add ad-hoc attribute/value pairs to your expression, and then use an AND or OR operator to add multiple conditions.
	• Click the Action icon to do the following in the subsequent steps:
	  • **Add Attribute or Value**: You can add ad-hoc attribute or value pairs
	  • **Add Condition from Library**: You can add Cisco predefined conditions
	  • **Duplicate**: Create a copy of the selected condition
	  • **Add Condition to Library**: You can save ad-hoc attribute/value pairs that you create to the policy elements library
	  • **Delete**: Delete the selected condition. You can use the AND or OR operator

Related Topics

Cisco ISE Profiling Service, on page 775
Create Endpoint Profiling Policies, on page 819
Endpoint Context Visibility Using UDID Attribute, on page 851

Endpoint Context Visibility Using UDID Attribute

The Unique Identifier (UDID) is an endpoint attribute that identifies MAC addresses of a particular endpoint. An endpoint can have multiple MAC addresses. For example, one MAC address for the wired interface and another for the wireless interface. The AnyConnect agent generates a UDID for that endpoint, and saves it as an endpoint attribute. You can use the UDID in authorization query. The UDID remains constant for an endpoint; the UDID does not change with the AnyConnect installation or uninstallation. When using UDID, **Context Visibility** window (**Context Visibility** > **Endpoints** > **Compliance**) displays one entry instead of multiple entries for endpoints with multiple NICs. You can ensure posture control on a specific endpoint rather than on a Mac address.

Note The endpoint must have AnyConnect 4.7 or higher to create the UDID.

Endpoint Scripts Wizard for Windows and MacOS Endpoints

The Endpoint Scripts Wizard allows you to run scripts on connected endpoints to carry out administrative tasks that comply with your organization’s requirements. This includes tasks like uninstalling obsolete software, starting or terminating processes or applications, and enabling or disabling specific services.

Endpoint scripts can be run on Windows and MacOS endpoints through the Endpoint Scripts Wizard.

Before you begin

- You must have the user role of Super Admin.

- Configure login credentials for Cisco ISE to access MacOS and Windows endpoints with administrative privileges.

  In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Protocols** > **Endpoint Login Configuration**, and configure the following:

  - Domain credentials with which Cisco ISE can log into endpoints.
  - Local user credentials for Windows and MacOS with which Cisco ISE can log into the endpoints as a local user.

    Domain user has precedence over local user. If you have configured both, and need to run a script with local user credentials, you must remove domain credentials.

- Windows endpoints must have Windows PowerShell version 5.1 or later installed. PowerShell remoting must be enabled.
- MacOS endpoints must have Bash installed.
- Both Windows and MacOS endpoints must have cURL version 7.34 or later installed.
- The Windows and MacOS endpoints must be connected to a network and have active sessions in Cisco ISE.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Context Visibility** > **Endpoints**

Step 2 Click the link icon in the top-right corner of the window, and choose **Run Endpoint Scripts** from the drop-down list.

The **Welcome** tab contains a link to the **Endpoint Login Configuration** window to configure login credentials, if this is not already done. You can click the **Start** button at the bottom-right corner of this tab only when login credentials are configured.

Step 3 In the **Select Category** tab, you can select endpoints based either on their operating systems, or the applications available on them. Click the radio button for **By OS** or **By Application** to make your choice. Click **Next** to continue.

Step 4 In the **Select Endpoints** window, a dashlet displays the filters available for OS type, or application, as applicable. In the dashlet, click the filter you wish to apply, and all the endpoints for that filter are listed in a table.

- To select all the endpoints for the chosen filter, check the checkbox in the title row of the table.
- To select specific endpoints, check the check box for that entry in the table. To find a specific endpoint from the table, click the **Filter** button above the table and choose **Quick Filter**. You can filter by any of the parameters displayed to find the required endpoints.

Note If you chose **By Application** in the **Select Categories** step, remember to select endpoints belonging to the same OS type in this step. In the case of application-based scripts, create a script for each OS type and set up a separate job for each OS type on the Endpoints Scripts Wizard.

Step 5 Click **Next** after choosing the endpoints on which to run a script.

Step 6 In the **Select Scripts** tab, click **Add**.

Step 7 Click **Add Script** to choose the script from your system. Click **Start Upload** to add the script to the **Select Scripts** tab.

Step 8 Check the check box for the script you wish to run and click **Next**.

Step 9 The **Summary** tab displays the endpoints selected and the script chosen. Review the selection here and click **Back** to change any details. Click **Finish** to initiate running the scripts.

A pop-up window named **Endpoints Script Report** is displayed, with the **Job ID** of this task. Click **Endpoint Scripts provisioning report** to be redirected to the window with the details of this task.

To view the reports of jobs run through the Endpoints Scripts Wizard, choose **Operations** > **Reports** > **Reports** > **Endpoints and Users** > **Endpoint Scripts Provisioning Summary**.

Endpoint Scripts Provisioning Summary Report

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Reports** > **Endpoints and Users** > **Endpoint Scripts Provisioning Summary**

The Endpoint Scripts Provisioning Summary window displays details of jobs run through the Endpoint Scripts Wizard, over the last 30 days. Click **Schedule** in the top-right corner of the window to schedule exporting reports and keep track of older reports.

Click **Export To** and choose an option from the drop-down list to save a CSV or PDF version of the report to a repository or a local destination.

The **Endpoint Scripts Provisioning Summary** window displays a table with the following columns by default:

Name of Column	Information Displayed
Logged At	Time stamp of submission of job.
Job ID	Click the Job ID entry to view details of this entry. A new tab open with **Endpoint Scripts Provisioning Details**, with timestamp, MAC addresses of the endpoints selected, script status and provisioning status of the script for each of the endpoints, name of PSN provisioning the job, and the Job ID. **Note** **Note**: Click the MAC address for granular step-by-step details of the script run.
Admin Name	Name of administrator who submitted the job.
Operating System	Operating system for which the selected script was run.
Total/ Success /Failed/In-Progress Endpoints	• Total number of endpoints selected. • Number of endpoints on which the script ran successfully. • Number of endpoints on which the script failed to run. • Number of endpoints on which the script is still running.
Script Name	Name of the script included in the job.

IF-MIB

Object	OID
ifIndex	1.3.6.1.2.1.2.2.1.1
ifDescr	1.3.6.1.2.1.2.2.1.2
ifType	1.3.6.1.2.1.2.2.1.3
ifSpeed	1.3.6.1.2.1.2.2.1.5
ifPhysAddress	1.3.6.1.2.1.2.2.1.6
ifAdminStatus	1.3.6.1.2.1.2.2.1.7
ifOperStatus	1.3.6.1.2.1.2.2.1.8

SNMPv2-MIB

Object	OID
system	1.3.6.1.2.1.1
sysDescr	1.3.6.1.2.1.1.1.0
sysObjectID	1.3.6.1.2.1.1.2.0
sysUpTime	1.3.6.1.2.1.1.3.0
sysContact	1.3.6.1.2.1.1.4.0
sysName	1.3.6.1.2.1.1.5.0
sysLocation	1.3.6.1.2.1.1.6.0
sysServices	1.3.6.1.2.1.1.7.0
sysORLastChange	1.3.6.1.2.1.1.8.0
sysORTable	1.3.6.1.2.1.1.9.0

IP-MIB

Object	OID
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3

Object	OID
ipNetToMediaPhysAddress	1.3.6.1.2.1.4.22.1.2
ipNetToPhysicalPhysAddress	1.3.6.1.2.1.4.35.1.4

CISCO-CDP-MIB

Object	OID
cdpCacheEntry	1.3.6.1.4.1.9.9.23.1.2.1.1
cdpCacheIfIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.1
cdpCacheDeviceIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.2
cdpCacheAddressType	1.3.6.1.4.1.9.9.23.1.2.1.1.3
cdpCacheAddress	1.3.6.1.4.1.9.9.23.1.2.1.1.4
cdpCacheVersion	1.3.6.1.4.1.9.9.23.1.2.1.1.5
cdpCacheDeviceId	1.3.6.1.4.1.9.9.23.1.2.1.1.6
cdpCacheDevicePort	1.3.6.1.4.1.9.9.23.1.2.1.1.7
cdpCachePlatform	1.3.6.1.4.1.9.9.23.1.2.1.1.8
cdpCacheCapabilities	1.3.6.1.4.1.9.9.23.1.2.1.1.9
cdpCacheVTPMgmtDomain	1.3.6.1.4.1.9.9.23.1.2.1.1.10
cdpCacheNativeVLAN	1.3.6.1.4.1.9.9.23.1.2.1.1.11
cdpCacheDuplex	1.3.6.1.4.1.9.9.23.1.2.1.1.12
cdpCacheApplianceID	1.3.6.1.4.1.9.9.23.1.2.1.1.13
cdpCacheVlanID	1.3.6.1.4.1.9.9.23.1.2.1.1.14
cdpCachePowerConsumption	1.3.6.1.4.1.9.9.23.1.2.1.1.15
cdpCacheMTU	1.3.6.1.4.1.9.9.23.1.2.1.1.16
cdpCacheSysName	1.3.6.1.4.1.9.9.23.1.2.1.1.17
cdpCacheSysObjectID	1.3.6.1.4.1.9.9.23.1.2.1.1.18
cdpCachePrimaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.19
cdpCachePrimaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.20
cdpCacheSecondaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.21

Object	OID
cdpCacheSecondaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.22
cdpCachePhysLocation	1.3.6.1.4.1.9.9.23.1.2.1.1.23
cdpCacheLastChange	1.3.6.1.4.1.9.9.23.1.2.1.1.24

CISCO-VTP-MIB

Object	OID
vtpVlanIfIndex	1.3.6.1.4.1.9.9.46.1.3.1.1.18.1
vtpVlanName	1.3.6.1.4.1.9.9.46.1.3.1.1.4.1
vtpVlanState	1.3.6.1.4.1.9.9.46.1.3.1.1.2.1

CISCO-STACK-MIB

Object	OID
portIfIndex	1.3.6.1.4.1.9.5.1.4.1.1.11
vlanPortVlan	1.3.6.1.4.1.9.5.1.9.3.1.3.1

BRIDGE-MIB

Object	OID
dot1dTpFdbPort	1.3.6.1.2.1.17.4.3.1.2
dot1dBasePortIfIndex	1.3.6.1.2.1.17.1.4.1.2

OLD-CISCO-INTERFACE-MIB

Object	OID
locIfReason	1.3.6.1.4.1.9.2.2.1.1.20

CISCO-LWAPP-AP-MIB

Object	OID
cLApEntry	1.3.6.1.4.1.9.9.513.1.1.1
cLApSysMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.1
cLApIfMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.2
cLApMaxNumberOfDot11Slots	1.3.6.1.4.1.9.9.513.1.1.1.1.3
cLApEntPhysicalIndex	1.3.6.1.4.1.9.9.513.1.1.1.1.4
cLApName	1.3.6.1.4.1.9.9.513.1.1.1.1.5
cLApUpTime	1.3.6.1.4.1.9.9.513.1.1.1.1.6
cLLwappUpTime	1.3.6.1.4.1.9.9.513.1.1.1.1.7
cLLwappJoinTakenTime	1.3.6.1.4.1.9.9.513.1.1.1.1.8
cLApMaxNumberOfEthernetSlots	1.3.6.1.4.1.9.9.513.1.1.1.1.9
cLApPrimaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.10
cLApPrimaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.11
cLApSecondaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.12
cLApSecondaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.13
cLApTertiaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.14
cLApTertiaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.15
cLApLastRebootReason	1.3.6.1.4.1.9.9.513.1.1.1.1.16
cLApEncryptionEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.17
cLApFailoverPriority	1.3.6.1.4.1.9.9.513.1.1.1.1.18
cLApPowerStatus	1.3.6.1.4.1.9.9.513.1.1.1.1.19
cLApTelnetEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.20
cLApSshEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.21
cLApPreStdStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.22
cLApPwrInjectorStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.23
cLApPwrInjectorSelection	1.3.6.1.4.1.9.9.513.1.1.1.1.24
cLApPwrInjectorSwMacAddr	1.3.6.1.4.1.9.9.513.1.1.1.1.25

Object	OID
cLApWipsEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.26
cLApMonitorModeOptimization	1.3.6.1.4.1.9.9.513.1.1.1.1.27
cLApDomainName	1.3.6.1.4.1.9.9.513.1.1.1.1.28
cLApNameServerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.29
cLApNameServerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.30
cLApAMSDUEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.31
cLApEncryptionSupported	1.3.6.1.4.1.9.9.513.1.1.1.1.32
cLApRogueDetectionEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.33

CISCO-LWAPP-DOT11-CLIENT-MIB

Object	OID
cldcClientEntry	1.3.6.1.4.1.9.9.599.1.3.1.1
cldcClientMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.1
cldcClientStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.2
cldcClientWlanProfileName	1.3.6.1.4.1.9.9.599.1.3.1.1.3
cldcClientWgbStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.4
cldcClientWgbMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.5
cldcClientProtocol	1.3.6.1.4.1.9.9.599.1.3.1.1.6
cldcAssociationMode	1.3.6.1.4.1.9.9.599.1.3.1.1.7
cldcApMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.8
cldcIfType	1.3.6.1.4.1.9.9.599.1.3.1.1.9
cldcClientIPAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.10
cldcClientNacState	1.3.6.1.4.1.9.9.599.1.3.1.1.11
cldcClientQuarantineVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.12
cldcClientAccessVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.13
cldcClientLoginTime	1.3.6.1.4.1.9.9.599.1.3.1.1.14
cldcClientUpTime	1.3.6.1.4.1.9.9.599.1.3.1.1.15

Object	OID
cldcClientPowerSaveMode	1.3.6.1.4.1.9.9.599.1.3.1.1.16
cldcClientCurrentTxRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.17
cldcClientDataRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.18

CISCO-AUTH-FRAMEWORK-MIB

Object	OID
cafPortConfigEntry	1.3.6.1.4.1.9.9.656.1.2.1.1
cafSessionClientMacAddress	1.3.6.1.4.1.9.9.656.1.4.1.1.2
cafSessionStatus	1.3.6.1.4.1.9.9.656.1.4.1.1.5
cafSessionDomain	1.3.6.1.4.1.9.9.656.1.4.1.1.6
cafSessionAuthUserName	1.3.6.1.4.1.9.9.656.1.4.1.1.10
cafSessionAuthorizedBy	1.3.6.1.4.1.9.9.656.1.4.1.1.12
cafSessionAuthVlan	1.3.6.1.4.1.9.9.656.1.4.1.1.14

EEE8021-PAE-MIB: RFC IEEE 802.1X

Object	OID
dot1xAuthAuthControlledPortStatus	1.0.8802.1.1.1.1.2.1.1.5
dot1xAuthAuthControlledPortControl	1.0.8802.1.1.1.1.2.1.1.6
dot1xAuthSessionUserName	1.0.8802.1.1.1.1.2.4.1.9

HOST-RESOURCES-MIB

Object	OID
hrDeviceDescr	1.3.6.1.2.1.25.3.2.1.3
hrDeviceStatus	1.3.6.1.2.1.25.3.2.1.5

LLDP-MIB

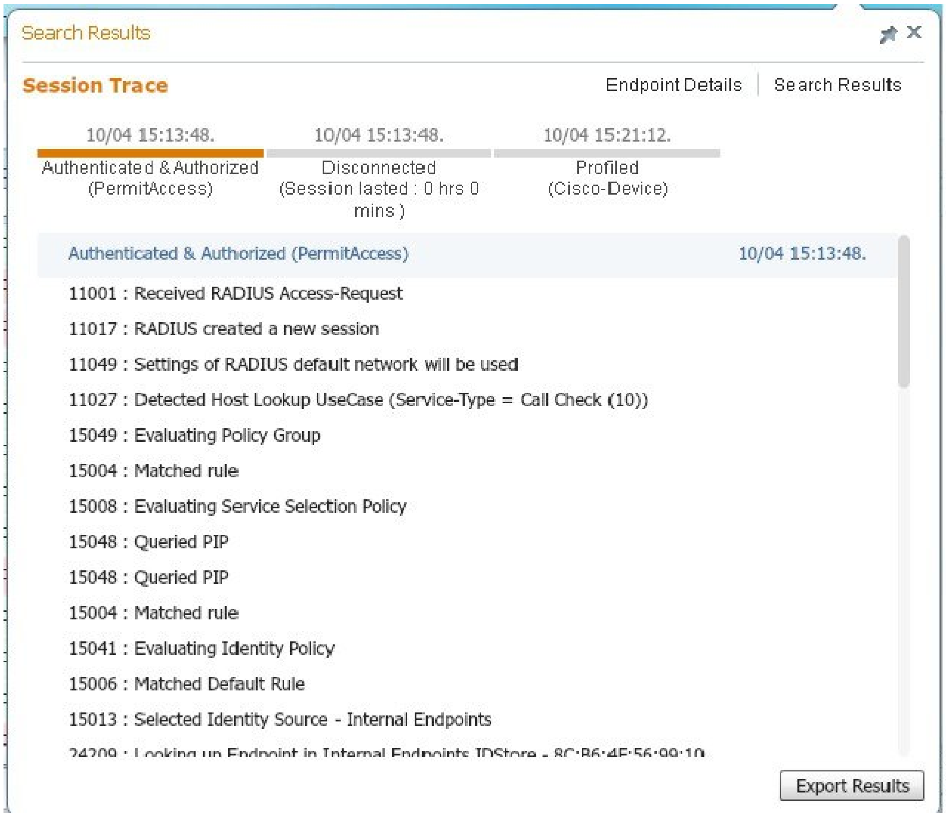
Object	OID
lldpEntry	1.0.8802.1.1.2.1.4.1.1
lldpTimeMark	1.0.8802.1.1.2.1.4.1.1.1
lldpLocalPortNum	1.0.8802.1.1.2.1.4.1.1.2
lldpIndex	1.0.8802.1.1.2.1.4.1.1.3
lldpChassisIdSubtype	1.0.8802.1.1.2.1.4.1.1.4
lldpChassisId	1.0.8802.1.1.2.1.4.1.1.5
lldpPortIdSubtype	1.0.8802.1.1.2.1.4.1.1.6
lldpPortId	1.0.8802.1.1.2.1.4.1.1.7
lldpPortDescription	1.0.8802.1.1.2.1.4.1.1.8
lldpSystemName	1.0.8802.1.1.2.1.4.1.1.9
lldpSystemDescription	1.0.8802.1.1.2.1.4.1.1.10
ldpCapabilitiesMapSupported	1.0.8802.1.1.2.1.4.1.1.11
lldpCacheCapabilities	1.0.8802.1.1.2.1.4.1.1.12

Session Trace for an Endpoint

You can use the global search box available at the top of the Cisco ISE home page to get session information for a particular endpoint. When you search with a criteria, you get a list of endpoints. Click on any of these endpoints to see the session trace information for that endpoint. The following figure shows an example of the session trace information displayed for an endpoint.

Note The dataset used for search is based on Endpoint ID as indexes. Therefore, when authentication occurs, it is mandatory to have Endpoint IDs for the endpoints for those authentications to include them in the search result set.

Figure 27: Session Trace of an Endpoint



10/04 15:13:48.	10/04 15:13:48.	10/04 15:21:12.
Authenticated & Authorized (PermitAccess)	Disconnected (Session lasted : 0 hrs 0 mins)	Profiled (Cisco-Device)

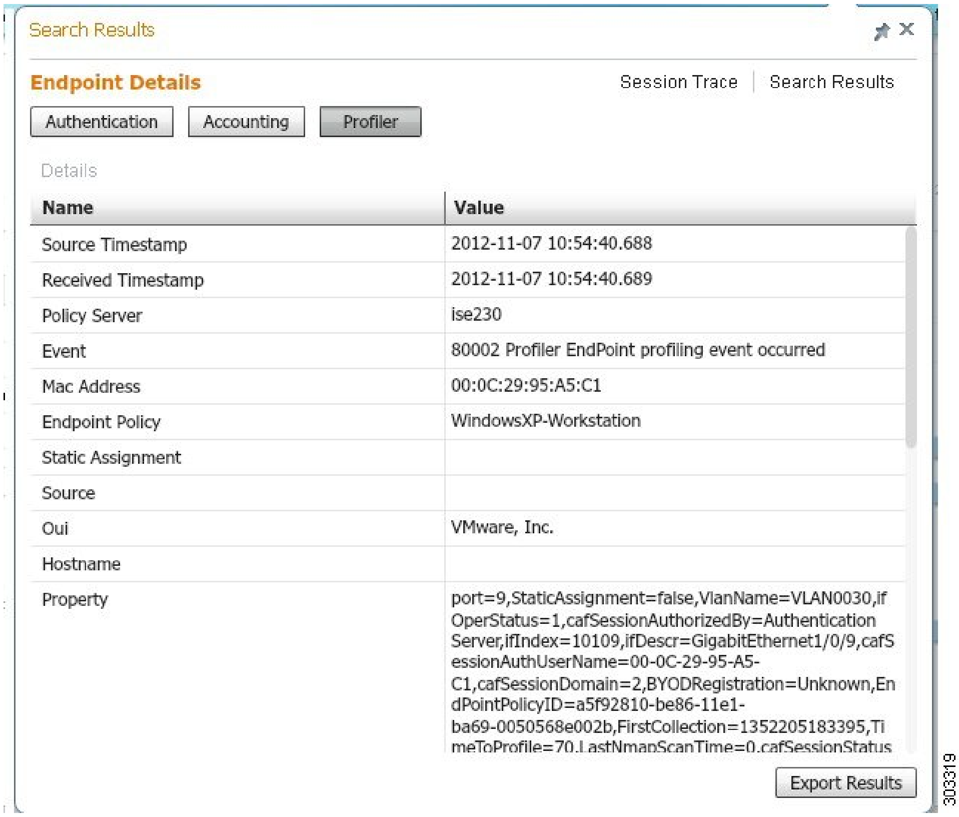
Authenticated & Authorized (PermitAccess) 10/04 15:13:48.

```
11001 : Received RADIUS Access-Request
11017 : RADIUS created a new session
11049 : Settings of RADIUS default network will be used
11027 : Detected Host Lookup UseCase (Service-Type = Call Check (10))
15049 : Evaluating Policy Group
15004 : Matched rule
15008 : Evaluating Service Selection Policy
15048 : Queried PIP
15048 : Queried PIP
15004 : Matched rule
15041 : Evaluating Identity Policy
15006 : Matched Default Rule
15013 : Selected Identity Source - Internal Endpoints
24209 : Looking up Endpoint in Internal Endpoints IDStore - 8C:B6:4F:56:99:10
```

You can use the clickable timeline at the top to see major authorization transitions. You can also export the results in .csv format by using the **Export Results** option. The report gets downloaded to your browser.

You can click the **Endpoint Details** link to see more authentication, accounting, and profiler information for a particular endpoint. The following figure shows an example of endpoint details information displayed for an endpoint.

Figure 28: Endpoint Details



Endpoint Details

Name	Value
Source Timestamp	2012-11-07 10:54:40.688
Received Timestamp	2012-11-07 10:54:40.689
Policy Server	ise230
Event	80002 Profiler EndPoint profiling event occurred
Mac Address	00:0C:29:95:A5:C1
Endpoint Policy	WindowsXP-Workstation
Static Assignment	
Source	
Oui	VMware, Inc.
Hostname	
Property	port=9,StaticAssignment=false,VlanName=VLAN0030,ifOperStatus=1,cafSessionAuthorizedBy=Authentication Server,ifIndex=10109,ifDescr=GigabitEthernet1/0/9,cafSessionAuthUserName=00-0C-29-95-A5-C1,cafSessionDomain=2,BYODRegistration=Unknown,EndPointPolicyID=a5f92810-be86-11e1-ba69-0050568e002b,FirstCollection=1352205183395,TimeToProfile=70,LastNmapScanTime=0,cafSessionStatus

Session Removal from the Directory

Sessions are cleaned from the session directory on the Monitoring and Troubleshooting node as follows:

- Terminated sessions are cleaned 15 minutes after termination.
- If there is authentication but no accounting, then such sessions are cleared after one hour.
- All inactive sessions are cleared after five days.

Global Search for Endpoints

You can use the global search box available at the top of the Cisco ISE home page to search for endpoints. You can use any of the following criteria to search for an endpoint:

- User name
- MAC Address
- IP Address
- Authorization Profile
- Endpoint Profile

- Failure Reason
- Identity Group
- Identity Store
- Network Device name
- Network Device Type
- Operating System
- Posture Status
- Location
- Security Group
- User Type

You should enter at least three characters for any of the search criteria in the Search field to display data.

Note If an endpoint has been authenticated by Cisco ISE, or its accounting update has been received, it can be found through the global search. Endpoints that have been manually added and are not authenticated by or accounted for in Cisco ISE will not show up in the search results.

The search result provides a detailed and at-a-glance information about the current status of the endpoint, which you can use for troubleshooting. Search results display only the top 25 entries. You can use filters to narrow down the results.

You can use any of the properties in the left panel to filter the results. You can also click on any endpoint to see more detailed information about the endpoint, such as:

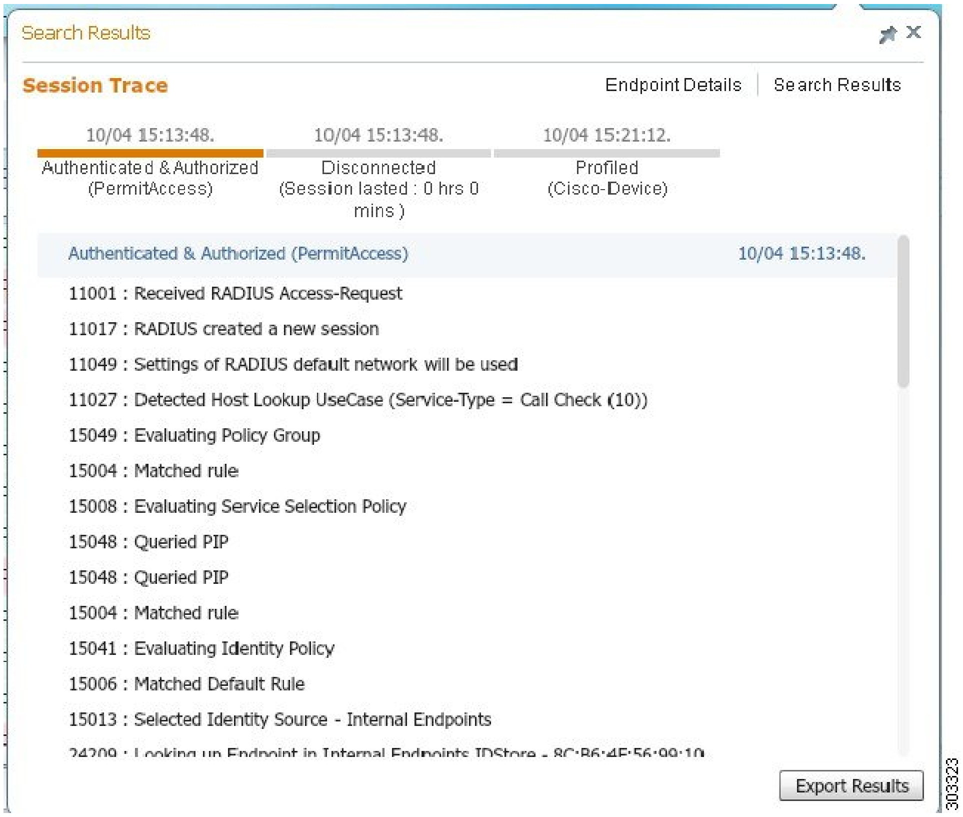
- Session trace
- Authentication details
- Accounting details
- Posture details
- Profiler details
- Client Provisioning details
- Guest accounting and activity

Session Trace for an Endpoint

You can use the global search box available at the top of the Cisco ISE home page to get session information for a particular endpoint. When you search with a criteria, you get a list of endpoints. Click on any of these endpoints to see the session trace information for that endpoint. The following figure shows an example of the session trace information displayed for an endpoint.

Note The dataset used for search is based on Endpoint ID as indexes. Therefore, when authentication occurs, it is mandatory to have Endpoint IDs for the endpoints for those authentications to include them in the search result set.

Figure 29: Session Trace of an Endpoint



10/04 15:13:48. Authenticated & Authorized (PermitAccess)
10/04 15:13:48. Disconnected (Session lasted : 0 hrs 0 mins)
10/04 15:21:12. Profiled (Cisco-Device)

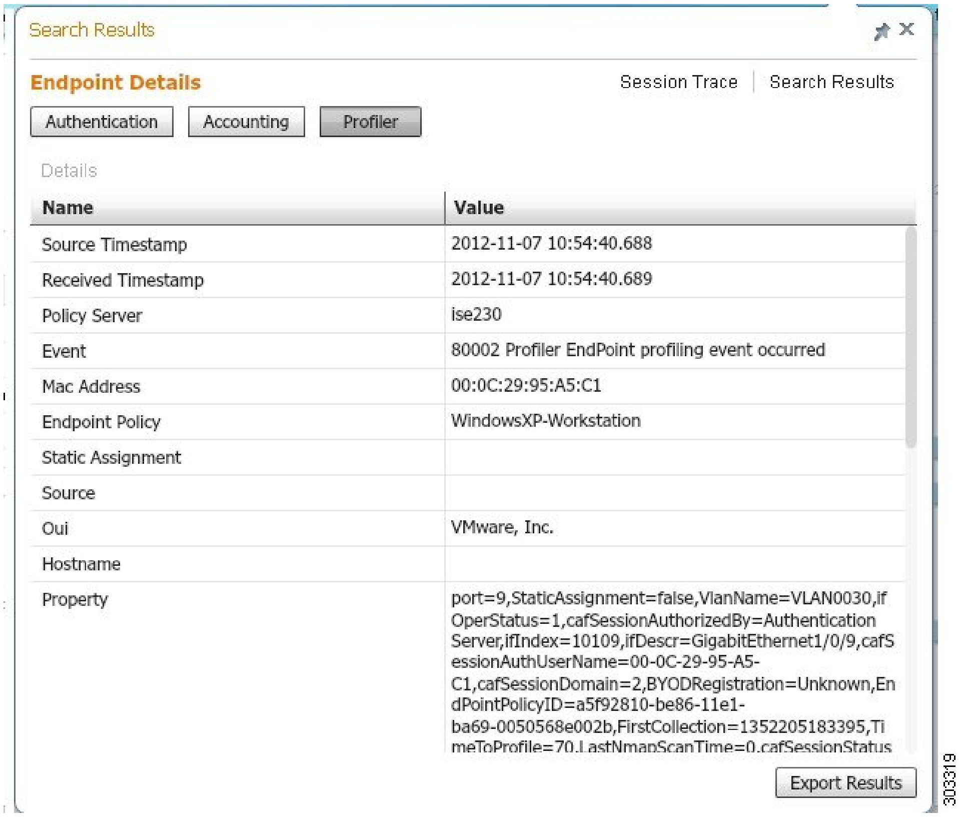
Authenticated & Authorized (PermitAccess) 10/04 15:13:48.

```
11001 : Received RADIUS Access-Request
11017 : RADIUS created a new session
11049 : Settings of RADIUS default network will be used
11027 : Detected Host Lookup UseCase (Service-Type = Call Check (10))
15049 : Evaluating Policy Group
15004 : Matched rule
15008 : Evaluating Service Selection Policy
15048 : Queried PIP
15048 : Queried PIP
15004 : Matched rule
15041 : Evaluating Identity Policy
15006 : Matched Default Rule
15013 : Selected Identity Source - Internal Endpoints
24209 : Looking up Endpoint in Internal Endpoints IDStore - 8C:B6:4F:56:99:10
```

You can use the clickable timeline at the top to see major authorization transitions. You can also export the results in .csv format by using the **Export Results** option. The report gets downloaded to your browser.

You can click the **Endpoint Details** link to see more authentication, accounting, and profiler information for a particular endpoint. The following figure shows an example of endpoint details information displayed for an endpoint.

Figure 30: Endpoint Details



Name	Value
Source Timestamp	2012-11-07 10:54:40.688
Received Timestamp	2012-11-07 10:54:40.689
Policy Server	ise230
Event	80002 Profiler EndPoint profiling event occurred
Mac Address	00:0C:29:95:A5:C1
Endpoint Policy	WindowsXP-Workstation
Static Assignment	
Source	
Oui	VMware, Inc.
Hostname	
Property	port=9,StaticAssignment=false,VlanName=VLAN0030,ifOperStatus=1,cafSessionAuthorizedBy=Authentication Server,ifIndex=10109,ifDescr=GigabitEthernet1/0/9,cafSessionAuthUserName=00-0C-29-95-A5-C1,cafSessionDomain=2,BYODRegistration=Unknown,EndPointPolicyID=a5f92810-be86-11e1-ba69-0050568e002b,FirstCollection=1352205183395,TimeToProfile=70,LastNmapScanTime=0,cafSessionStatus

Session Removal from the Directory

Sessions are cleaned from the session directory on the Monitoring and Troubleshooting node as follows:

- Terminated sessions are cleaned 15 minutes after termination.
- If there is authentication but no accounting, then such sessions are cleared after one hour.
- All inactive sessions are cleared after five days.

Global Search for Endpoints

You can use the global search box available at the top of the Cisco ISE home page to search for endpoints. You can use any of the following criteria to search for an endpoint:

- User name
- MAC Address
- IP Address
- Authorization Profile
- Endpoint Profile

- Failure Reason
- Identity Group
- Identity Store
- Network Device name
- Network Device Type
- Operating System
- Posture Status
- Location
- Security Group
- User Type

You should enter at least three characters for any of the search criteria in the Search field to display data.

Note If an endpoint has been authenticated by Cisco ISE, or its accounting update has been received, it can be found through the global search. Endpoints that have been manually added and are not authenticated by or accounted for in Cisco ISE will not show up in the search results.

The search result provides a detailed and at-a-glance information about the current status of the endpoint, which you can use for troubleshooting. Search results display only the top 25 entries. You can use filters to narrow down the results.

You can use any of the properties in the left panel to filter the results. You can also click on any endpoint to see more detailed information about the endpoint, such as:

- Session trace
- Authentication details
- Accounting details
- Posture details
- Profiler details
- Client Provisioning details
- Guest accounting and activity

CHAPTER 10

Bring Your Own Device (BYOD)

- Personal Devices on a Corporate Network (BYOD), on page 877
- Personal Device Portals, on page 878
- Support Device Registration Using Native Supplicants, on page 884
- Device Portals Configuration Tasks, on page 886
- Manage Personal Devices Added by Employees, on page 900
- Monitor My Devices Portals and Endpoints Activity, on page 901

Personal Devices on a Corporate Network (BYOD)

When supporting personal devices on a corporate network, you must protect network services and enterprise data by authenticating and authorizing users (employees, contractors, and guests) and their devices. Cisco ISE provides the tools you need to allow employees to securely use personal devices on a corporate network.

Guests can automatically register their devices when logging in to the Guest portals. Guests can register additional devices up to the maximum limit that you define in their guest type. These devices are registered into endpoint identity groups based on the portal configuration.

Guests can add their personal devices to the network by running the native supplicant provisioning (Network Setup Assistant), or by adding their devices to the My Devices portal. You can create native supplicant profiles, which determine the proper native supplicant provisioning wizard to use, based on the operating system.

Because native supplicant profiles are not available for all devices, users can use the My Devices portal to add these devices manually; or you can configure BYOD rules to register these devices.

Cisco ISE Community Resource

End-User Device Portals in a Distributed Environment

Cisco ISE end-user web portals depend on the Administration, Policy Services, and Monitoring personas to provide configuration, session support, and reporting.

- **Policy Administration node (PAN)**: Configuration changes that you make to the users, devices, and end-user portals are written to the PAN.
- **Policy Service node (PSN)**: The end-user portals run on a PSN, which handles all session traffic, including: network access, client provisioning, guest services, posture, and profiling. If a PSN is part of a node group, and one node fails, the other nodes detect the failure and reset any pending sessions.

- **Monitoring node (MnT node)**: The MnT node collects, aggregates, and reports data about the end-user and device activity on the My Devices, Sponsor, and Guest portals. If the primary MnT node fails, the secondary MnT node automatically becomes the primary MonT node.

Global Settings for Device Portals

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Settings**.

You can configure the following general settings for the BYOD and My Devices portals:

- **Employee Registered Devices**: Enter the maximum number of devices that an employee can register in **Restrict employees to**. By default, this value is set to **5** devices.
- **Retry URL**: Enter a URL that can be used to redirect the device back to Cisco ISE in **Retry URL for onboarding**.

Once you configure these general settings, they apply to all BYOD and My Devices portals that you set up for your company.

Personal Device Portals

Cisco ISE provides several web-based portals to support employee-owned personal devices. These device portals do not participate in the guest or sponsor portal flows.

- **Blocked List Portal**: Provides information about personal devices that are block listed and cannot be used to gain access to the network.
- **BYOD Portals**: Enables employees to register their personal devices using native supplicant provisioning functionality.
- **Certificate Provisioning Portal**: Enables administrators and employees to request for user or device certificate(s) for devices that cannot go through the BYOD flow.
- **Client Provisioning Portals**: Forces employees to download a posture agent on their devices that checks for compliance.
- **MDM Portals**: Enables employees to enroll their mobile devices with an external Mobile Device Management (MDM) system.
- **My Devices Portals**: Enables employees to add and register personal devices, including those that do not support native supplicant provisioning, and then manage them.

Cisco ISE provides you with the ability to host multiple device portals on the Cisco ISE server, including a predefined set of default portals. The default portal themes have standard Cisco branding that you can customize through the Administrators portal (**Administration** > **Device Portal Management**). You can also choose to further customize a portal by uploading images, logos, and cascading style sheets (CSS) files that are specific to your organization.

Access Device Portals

You can access any of the Personal Device Portals from the Cisco ISE GUI as follows:

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management**.

Step 2 Select the specific device portal that you want to configure.

Blocked List Portal

Employees do not access this portal directly, but are redirected to it.

If employees lose their personal device or it is stolen, they can update its status in the My Devices portal, which adds it to the Blocked List endpoint identity group. This prevents others from using the device to obtain unauthorized network access. If anyone attempts to connect to the network using one of these devices, they are redirected to the Blocked List portal which informs them that the device is denied access to the network. If the device is found, employees can reinstate it (in the My Devices portal) and regain network access without having to register the device again. Depending on whether the device was lost or stolen, additional provisioning may be required before the device can be connected to the network.

You can configure the port settings (default is port 8444) for the Blocked List portal. If you change the port number, make sure it is not being used by another end-user portal.

For information about configuring a Blocked List portal, see Edit the Blocked List Portal, on page 889.

Certificate Provisioning Portal

Employees can access the Certificate Provisioning portal directly.

The Certificate Provisioning portal allows employees to request certificates for devices that cannot go through the onboarding flow. For example, devices such as point-of-sale terminals cannot go through the BYOD flow and need to be issued certificates manually. The Certificate Provisioning portal allows a privileged set of users to upload a certificate request for such devices, generate key pairs (if required), and download the certificate.

Employees can access this portal and request for a single certificate or make a bulk certificate request using a CSV file.

ISE Community Resource

For information about the functionality and configuration of Cisco ISE Certificate Provisioning Portal, see ISE 2.0: Certificate Provisioning Portal.

Bring Your Own Device Portal

Employees do not access this portal directly.

Employees are redirected to the Bring Your Own Device (BYOD) portal when registering personal devices using native supplicants. The first time employees attempt to access the network using a personal device, they may be prompted to manually download and launch the Network Setup Assistant (NSA) wizard and be guided through registering and installing the native supplicant. After they have registered a device, they can use the My Devices portal to manage it.

If you're using Microsoft Edge 93 or Microsoft Edge 94 as your web browser for downloading NSA and AnyConnect wizards, copy-paste the **redirected URL** or **download link** in a new tab and click **Enter** on your keyboard.

Alternatively, you can click on **Download icon** > **right click on downloaded file** > **Keep file** on your Microsoft Edge 93 or Microsoft Edge 94 browser.

If you are using Google Chrome 93 or Google Chrome 95 as your web browser for downloading Network Setup Assistant (NSA) and AnyConnect wizards, click the **Keep** option in the download notification to keep and install the NSA and AnyConnect packages on your system.

Note

- BYOD flow is not supported when a device is connected to a network using Network Access Manager (NAM).
- If you are using the BYOD flow for Android devices, upgrade to Android 11 or enable the Broadcast SSID option in WLAN configuration.

Related Topics

Create a BYOD Portal, on page 892
Personal Devices on a Corporate Network (BYOD), on page 877

Client Provisioning Portal

Employees do not access this portal directly, but are redirected to it.

The Client Provisioning system provides posture assessments and remediations for devices that are attempting to gain access to your corporate network. When employees request network access using their devices, you can route them to a Client Provisioning portal and require them to first download the posture agent. The posture agent scans the device for compliance, such as verifying that virus protection software is installed on it and that its operating system is supported.

Related Topics

Create a Client Provisioning Portal, on page 894

Mobile Device Management Portal

Employees do not access this portal directly, but are redirected to it.

Many companies use a Mobile Device Management (MDM) system to manage employees' mobile devices.

Cisco ISE allows integration with external MDM systems that employees can use to enroll their mobile device and gain access to your corporate network. Cisco provides an external MDM interface that employees can enroll in to register their devices and then connect to the network.

The MDM portal enables employees to enroll in an external MDM system.

Employees can then use the My Devices portal to manage their mobile devices, such as lock their devices with a pin code, reset their device to its default factory settings, or remove applications and settings that were installed when registering the device.

Cisco ISE allows you to have a single MDM portal for all external MDM systems, or a portal for each individual MDM system.

For information about configuring MDM servers to work with Cisco ISE, see Create an MDM Portal, on page 896.

My Devices Portal

Employees can access the My Devices portal directly.

Some network devices that need network access are not supported by native supplicant provisioning and cannot be registered using the BYOD portal. However, employees can add and register personal devices, whose operating systems are not supported or do not have web browsers (such as printers, internet radios, and other devices), using the My Devices portal.

Employees can add and manage new devices by entering the MAC address for the device. When employees add devices using the My Devices portal, Cisco ISE adds the devices to the Endpoints window (**Administration** > **Context Visibility** > **Endpoints**) as members of the **RegisteredDevices** endpoint identity group (unless already statically assigned to a different endpoint identity group). The devices are profiled like any other endpoint in Cisco ISE and go through a registration process for network access.

When two MAC addresses from one device are entered into the My Devices portal by a user, profiling determines that they have the same hostname, and they are merged together as a single entry in Cisco ISE. For example, a user registers a laptop with wired and wireless addresses. Any operations on that device, such as delete, acts on both addresses.

When a registered device is deleted from the portal, the **DeviceRegistrationStatus** and **BYODRegistration** attributes change to **Not Registered** and **No**, respectively. However, these attributes remain unchanged when a guest (who is not an employee) registers a device using the Guest Device Registration window in the credentialed Guest portals, because these BYOD attributes are used only during employee device registration.

Regardless of whether employees register their devices using the BYOD or the My Devices portals, they can use the My Devices portal to manage them.

Note The My Devices portal is not available when the Administrator's portal is down.

When endpoints are imported from Context visibility, they are not automatically linked to BYOD user accounts. They must follow the usual BYOD registration process to be added to the My Devices portal.

Related Topics

Create a My Devices Portal, on page 897

BYOD Deployment Options and Status Flow

The BYOD deployment flows that support personal devices vary slightly based on these factors:

- Single or dual SSID: With single SSID, the same Wireless Local Area Network (WLAN) is used for certificate enrollment, provisioning, and network access. In a dual SSID deployment, there are two SSIDs.One provides enrollment and provisioning, and the other provides secure network access.
- Windows, macOS, iOS, or Android device: The native supplicant flow starts similarly, regardless of the device type, by redirecting employees using a supported personal device to the BYOD portal to confirm their device information. The process diverges based on the device type.

If you use Cisco ISE Release 3.1 Patch 5 or later releases, in the case of single or dual SSID BYOD flows, a BYOD user with an iOS device must carry out the following steps before they connect to the enterprise network:

1. Go to **Settings** > **Safari**.

2. Tap **Clear History and Website Data**.

In the **Administration** > **Administration** > **Certificates** > **System Certificates** > **Default Self-Signed Certificate** window, the Subject Alternative Name field for BYOD certificates must include both the DNS name and the IP address.

Employee Connects to Network

1. Cisco ISE authenticates the employee's credentials against the corporate Active Directory or other corporate identity stores and provides an authorization policy.
2. The device is redirected to the BYOD portal. The device’s MAC address field is preconfigured, and the user can add a device name and description.
3. The native supplicant is configured (MacOS, Windows, iOS, Android) but the process varies by device:
   - MacOS and Windows devices: Employee clicks **Register** in the BYOD portal to download and install the supplicant provisioning wizard (Network Setup Assistant), which configures the supplicant and provides the certificate (if necessary) used for EAP-TLS certificate-based authentication. The issued certificate is embedded with the device's MAC address and employee's username.

     Starting with version MacOS 10.15, the user must allow download of the Supplicant Provisioning Wizard (SPW). A window displays on the user's device asking them to allow or deny downloads from the Cisco ISE server.

Note Network Setup Assistant cannot be downloaded to a Windows device, unless the user of that device has administrative privileges. If you cannot grant end users administrative privileges, then use your Group Policy object (GPO) to push the certificate to the user's device, instead of using the BYOD flow.

   - iOS devices: The Cisco ISE policy server sends a new profile using Apple’s iOS over the air to the iOS device, which includes:
     - The issued certificate (if configured) is embedded with the iOS device's MAC address and employee's username.
     - A Wi-Fi supplicant profile that enforces the use of EAP-TLS for 802.1X authentication. An additional profile can be installed on the endpoint device to protect Over-The-Air (OTA) communication.

     Check the **Enable if Target Network is Hidden** check box only when the actual Wi-Fi network is hidden. Otherwise, Wi-Fi network configuration may not be provisioned properly for certain iOS devices, especially in the single SSID flow (where the same Wi-Fi network or SSID is used for both onboarding and connectivity).

   - Android devices: Cisco ISE prompts and routes employee to download the Network Setup Assistant (NSA) from the Google Play store. After installing the application, the employee can open NSA and start the setup wizard, which generates the supplicant configuration and issued certificate used to configure the device.
4. After the user goes through the on boarding flow, Cisco ISE initiates a Change of Authorization (CoA). This causes the MacOS, Windows, and Android devices to reconnect to the secure 802.1X network. For

single SSID, iOS devices also connect automatically, but for dual SSID, the wizard prompts iOS users to manually connect to the new network.

You can configure a BYOD flow that does not use supplicants. For more information, see the Cisco ISE Community Resource document.

Note Mac randomization is not enabled for this flow.

As Android 10 generates a random MAC address whenever a new connection profile is created, you must modify the default rule to remove *BYOD_is_Registered* and *MAC_in_SAN* conditions from the authorization profile for the BYOD flow to work with Android clients.

BYOD Session Endpoint Attribute

The state of the endpoint attribute *BYODRegistration* changes during the BYOD flow to the following states.

- *Unknown*: The device has not been through a BYOD flow.
- *Yes*: The device has been through BYOD flow, and is registered.
- *No*: The device has been through BYOD flow, but is not registered. This means that the device was deleted.

Device Registration Status Endpoint Attribute

The state of the endpoint attribute *DeviceRegistrationStatus* changes during device registration to the following states.

- *Registered*: The device has been through BYOD flow, and it is registered. There is a 20-minute delay before the attribute changes from pending to registered.
- *Pending*: The device has been through BYOD flow, and it is registered. But, Cisco ISE has not seen it on the network.
- *Not Registered*: The device has not been through BYOD flow. *Not Registered* is the default state of the *DeviceRegistrationStatus* attribute.
- *Stolen*: The user logs onto the My Devices portal, and marks a currently onboarded device as Stolen. This happens:
  - If the device was onboarded by provisioning a certificate and a profile, Cisco ISE revokes the certificate that was provisioned to the device, and assigns the device's MAC address to the Blocked List endpoint identity group. That device no longer has network access.
  - If the device was onboarded by provisioning a profile (no certificate), Cisco ISE assigns the device to the Blocked List endpoint identity group. The device still has network access, unless you create an authorization policy for this situation. For example, **IF Endpoint Identity Group is Blocked List AND BYOD_is_Registered THEN DenyAccess**.

  An administrator performs an action that disables network access for several devices, such as deleting or revoking a certificate.

If a user reinstates a stolen device, the status reverts to *Not Registered*. The user must delete that device, and add it back. This starts the onboarding process.

- *Lost*: The user logs on to the My Devices portal, and marks a currently onboarded device as *Lost* that causes the following actions:
    - The device is assigned to Blocked List identity group.
    - Certificates provisioned to the device are not revoked.
    - The device status is updated to *Lost*.
    - *BYODRegistration* status is updated to *No*.

  A lost device still has network access unless you create an authorization policy to block lost devices. You can use the Blocked List identity group or the *endpoint:BYODRegistration* attribute in your rule. For example, **IF Endpoint Identity Group is Blocked List AND EndPoints:BYODRegistrations Equals No THEN BYOD**. For more granular access, you can also add *NetworkAccess:EAPAuthenticationMethod Equals PEAP or EAP-TLS or EAP-FAST" , InternalUser:IdentityGroup Equals <<group>>* to the IF part of the rule.

Limit the Number of Personal Devices Registered by Employees

You can allow employees to register between 1 and 999 personal devices. Regardless of the portal that employees used to register their personal devices, this setting defines the maximum number of devices registered across all portals.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Settings** > **Employee Registered Devices**.

Step 2 Enter the maximum number of devices that an employee can register in the **Restrict employees to** field. By default, this value is set to **5** devices.

Step 3 Click **Save**. If you do not want to save any updates you made to the settings, click **Reset** to revert to the last saved values.

Support Device Registration Using Native Supplicants

You can create native supplicant profiles to support personal devices on the Cisco ISE network. Based on the profile that you associate with a user's authorization requirements, Cisco ISE provides the necessary supplicant provisioning wizard to set up the user's personal device to access the network.

The first time employees attempt to access the network using a personal device, they are guided automatically through the registration and supplicant configuration. After they have registered the device, they can use the My Devices portal to manage their devices.

Operating Systems Supported by Native Supplicants

Native supplicants are supported for these operating systems:

- Android (excluding Amazon Kindle, B&N Nook)

- MacOS (for Apple Mac computers)
- Apple iOS devices (Apple iPod, iPhone, and iPad)
- Microsoft Windows 7, 8 (excluding RT), Vista, and 10

Allow Employees to Register Personal Devices Using Credentialed Guest Portals

Employees using credentialed Guest portals can register their personal devices. The self-provisioning flow supplied by the BYOD portal enables employees to connect devices to the network directly using native supplicants, which are available for Windows, MacOS, iOS, and Android devices.

Before you begin

You must create the native supplicant profiles.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals**.

Step 2 Choose the credentialed Guest portal that you want to allow employees to use to register their devices using native supplicants and click **Edit**.

Step 3 Click the **Portal Behavior and Flow Settings** tab.

Step 4 Under **BYOD Settings**, check the **Allow employees to use personal devices on the network** check box.

Step 5 Click **Save**.

Provide a URL to Reconnect with BYOD Registration

You can provide information that enables employees, who encounter a problem while registering their personal devices using the BYOD portal to reconnect with the registration process.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Settings** > **Retry URL**.

Step 2 In the **Retry URL for Onboarding** field, enter the URL to be used to redirect the device back to Cisco ISE.

When a device encounters a problem during the registration process, it tries to reconnect to the internet automatically. At this point, the URL that you enter here is used to redirect the device back to Cisco ISE (which reinitiates the onboarding process). The default value is 192.0.2.123.

Step 3 Click **Save**.

If you do not want to save any updates you made to the settings, click **Reset** to revert to the last saved values.

Device Portals Configuration Tasks

You can use a default portal and its default settings such as certificates, endpoint identity group, identity source sequence, portal themes, images, and other details provided by Cisco ISE. If you do not want to use the default settings, you should create a new portal or edit an existing one to meet your needs. You can duplicate a portal if you want to create multiple portals with the same settings.

After creating a new portal or editing a default one, you must authorize the portal for use. Once you authorize a portal for use, any subsequent configuration changes you make are effective immediately.

You do not need to authorize the My Devices portal for use.

If you choose to delete a portal, you must first delete any authorization policy rules and authorization profiles associated with it or modify them to use another portal.

Use this table for the tasks related to configuring the different Device portals.

Task	Blocked List Portal	BYOD Portal	Client Provisioning Portal	MDM Portal	My Devices Portal
Enable Policy Services, on page 887	Required	Required	Required	Required	Required
Add Certificates to the Device Portal, on page 887	Required	Required	Required	Required	Required
Create External Identity Sources, on page 888	Not Required	Not Required	Not Required	Not Required	Required
Create Identity Source Sequences, on page 888	Not Required	Not Required	Not Required	Not Required	Required
Create Endpoint Identity Groups, on page 889	Not Required	Required	Not Required	Required	Required
Edit the Blocked List Portal	Required	Not applicable	Not applicable	Not applicable	Not applicable
Create a BYOD Portal, on page 892	Not applicable	Required	Not applicable	Not applicable	Not applicable
Create a Client Provisioning Portal, on page 894	Not applicable	Not applicable	Required	Not applicable	Not applicable

Task	**Blocked List Portal**	**BYOD Portal**	**Client Provisioning Portal**	**MDM Portal**	**My Devices Portal**
Create an MDM Portal, on page 896	Not applicable	Not applicable	Not applicable	Required	Not applicable
Create a My Devices Portal, on page 897	Not applicable	Not applicable	Not applicable	Not applicable	Required
Create Authorization Profiles, on page 898	Not applicable	Required	Required	Required	Not Required
Customize Device Portals, on page 899	Optional	Optional	Optional	Optional	Optional

Enable Policy Services

To support the Cisco ISE end-user web portals, you must enable the portal-policy services on the node on which you want to host them.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 2 Click the node and click **Edit**.

Step 3 Under the **General Settings** tab, enable the **Policy Service** toggle button.

Step 4 Check the **Enable Session Services** check box.

Step 5 Click **Save**.

Add Certificates to the Device Portal

If you do not want to use the default certificates, you can add a valid certificate and assign it to a certificate group tag. The default certificate group tag used for all end-user web portals is **Default Portal Certificate Group**.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **System Certificates**.

Step 2 Add a system certificate and assign it to a certificate group tag that you want to use for the portal.

This certificate group tag will be available to select during portal creation or editing.

Step 3 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **(any portal)** > **Create or Edit** > **Portal Settings**.

Step 4 Select the specific certificate group tag from the **Certificate Group Tag** drop-down list that is associated with the newly added certificate.

Note

- BYOD does not support certificate chains longer than three certificates.
- During BYOD onboarding, certificates are issued twice for iOS devices.

Create External Identity Sources

Cisco ISE can connect with external identity sources such as Active Directory, LDAP, RADIUS Token, and RSA SecurID servers to obtain user information for authentication and authorization. External identity sources also include certificate authentication profiles that you need for certificate-based authentications.

Note To work with passive identity services, which enable you to receive and share authenticated user identities, see Additional Passive Identity Service Providers, on page 690.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources**.

Step 2 Choose one of these options:

- **Certificate Authentication Profile** for certificate-based authentications.
- **Active Directory** to connect to an Active Directory as an external identity source. See Active Directory as an External Identity Source, on page 641 for more details.
- **LDAP** to add an LDAP identity source. See LDAP, on page 730 for more details.
- **RADIUS Token** to add a RADIUS Token server. See RADIUS Token Identity Sources, on page 752 for more details.
- **RSA SecurID** to add an RSA SecurID server. See RSA Identity Sources, on page 758 for more details.
- **SAML Id Providers** to add an identity provider (IdP), such as Oracle Access Manager. See SAMLv2 Identity Provider as an External Identity Source, on page 764 for more details.
- **Social Login** to add a Social Login, such as Facebook, as an external identity source. See Social Login for Self-Registered Guests, on page 493 for more details.

Create Identity Source Sequences

Before you begin

Ensure that you have configured your external identity sources in Cisco ISE.

To perform the following task, you must be a Super Admin or System Admin.

For allowing guest users to authenticate through Local WebAuth, you must configure both the Guest portal authentication source and the identity source sequence to contain the same identity stores.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **Identity Source Sequences** > **Add**.

Step 2 Enter a name for the identity source sequence. You can also enter an optional description.

Step 3 Check the **Select Certificate Authentication Profile** check box and choose a certificate authentication profile for certificate-based authentication.

Step 4 Choose the database or databases that you want to include in the identity source sequence in the **Selected List** field.

Step 5 Rearrange the databases in the **Selected list** field in the order in which you want Cisco ISE to search the databases.

Step 6 If a selected identity store cannot be accessed for authentication, choose one of the following options in the **Advanced Search List** area:

- **Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError**
- **Treat as if the user was not found and proceed to the next store in the sequence**

While processing a request, Cisco ISE searches these identity sources in sequence. Ensure that you have the identity sources in the Selected list field listed in the order in which you want Cisco ISE to search them.

Step 7 Click **Submit** to create the identity source sequence that you can then use in policies.

Create Endpoint Identity Groups

Cisco ISE groups endpoints that it discovers in to the corresponding endpoint identity groups. Cisco ISE comes with several system-defined endpoint identity groups. You can also create additional endpoint identity groups from the **Endpoint Identity Groups** window. You can edit or delete the endpoint identity groups that you have created. You can only edit the description of the system-defined endpoint identity groups. You cannot edit the name of these groups or delete them.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **Groups** > **Endpoint Identity Groups**.

Step 2 Click **Add**.

Step 3 Enter the **Name** for the endpoint identity group that you want to create (do not include spaces in the name of the endpoint identity group).

Step 4 Enter the **Description** for the endpoint identity group that you want to create.

Step 5 Click the **Parent Group** drop-down list to choose an endpoint identity group to which you want to associate the newly created endpoint identity group.

Step 6 Click **Submit**.

Edit the Blocked List Portal

Cisco ISE provides a single Blocked List portal that displays information when a lost or stolen device that is block listed in Cisco ISE is attempting to access your corporate network.

You can only edit the default portal settings and customize the default message that displays for the portal. You cannot create a new Blocked List portal, or duplicate or delete the default portal.

Before you begin

Ensure that you have the required certificates configured for use with this portal.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Blocked List Portal** > **Edit**.

Step 2 Provide a unique **Portal Name** and a **Description** for the portal.

Ensure that the portal name that you use here is not used for any other end-user portals.

Step 3 From the **Language File** drop-down list, choose the desired action to import or export language files to be used with the portal.

Step 4 Click the **Portal test URL** link to open a new browser tab that displays the URL for this portal. Policy Services Node (PSN) with Policy Services must be turned on. If Policy Services are disabled, the PSN only displays the Admin portal.

Note The test portal does not support RADIUS sessions, so you won't see the entire portal flow for all portals. BYOD and Client Provisioning are examples of portals that depend on RADIUS sessions. For example, a redirect to an external URL will not work. If you have more than one PSN, Cisco ISE chooses the first active PSN.

Step 5 Expand **Portal Settings**. Update the default values for ports, certificate group tags, endpoint identity groups, and so on, and define behavior that applies to the overall portal.

- **HTTPS Port**: Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blocked List Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you modify this window. If you modify this window, update the port setting to comply with this restriction.

  If you assign ports used by a non-guest (such as My Devices) portal to a guest portal, an error message appears.

  For posture assessments and remediation only, the Client Provisioning portal also uses ports 8905 and 8909. Otherwise, it uses the same ports assigned to the Guest portal.

  Portals assigned to the same HTTPS port can use the same Gigabit Ethernet interface or another interface. If they use the same port and interface combination, they must use the same certificate group tag. For example:

  - Valid combinations include, using the Sponsor portal as an example:
    - Sponsor portal: Port **8443**, Interface **0**, Certificate tag **A** and My Devices portal: Port **8443**, Interface **0**, Certificate group **A**.
    - Sponsor portal: Port **8443**, Interface **0**, Certificate group **A** and My Devices portal: Port **8445**, Interface **0**, Certificate group **B**.
    - Sponsor portal: Port **8444**, Interface **1**, Certificate group **A** and Blocked List portal: Port **8444**, Interface **0**, Certificate group **B**.
  - Invalid combinations include:
    - Sponsor portal: Port **8443**, Interface **0**, Certificate group **A** and My Devices portal: **8443**, Interface **0**, Certificate group **B**.
    - Sponsor portal: Port **8444**, Interface **0**, Certificate tag **A** and Blocked List portal: Port **8444**, Interface **0**, Certificate group **A**.

Note We recommend that you use interface 0 for Guest services for best performance. You can either configure only interface 0 in the **Portal Settings**, or you can use the CLI command **ip host** to map a hostname or FQDN to the IP address of interface 0.

- **Allowed Interfaces**: Select the PSN interfaces which a PAN can use to run a portal. When a request to open a portal is made on the PAN, the PAN looks for an available allowed port on the PSN. You must configure the Ethernet interfaces using IP addresses on different subnets.

  These interfaces must be available on all the PSNs, including VM-based ones, that have Policy Services turned on. This is a requirement because any of these PSNs can be used for the redirect at the start of the guest session.

  - The Ethernet interfaces must use IP addresses on different subnets.
  - The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
  - The portal certificate Subject Name or Alternate Subject Name must resolve to the interface IP address.
  - Configure **ip host x.x.x.x yyy.domain.com** in Cisco ISE CLI to map the secondary interface IP address to the FQDN, which is used to match the certificate Subject Name or Alternate Subject Name.
  - If only the bonded NIC is selected, when the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN logs an error and exits. The PSN will not try to start the portal on the physical interface.
  - NIC Teaming or bonding is a configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based in the **Portal Settings** configuration. If both physical NICs and the corresponding bonded NIC are configured, when the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.

- **Certificate Group tag**: Pick a certificate group tag that specifies the certificate to be used for the portal’s HTTPS traffic.
- **Display Language**
  - **Use Browser Locale**: Use the language specified in the client browser's locale setting as the display language of the portal. If browser locale's language is not supported by Cisco ISE, then the **Fallback Language** is used as the language portal.
  - **Fallback Language**: Choose the language to use when the language cannot be obtained from the browser locale, or if the browser locale language is not supported by Cisco ISE.
  - **Always Use**: Choose the display language to use for the portal. This setting overrides the **User Browser Locale** option.

Step 6 On the **Portal Page Customization** tab, customize the page title and message text that appears in the portal when an unauthorized device is attempting to gain access to the network.

Step 7 Click **Save** and then **Close**.

Create a BYOD Portal

You can provide a Bring Your Own Device (BYOD) portal to enable employees to register their personal devices, so that the registration and supplicant configuration can be done before allowing access to the network.

You can create a new BYOD portal, or you can edit or duplicate an existing one. You can delete any BYOD portal, including the default portal provided by Cisco ISE.

Any changes that you make to the **Portal & Page Settings** under the **Portal Behavior and Flow Settings** tab are reflected in the graphical flow in the device portal flow diagram. If you enable a window, such as the **Support Information** window, the window appears in the flow and the employee experiences it in the portal. Disabling the window removes it from the flow.

Before you begin

Ensure that you have the required certificates and endpoint identity groups configured for use within this portal.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **BYOD** > **Create**.

Step 2 Provide a unique **Portal Name** and a **Description** for the portal.

Ensure that the portal name you use here is not used for any other end-user portals.

Step 3 From the **Language File** drop-down list, choose the desired action to import or export language files to be used with the portal.

Step 4 Click the **Portal Behavior and Flow Settings** tab.

Step 5 Expand **Portal Settings**. Update the default values for ports, certificate group tags, endpoint identity groups, and so on, and define behavior that applies to the overall portal.

Step 6 Expand **Support Information Page Settings**. Update the required information here to help employees provide information that the Help Desk can use to troubleshoot network access issues.

Step 7 Click the **Portal Page Customization** tab. Scroll down to the **Page Customizations** area to customize the following end user portal windows. Choose the portal window you want to customize by clicking the corresponding option listed under **Pages**in the left side menu.

- **BYOD Welcome**:
    - **Device Configuration Required**: Enter the content to be displayed when the device is redirected to the BYOD portal for the first time and requires certificate provisioning.
    - **Certificate Needs Renewal**: Enter the content to be displayed when the previous certificate needs to be renewed.
- **BYOD Device Information**:
    - **Maximum Devices Reached**: Enter the content to be displayed when the maximum limit of devices that an employee can register is reached.
    - **Required Device Information**: Enter the content to be displayed when requesting device information that is required to enable an employee to register the device.
- **BYOD Installation**:
    - **Desktop Installation**: Enter the content to be displayed when providing installation information for a desktop device.

    - **iOS Installation**: Enter the content to be displayed when providing installation instructions for an iOS mobile device.
    - **Android Installation**: Enter the content to be displayed when providing installation instructions for an Android mobile device.
- **BYOD Success**:
    - **Success**: Enter the content to be displayed when the device is configured and automatically connected to the network.
    - **Success: Manual Instructions**: Enter the content to be displayed when the device is successfully configured and an employee must manually connect to the network.
    - **Success: Unsupported Device**: Enter the content to be displayed when an unsupported device is allowed to connect to the network.

Step 8 Click **Save** and then click **Close**.

What to do next

You must authorize the portal in order to use it. You can also customize your portal either before or after you authorize it for use.

Create a Certificate Provisioning Portal

Cisco ISE provides a Certificate Provisioning portal that allows you to request for certificates for devices that cannot go through the onboarding flow. For example, devices such as point-of-sale terminals. You can request for a single certificate or make a bulk certificate request using a CSV file.

You can edit the default portal settings and customize the messages that appear on the portal. You can also create, duplicate, and delete the Certificate Provisioning portal.

There are two types of users who can access the Certificate Provisioning portal:

- Internal or external users with administrative privileges: Can generate certificates for themselves as well as for others.
- All other users: Can generate certificates only for themselves.

Users (network access users) who are assigned the Super Admin or ERS Admin role have access to this portal and can request certificates for others. However, if you create a new internal admin user and assign the Super Admin or ERS Admin role, the internal admin user will not have access to this portal. You must first create a network access user and then add the user to the Super Admin or ERS Admin group. Any existing network access users who are added to the Super Admin or ERS Admin group will have access to this portal.

For other users to be able to access the portal and to generate certificates for themselves, configure the Certificate Provisioning Portal Settings. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Certificate Provisioning** > **Edit** > **Portal Behavior and Flow Settings** > **Portal Settings**. Ensure that you choose the appropriate identity source or identity source sequence under **Authentication Method** and choose the user group under **Configure Authorized Groups**.

All users who belong to the groups that you choose will have access to the portal and can generate certificates for themselves.

Before you begin

Ensure that you have the required certificates configured for use with this portal.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Certificate Provisioning** > **Create**.

Ensure that the portal name that you use here is not used for any other end-user portals.

Step 2 Provide a unique **Portal Name** and a **Description** for the portal.

Step 3 From the **Language File** drop-down list, choose the desired action to import or export language files to be used with the portal.

Step 4 Click the **Portal Behavior and Flow Settings** tab.

Step 5 Expand **Portal Settings**. Update the default values for ports, certificate group tags, endpoint identity groups, and so on, and define behavior that applies to the overall portal.

Step 6 Click the **Portal Page Customization** tab. Customize the page title and the message text that appears in the portal.

Step 7 Click **Save** and then **Close**.

Create a Client Provisioning Portal

You can provide a Client Provisioning portal to enable employees to download the Cisco AnyConnect posture component, that verifies the posture compliance of the device before allowing access to the network.

You can create a new Client Provisioning portal, or you can edit or duplicate an existing one. You can delete any Client Provisioning portal, including the default portal provided by Cisco ISE.

Users (network access users) who are assigned the Super Admin or ERS Admin role have access to this portal. However, if you create a new internal admin user and assign the Super Admin or ERS Admin role, the internal admin user will not have access to this portal. You must first create a network access user and then add the user to the Super Admin or ERS Admin group. Any existing network access users who are added to the Super Admin or ERS Admin group will have access to this portal.

For other users to be able to access the portal and to generate certificates for themselves, configure the Certificate Provisioning Portal settings. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Client Provisioning** > **Edit** > **Portal Behavior and Flow Settings** > **Portal Settings**. Ensure that you choose the appropriate identity source or identity source sequence under **Authentication Method** and choose the user group under **Configure Authorized Groups**. All users who belong to the groups that you choose will have access to the portal and can generate certificates for themselves.

Any changes that you make to the **Portal & Page Settings** under the **Portal Behavior and Flow Settings** tab are reflected in the graphical flow in the device portal flow diagram. If you enable a window, such as the **Support Information** window, the window appears in the flow and the employee experiences it in the portal. Disabling the window removes it from the flow.

Before you begin

Ensure that you have the required certificates and client provisioning policies configured for use with this portal.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Client Provisioning** > **Create**.

Step 2 Provide a unique **Portal Name** and a **Description** for the portal.

Ensure that the portal name

Step 3 From the **Language File** drop-down list, choose the desired action to import or export language files to be used with the portal.

Step 4 Click the **Portal Behavior and Flow Settings** tab.

Step 5 Expand **Portal Settings**. Update the default values for ports, certificate group tags, endpoint identity groups, and so on, and define behavior that applies to the overall portal.

Step 6 Expand **Support Information Page Settings**. Update the required information here to help employees provide information that the Help Desk can use to troubleshoot network access issues.

Step 7 Click the **Portal Page Customization** tab. Scroll down to the **Page Customizations** area to customize the following end user portal windows. Choose the portal window you want to customize by clicking the corresponding option listed under **Pages**in the left side menu.

- **Client Provisioning Portals**:
    - **Agent Unknown**: Enter the content to be displayed when the agent is unknown.
    - **Checking**, **Scanning** and **Compliant**: Enter the content to be displayed when the posture agent is successfully installed and checks, scans and verifies that the device is compliant with posture requirements.
    - **Non-compliant**: Enter the content to be displayed when the posture agent determines that the device is not compliant with posture requirements.
- **Client Provisioning (Agent Not Found)**:
    - **Agent Not Found**: Enter the content to be displayed when the posture agent is not detected on the device.
    - **Manual Installation Instructions**: Enter the content to be displayed when devices do not have Java or Active X software installed on them, instructions on how to manually download and install the posture agent.
    - **Install, No Java/ActiveX**: Enter the content to be displayed when devices do not have Java or Active X software installed on them, instructions on how to download and install the Java plug-in.
    - **Agent Installed**: Enter the content to be displayed when the posture agent is detected on the device, instructions on how to start the posture agent, which checks the device for compliance with posture requirements.

Step 8 Click **Save** and then click **Close**.

What to do next

You must authorize the portal in order to use it. You can also customize your portal either before or after you authorize it for use.

Related Topics

Authorize Portals, on page 510
Customize Device Portals, on page 899

Create an MDM Portal

You can provide a Mobile Device Management (MDM) portal to enable employees to manage their mobile devices that are registered for use on your corporate network.

You can create a new MDM portal, or you can edit or duplicate an existing one. You can have a single MDM portal for all of your MDM systems or you can create a portal for each system. You can delete any MDM portal, including the default portal provided by Cisco ISE. The default portal is for third-party MDM providers.

You can create a new MDM portal, or you can edit or duplicate an existing one. You can delete any MDM portal, including the default portal provided by Cisco ISE. The default portal is for third-party MDM providers.

Any changes that you make to the **Portal & Page Settings** under the **Portal Behavior and Flow Settings** tab are reflected in the graphical flow in the device portal flow diagram. If you enable a window, such as the **Support Information** window, the window appears in the flow and the employee experiences it in the portal. Disabling the window removes it from the flow.

Before you begin

Ensure that you have the required certificates and endpoint identity groups configured for use with this portal.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Mobile Device Management** > **Create, Edit or Duplicate**.

Step 2 Provide a unique **Portal Name** and a **Description** for the portal.

Ensure that the portal name you use here is not used for any other end-user portals.

Step 3 From the **Language File** drop-down list, choose the desired action to import or export language files to be used with the portal.

Step 4 Click the **Portal Behavior and Flow Settings** tab.

Step 5 Expand **Portal Settings**. Update the default values for ports, certificate group tags, endpoint identity groups, and so on, and define behavior that applies to the overall portal.

Step 6 Expand **Employee Mobile Device Management Settings**. Access the link provided to configure third-party MDM providers and then define the acceptance policy behavior for employees using the MDM portals.

Step 7 Expand **Support Information Page Settings**. Update the required information here to help employees provide information that the help desk can use to troubleshoot network access issues.

Step 8 Click the **Portal Page Customization** tab.

Step 9 Customize the **Content Area** messages that appears in the MDM portal during the device enrollment process.

- **Unreachable**: Enter the content to be displayed when the selected MDM system cannot be reached.
- **Non-compliant**: Enter the content to be displayed when the device being enrolled is not compliant with the requirements of the MDM system.
- **Continue**: Enter the content to be displayed when the device should try connecting to the network in case of connectivity issues.

- **Enroll**: Enter the content to be displayed when the device requires the MDM agent and needs to be enrolled in the MDM system.

Step 10 Click **Save** and then click **Close**.

What to do next

You must authorize the portal in order to use it. You can also customize your portal either before or after you authorize it for use. Also see the following topics:

- Add Certificates to the Device Portal, on page 887
- Create Endpoint Identity Groups, on page 889
- Create Authorization Profiles, on page 898
- Customize Device Portals, on page 899

Create a My Devices Portal

You can provide a My Devices portal to enable employees to add and register their personal devices that do not support native supplicants and cannot be added using the Bring Your Own Device (BYOD) portal. You can then use the My Devices portal to manage all devices that have been added using either portal.

You can create a new My Devices portal, or you can edit or duplicate an existing one. You can delete any My Devices portal, including the default portal provided by Cisco ISE.

Any changes that you make to the **Portal & Page Settings** under the **Portal Behavior and Flow Settings** tab are reflected in the graphical flow in the device portal flow diagram. If you enable a window, such as the **Support Information** window, the window appears in the flow and the employee experiences it in the portal. Disabling the window removes it from the flow.

Before you begin

Ensure that you have the required certificates, external identity stores, identity source sequences, and endpoint identity groups configured for use with this portal.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **My Devices** > **Create**.

Step 2 Provide a unique **Portal Name** and a **Description** for the portal.

Ensure that the portal name you use here is not used for any other end-user portals.

Step 3 From the **Language File** drop-down list, choose the desired action to import or export language files to be used with the portal.

Step 4 Click the **Portal Behavior and Flow Settings** tab.

Step 5 Expand **Portal Settings** to update the default values for ports, certificate group tags, endpoint identity groups, and so on, and define behavior that applies to the overall portal.

Step 6 Expand **Login Page Settings** to specify employee credential and login guidelines.

Step 7 Expand **Acceptable Use Policy (AUP) Page Settings** to add a separate AUP page and define the acceptable use policy behavior for employees.

Step 8 Expand **Post-Login Banner Page Settings** to notify employees of additional information after they log into the portal.

Step 9 Expand **Employee Change Password Settings** to allow employees to change their own passwords. This option is enabled only if the employee is part of the internal users database.

Step 10 In the **Portal Page Customization** tab, customize the following information that appears in the My Devices portal during registration and management:

- Titles, instructions, content, field and button labels
- **Error messages** and **Notification Messages**

Step 11 Click **Save** and then click **Close**.

What to do next

You can customize the portal if you want to change its appearance.

Related Topics

Customize Device Portals, on page 899
My Devices Portal, on page 881
Display Devices Added by an Employee, on page 900

Create Authorization Profiles

When you authorize a portal, you are setting up the network authorization profiles and rules for network access.

Before you begin

You must create a portal before you can authorize it.

Step 1 Set up a special authorization profile for the portal.

Step 2 Create an authorization policy rule for the profile.

Create Authorization Profiles

Each portal requires that you set up a special authorization profile for it.

Before you begin

If you do not plan to use a default portal, you must first create the portal so you can associate the portal name with the authorization profile.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.

Step 2 Create an authorization profile using the name of the portal that you want to authorize for use.

What to do next

You should create a portal authorization policy rule that uses the newly created authorization profile.

Create Authorization Policy Rules

To configure the redirection URL for a portal to use when responding to the users' (guests, sponsors, employees) access requests, define an authorization policy rule for that portal.

The url-redirect takes the following form based on the portal type, where:

ip:port : the IP address and port number

PortalID: the unique portal name

For a Hotspot Guest portal: https://*ip:port*/guestportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=cwa&type=drw

For a Mobile Device Management (MDM) portal: https://*ip:port*/mdmportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=mdm

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Sets** to create a new authorization policy rule under **Standard** policies.

Step 2 For **Conditions**, select an endpoint identity group that you want to use for the portal validation. For example, for the Hotspot Guest portal, select the default **GuestEndpoints** endpoint identity group and, for the MDM portal, select the default **RegisteredDevices** endpoint identity group.

Note Reauthenticate and Terminate CoA types are supported by Hotspot Guest portals. You can use Network Access:UseCase EQUALS Guest Flow as one of the validation conditions in the Hotspot Guest authorization policy only when Reauthentication CoA type is chosen in the Hotspot Guest Portal.

Step 3 For **Permissions**, select the portal authorization profile that you created.

Note While creating an authorization condition using a dictionary attribute with the MAC option enabled, such as RADIUS.Calling-Station-ID, you must use a Mac operator (for example, Mac_equals) to support different MAC formats.

Customize Device Portals

You can customize the portal appearance and user (guests, sponsors, or employees as applicable) experience by customizing the portal themes, changing UI elements on the portal pages, and editing error messages and notifications that are displayed to the users. For more information about customizing portals, see Customization of End-User Web Portals , on page 563.

Manage Personal Devices Added by Employees

When employees register a device using the Bring Your Own Device (BYOD) or the My Devices portals, the registered device is displayed in the **Endpoints** list. Although employees can disassociate a device from their account by deleting it, the device remains in the Cisco ISE database. As a result, employees might need your assistance in resolving errors they encounter when working with their devices.

Display Devices Added by an Employee

You can locate devices added by a specific employee using the **Portal User** field displayed on the **Endpoints** listing window. This might be useful if you need to delete devices registered by a specific user. By default, this field does not display, so you must enable it first before searching.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Identities** > **Endpoints**.

Step 2 Click the **Settings** icon available on the top right corner of the endpoints list, below the dashlets.

Step 3 Check the **Portal User** check boxEnable the **Portal User** toggle button to display this information in the endpoints listing.

Step 4 Click **Go**.

Step 5 Click the **Filter** drop-down list and choose **Quick Filter**.

Step 6 Enter the user’s name in the **Portal User** field to display only the endpoints that are assigned to that particular user.

Errors When Adding Devices to My Devices Portal

Employees cannot add a device that was already added by another employee, and that device is still in the endpoints database.

If employees attempt to add a device that already exists in the Cisco ISE database:

- We recommend adding the device through the BYOD portal, if it supports native supplicant provisioning. This overwrites any registration details that were created when it was initially added to the network.
- If the device is a MAC Authentication Bypass (MAB) device, such as a printer, then first resolve the ownership of the device. If appropriate, you can remove the device from the endpoints database using the Administrator's portal, so that the new owner can successfully add the device using the My Devices portal.

Note The My Devices portal is not available when the Administrator's portal is down.

Devices Deleted from My Devices Portal Remain in Endpoints Database

When an employee deletes a device from the My Devices portal, the device is removed from the employee’s list of registered devices, but the device remains in the Cisco ISE endpoints database and is displayed in the **Endpoints** list.

You can permanently delete the device from the Endpoints window. To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Identities** > **Endpoints**.

Limit the Number of Personal Devices Registered by Employees

You can allow employees to register between 1 and 999 personal devices. Regardless of the portal that employees used to register their personal devices, this setting defines the maximum number of devices registered across all portals.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Settings** > **Employee Registered Devices**.

Step 2 Enter the maximum number of devices that an employee can register in the **Restrict employees to** field. By default, this value is set to **5** devices.

Step 3 Click **Save**. If you do not want to save any updates you made to the settings, click **Reset** to revert to the last saved values.

Monitor My Devices Portals and Endpoints Activity

Cisco ISE provides various reports and logs that allow you to view endpoint and user management information and guest and sponsor activity.

You can run these reports either on demand or on a scheduled basis.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Reports**.

Step 2 Choose **Guest** or **Endpoints and Users** to view the various guest, sponsor, and endpoint related reports

Step 3 Choose the data with which you want to search using the **Filters** drop-down list.

Step 4 Select the **Time Range** during which you want to view the data.

Step 5 Click **Run**.

My Devices Login and Audit Report

The **My Devices Login and Audit** report is a combined report that tracks:

- Login activity by employees at the My Devices portal.
- Device related operations performed by the employees in the My Devices portal.

This report is available at: **Operations** > **Reports** > **Reports** > **Guest** > **My Devices Login and Audit**.

Registered Endpoints Report

The **Registered Endpoints** report provides information about all the endpoints that are registered by employees. This report is available at: **Operations** > **Reports** > **Reports** > **Endpoints and Users** > **Registered Endpoints**.

You can filter on attributes such as **Identity**, **Endpoint ID**, **Identity Group**, **Endpoint Profile** and you can generate a report.

You can query the endpoint database for endpoints that are assigned to the **Registered Devices** endpoint identity group. You can also generate reports for specific users that have the **Portal User** attribute set to a non null value.

The **Registered Endpoints** report provides information about a list of endpoints that are registered through device registration portals by a specific user for a selected period of time.

CHAPTER 11

Secure Access

- Define Network Devices in Cisco ISE, on page 903
- Third-Party Network Device Support in Cisco ISE, on page 919
- Manage Network Device Groups, on page 926
- Network Device Groups, on page 928
- Import Templates in Cisco ISE, on page 931
- IPsec Security to Secure Communication Between Cisco ISE and NAD, on page 935
- Mobile Device Manager Interoperability with Cisco ISE, on page 945
- Set Up Mobile Device Management Servers with Cisco ISE, on page 953

Define Network Devices in Cisco ISE

A network device, such as a switch or a router, is an authentication, authorization, and accounting (AAA) client that sends AAA service requests to Cisco ISE. Defining network devices in Cisco ISE enables interactions between Cisco ISE and network devices.

Configure network devices for RADIUS or TACACS AAA, and Simple Network Management Protocol (SNMP) for the Profiling service to collect Cisco Discovery Protocol and Link Layer Discovery Protocol (LLDP) attributes for profiling endpoints, and TrustSec attributes for Cisco TrustSec devices. A network device that is not defined in Cisco ISE cannot receive AAA services from Cisco ISE.

From the Cisco ISE main menu, choose **Administration** > **Network Resources** > **Network Devices**, and click **Add**. In the **New Network Device** window that is displayed, enter the following details to define a network device:

- Select the vendor profile that fits the network device. The profile includes predefined configurations for the device, such as settings for URL redirect and change of authorization.
- Configure the RADIUS protocol for RADIUS authentications. When Cisco ISE receives a RADIUS request from a network device, it looks for the corresponding device definition to retrieve the configured shared secret. If Cisco ISE finds the device definition, it obtains the configured shared secret on the device and matches it against the shared secret in the request to authenticate access. If the shared secrets match, the RADIUS server processes the request further based on the policy and configuration. If the shared secrets do not match, a reject response is sent to the network device. A failed authentication report is generated, which provides the failure reason.
- Configure the TACACS+ protocol for TACACS+ authentications. When Cisco ISE receives a TACACS+ request from a network device, it looks for the corresponding device definition to retrieve the shared secret that is configured. If it finds the device definition, it obtains the shared secret that is configured

on the device and matches it against the shared secret in the request to authenticate access. If the shared secrets match, the TACACS+ server processes the request further based on the policy and configuration. If they do not match, a reject response is sent to the network device. A failed authentication report is generated, which provides the failure reason.

- You can configure the Simple Network Management Protocol (SNMP) in the network device definition for the Profiling service to communicate with the network devices and profile endpoints that are connected to the network devices.
- You must define Cisco TrustSec-enabled devices in Cisco ISE to process requests from TrustSec-enabled devices that can be part of the Cisco TrustSec solution. Any switch that supports the Cisco TrustSec solution is a Cisco TrustSec-enabled device.

  Cisco TrustSec devices do not use IP addresses. Instead, you must define other settings so that Cisco TrustSec devices can communicate with Cisco ISE.

  Cisco TrustSec-enabled devices use the TrustSec attributes to communicate with Cisco ISE. Cisco TrustSec-enabled devices, such as the Cisco Nexus 7000 Series Switches, Cisco Catalyst 6000 Series Switches, Cisco Catalyst 4000 Series Switches, and Cisco Catalyst 3000 Series Switches are authenticated using the Cisco TrustSec attributes that you define while adding Cisco TrustSec devices.

Note When you configure a network device on Cisco ISE, we recommend that you do not include a backslash (\) as part of the shared secret. This is because when you upgrade Cisco ISE, the backslash will not appear in the shared secret. However, if you reimage Cisco ISE instead of upgrading it, the backslash appears in the shared secret.

Define a Default Network Device in Cisco ISE

Cisco ISE supports the default device definition for RADIUS and TACACS authentications. You can define a default network device that Cisco ISE can use if it does not find a device definition for a particular IP address. This feature enables you to define a default RADIUS or TACACS shared secret and the level of access for newly provisioned devices.

Note We recommend that you add the default device definition only for basic RADIUS and TACACS authentications. For advanced flows, you must add a separate device definition for each network device.

Cisco ISE looks for the corresponding device definition to retrieve the shared secret that is configured in the network device definition when it receives a RADIUS or TACACS request from a network device.

Cisco ISE performs the following procedure when a RADIUS or TACACS request is received:

1. Looks for a specific IP address that matches the one in the request.
2. Looks up the ranges to see if the IP address in the request falls within the range that is specified.
3. If both step 1 and 2 fail, it uses the default device definition (if defined) to process the request.

Cisco ISE obtains the shared secret that is configured in the device definition for that device and matches it against the shared secret in the RADIUS or TACACS request to authenticate access. If no device definitions are found, Cisco ISE obtains the shared secret from the default network device definition and processes the RADIUS or TACACS request.

Network Devices

The windows described in the following sections enable you to add and manage network devices in Cisco ISE.

Network Device Definition Settings

The following tables describe the fields in the **Network Devices** window, which you can use to configure a network access device in Cisco ISE. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Devices**, and click **Add**.

Network Device Settings

The following table describes the fields in the **New Network Devices** window.

Table 126: Network Device Settings

Field Name	Description
Name	Enter a name for the network device. You can provide a descriptive name to the network device, which is different from the hostname of the device. The device name is a logical identifier. **Note** If needed, the name of a device can be changed after it is configured.
Description	Enter a description for the device.

Field Name	Description
IP Address or **IP Range**	Choose one of the following from the drop-down list and enter the required values in the fields displayed: - **IP Address**: Enter a single IP address (IPv4 or IPv6 address) and a subnet mask. - **IP Range**: Enter the required IPv4 address range. To exclude IP addresses during authentication, enter an IP address or IP address range in the **Exclude** field. The following are the guidelines for defining the IP addresses and subnet masks, or IP address ranges: - You can define a specific IP address, or an IP range with a subnet mask. If device A has an IP address range defined, you can configure another device, B, with an individual address from the range that is defined in device A. - You can define IP address ranges in all the octets. You can use a hyphen (-) or an asterisk (*) as wildcard to specify a range of IP addresses. For example, *.*.*.*, 1-10.1-10.1-10.1-10, or 10-11.*.5.10-15. - You can exclude a subset of IP address range from the configured range in a scenario where that subset has already been added, for example, 10.197.65.*/10.197.65.1, or 10.197.65.* exclude 10.197.65.1. - You can configure up to 40 IP addresses or IP ranges for each network device. - You cannot define two devices with the same specific IP addresses. - You cannot define two devices with the same IP range. The IP ranges must not overlap either partially or completely.
Device Profile	Choose the vendor of the network device from the drop-down list. Use the tooltip next to the drop-down list to see the flows and services that the selected vendor's network devices support. The tooltip also displays the RADIUS Change of Authorization (CoA) port and type of URL redirect that is used by the device. These attributes are defined in the device type's network device profile.
Model Name	Choose the device model from the drop-down list. Use the model name as one of the parameters while checking for conditions in rule-based policies. This attribute is present in the device dictionary.
Software Version	Choose the version of the software running on the network device from the drop-down list. You can use the software version as one of the parameters while checking for conditions in rule-based policies. This attribute is present in the device dictionary.
Network Device Group	In the **Network Device Group** area, choose the required values from the **Location**, **IPsec**, and **Device Type** drop-down lists. If you do not specifically assign a device to a group, it becomes a part of the default device groups (root network device groups), which is **All Locations** by location and **All Device Types** by device type.

Note While using a filter to choose and delete a Network Access Device (NAD) from your Cisco ISE deployment, clear your browser cache to ensure that only chosen NADs are deleted.

RADIUS Authentication Settings

The following table describes the fields in the **RADIUS Authentication Settings** area.

Table 127: Fields in the RADIUS Authentication Settings Area

Field Name	Usage Guidelines
RADIUS UDP Settings	
Protocol	Displays **RADIUS** as the selected protocol.
Shared Secret	Enter the shared secret for the network device. The shared secret is the key that is configured on the network device using the **radius-host** command with the **pac** option. **Note** The length of the shared secret must be equal to or greater than the value configured in the **Minimum RADIUS Shared Secret Length** field in the **Device Security Settings** window (**Administration > Network Resources > Network Devices > Device Security Settings**). For a RADIUS server, the best practice is to have 22 characters. For new installations and upgraded deployments, the shared secret length is four characters by default. You can change this value in the **Device Security Settings** window.
Use Second Shared Secret	Specify a second shared secret to be used by the network device and Cisco ISE. **Note** Although Cisco TrustSec devices can take advantage of the dual shared secrets (keys), Cisco TrustSec CoA packets sent by Cisco ISE will always use the first shared secret (key). To enable the use of the second shared secret, choose the Cisco ISE node from which the Cisco TrustSec CoA packets must be sent to the Cisco TrustSec device. Configure the Cisco ISE node to be used for this task in the **Send From** drop-down list in the **Work Centers** > **Device Administration** > **Network Resources** > **Network Devices** > **Add** > **Advanced TrustSec Settings** window. You can select a primary administration node (PAN) or a policy service node (PSN). If the chosen PSN node is down, the PAN sends the Cisco TrustSec CoA packets to the Cisco TrustSec device. **Note** The Second Shared Secret feature for RADIUS Access Request works only for packets containing the **Message-Authenticator** field.

Field Name	Usage Guidelines
CoA Port	Specify the port to be used for RADIUS CoA. The default CoA port for the device is defined in the network device profile that is configured for a network device (**Administration** > **Network Resources** > **Network Device Profiles** > **Network Resources** > **Network Device Profiles**). Click **Set To Default** to use the default CoA port. **Note** If you modify the CoA port specified in the **Network Devices** window (**Administration** > **Network Resources** > **Network Devices**) under **RADIUS Authentication Settings**, make sure that you specify the same CoA port for the corresponding profile in the **Network Device Profile** window (**Administration** > **Network Resources** > **Network Device Profiles**).
RADIUS DTLS Settings	
DTLS Required	If you check the **DTLS Required** check box, Cisco ISE processes only the DTLS requests from this device. If this option is disabled, Cisco ISE processes both UDP and DTLS requests from this device. RADIUS DTLS provides improved security for Secure Sockets Layer (SSL) tunnel establishment and RADIUS communication.
Shared Secret	Displays the shared secret that is used for RADIUS DTLS. This value is fixed and used to compute the Message Digest 5 (MD5) integrity checks.
CoA Port	Specify the port to be used for RADIUS DTLS CoA.
Issuer CA of ISE Certificates for CoA	Choose the Certificate Authority to be used for RADIUS DTLS CoA from the drop-down list.
DNS Name	Enter the DNS name of the network device. If the **Enable RADIUS/DTLS Client Identity Verification** option is enabled in the **RADIUS Settings** window (**Adminstration** > **System** > **Settings** > **Protocols** > **RADIUS**, Cisco ISE compares this DNS name with the DNS name that is specified in the client certificate to verify the identity of the network device.
General Settings	
Enable KeyWrap	Check the **Enable KeyWrap** check box only if KeyWrap algorithms are supported by the network device. The network device must be compatible with AES KeyWrap RFC (RFC 3394). This option is used to increase the RADIUS security through an AES KeyWrap algorithm.
Key Encryption Key	Enter the encryption key that is used for session encryption (secrecy).
Message Authenticator Code Key	Enter the key that is used for keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages.

Field Name	Usage Guidelines
Key Input Format	Click one of the following radio buttons: • **ASCII**: The value that is entered in the **Key Encryption Key** field must be 16 characters (bytes) in length, and the value that is entered in the **Message Authenticator Code Key** field must be 20 characters (bytes) in length. • **Hexadecimal**: The value that is entered in the **Key Encryption Key** field must be 32 characters (bytes) in length, and the value that is entered in the **Message Authenticator Code Key** field must be 40 characters (bytes) in length. You can specify the key input format that you want to use to enter the Key Encryption Key and Message Authenticator Code Key so that it matches the configuration on the network device. The value that you specify must be the correct (full) length for the key, and shorter values are not permitted.

TACACS Authentication Settings

Table 128: Fields in the TACACS Authentication Settings Area

Field Name	Usage Guidelines
Shared Secret	A string of text that is assigned to a network device when TACACS+ protocol is enabled. The user must enter the text before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
Retired Shared Secret is Active	Displayed when the retirement period is active.
Retire	Retires an existing shared secret instead of ending it. When you click **Retire**, a dialog box is displayed. You can click either **Yes** or **No**.
Remaining Retired Period	(Available only if you click **Yes** in the **Retire** dialog box) Displays the default value that is specified in **Work Centers** > **Device Administration** > **Settings** > **Connection Settings** > **Default Shared Secret Retirement Period.** You can change the default value, as necessary. The old shared secret remains active for the specified number of days.
End	(Available only if you click **Yes** in the **Retire** dialog box) Ends the retirement period and terminates the old shared secret.
Enable Single Connect Mode	Check the **Enable Single Connect Mode** check box to use a single TCP connection for all TACACS communications with the network device. Click one of the following radio buttons: • **Legacy Cisco Devices** • **TACACS Draft Compliance Single Connect Support** **Note** If you disable **Single Connect Mode**, Cisco ISE uses a new TCP connection for every TACACS request.

SNMP Settings

The following table describes the fields in the **SNMP Settings** section.

Table 129: Fields in the SNMP Settings Area

Field Name	Usage Guidelines
SNMP Version	Choose one of the following options from the **SNMP Version** drop-down list: • **1**: SNMPv1 does not support informs. • **2c** • **3**: SNMPv3 is the most secure model because it allows packet encryption when you choose **Priv** in the **Security Level** field. **Note** If you have configured your network device with SNMPv3 parameters, you cannot generate the **Network Device Session Status** summary report that is provided by the monitoring service (**Operations** > **Reports** > **Diagnostics** > **Network Device Session Status**). You can generate this report successfully if your network device is configured with SNMPv1 or SNMPv2c parameters.
SNMP RO Community	(Applicable only for SNMP versions 1 and 2c) Enter the Read Only Community string that provides Cisco ISE with a particular type of access to the device. **Note** The caret (circumflex ^) symbol is not allowed.
SNMP Username	(Only for SNMP Version 3) Enter the SNMP username.
Security Level	(Only for SNMP Version 3) Choose one the following options from the **Security Level** drop-down list: • **Auth**: Enables MD5 or Secure Hash Algorithm (SHA) packet authentication. • **No Auth**: No authentication and no privacy security level. • **Priv**: Enables Data Encryption Standard (DES) packet encryption.
Auth Protocol	(Only for SNMP Version 3 when the security levels **Auth** or **Priv** are selected) Choose the authentication protocol that you want the network device to use from the **Auth Protocol** drop-down list. • **MD5** • **SHA**
Auth Password	(Only for SNMP Version 3 when the **Auth** or **Priv** security levels are selected) Enter the authentication key. It must be at least eight characters in length. Click **Show** to display the authentication password that is already configured for the device. **Note** The caret (circumflex ^) symbol cannot be used.

Field Name	Usage Guidelines
Privacy Protocol	(Only for SNMP Version 3 when **Priv** security level is selected) Choose one of the following options from the **Privacy Protocol** drop-down list: • **DES** • **AES128** • **AES192** • **AES256** • **3DES**
Privacy Password	(Only for SNMP Version 3 when **Priv** security level is selected) Enter the privacy key. Click **Show** to display the privacy password that is already configured for the device. **Note** The caret (circumflex ^) symbol cannot be used.
Polling Interval	Enter the polling interval, in seconds. The default value is 3600.
Link Trap Query	Check the **Link Trap Query** check box to receive and interpret linkup and linkdown notifications that are received through the SNMP trap.
Mac Trap Query	Check the **Link Trap Query** check box to receive and interpret MAC notifications received through the SNMP trap.
Originating Policy Services Node	Choose the Cisco ISE server to be used to poll for SNMP data, from the **Originating Policy Services Node** drop-down list. The default value for this field is **Auto**. Overwrite the setting by choosing a specific value from the drop-down list.

Advanced TrustSec Settings

The following table describes the fields in the **Advanced TrustSec Settings** section.

Table 130: Fields in the Advanced TrustSec Settings Area

Field Name	Usage Guidelines
Device Authentication Settings	
Use Device ID for TrustSec Identification	Check the **Use Device ID for TrustSec Identification** check box if you want the device name to be listed as the device identifier in the **Device ID** field.
Device ID	You can use this field only if you have not checked the **Use Device ID for TrustSec Identification** check box.
Password	Enter the password that you have configured in the Cisco TrustSec device's CLI to authenticate the Cisco TrustSec device. Click **Show** to display the password.
HTTP REST API Settings	

Field Name	Usage Guidelines
Enable HTTP REST API	Check the **Enable HTTP REST API** check box to use the HTTP REST API to provide the required Cisco TrustSec information to the network devices. This enhances the efficiency and ability to download large configurations in a short time as compared to the RADIUS protocol. It also improves reliability by using TCP over UDP.
Username	Enter the username that you have configured in the Cisco TrustSec device's CLI to authenticate the Cisco TrustSec device. The username cannot contain special characters such as space ! % ^ : ; , [{ | }] ` " = < > ?
Password	Enter the password that you have configured in the Cisco TrustSec device's CLI to authenticate the Cisco TrustSec device.
TrustSec Device Notification and Updates	
Device ID	You can use this field only if you have not checked the **Use Device ID for TrustSec Identification** check box.
Password	Enter the password that you have configured in the Cisco TrustSec device's CLI to authenticate the Cisco TrustSec device. Click **Show** to display the password.
Download Environment Data Every <...>	Specify the time interval at which the device must download its environment data from Cisco ISE, by choosing the required values from the drop-down lists in this area. You can choose the time interval in seconds, minutes, hours, days, or weeks. The default value is one day.
Download Peer Authorization Policy Every <...>	Specify the time interval at which the device must download the peer authorization policy from Cisco ISE by choosing the required values from the drop-down lists in this area. You can specify the time interval in seconds, minutes, hours, days, or weeks. The default value is one day.
Reauthentication Every <...>	Specify the time interval at which the device reauthenticates itself against Cisco ISE after the initial authentication, by choosing the required values from the drop-down lists in this area. You can configure the time interval in seconds, minutes, hours, days, or weeks. For example, if you enter 1000 seconds, the device authenticates itself against Cisco ISE every 1000 seconds. The default value is one day.
Download SGACL Lists Every <...>	Specify the time interval at which the device downloads SGACL lists from Cisco ISE, by choosing the required values from the drop-down lists in this area. You can configure the time interval in seconds, minutes, hours, days, or weeks. The default value is one day.
Other TrustSec Devices to Trust This Device (TrustSec Trusted)	Check the **Other TrustSec Devices to Trust This Device** check box to allow all the peer devices to trust this Cisco TrustSec device. If this check box is not checked, the peer devices do not trust this device, and all the packets that arrive from this device are colored or tagged accordingly.

Field Name	Usage Guidelines
Send Configuration Changes to Device	Check the **Send Configuration Changes to Device** check box if you want Cisco ISE to send Cisco TrustSec configuration changes to the Cisco TrustSec device using CoA or CLI (SSH). Click the **CoA** or **CLI (SSH)** radio button, as required. Click the **CoA** radio button if you want Cisco ISE to send the configuration changes to the Cisco TrustSec device using CoA. Click the **CLI (SSH)** radio button if you want Cisco ISE to send the configuration changes to the Cisco TrustSec device using the CLI (using the SSH connection). For more information, see Push Configuration Changes to Non-CoA Supporting Devices, on page 1112.
Send From	From the drop-down list, choose the Cisco ISE node from which the configuration changes must be sent to the Cisco TrustSec device. You can select a PAN or a PSN. If the PSN that you choose is down, the configuration changes are sent to the Cisco TrustSec device using the PAN.
Test Connection	You can use this option to test the connectivity between the Cisco TrustSec device and the selected Cisco ISE node (PAN or PSN).
SSH Key	To use this feature, open an SSHv2 tunnel from Cisco ISE to the network device, and use the device's CLI to retrieve the SSH key. You must copy this key and paste it in the **SSH Key** field for validation. For more information, see SSH Key Validation, on page 1113.
Device Configuration Deployment	
Include this device when deploying Security Group Tag Mapping Updates	Check the **Include this device when deploying Security Group Tag Mapping Updates** check box if you want the Cisco TrustSec device to obtain the IP-SGT mappings using the device interface credentials.
EXEC Mode Username	Enter the username that you use to log in to the Cisco TrustSec device.
EXEC Mode Password	Enter the device password. Click **Show** to view the password. **Note** We recommend that you avoid using the % character in passwords, including in the EXEC modes and Enable mode passwords to avoid security vulnerabilities.
Enable Mode Password	(Optional) Enter the enable password that is used to edit the configuration of the Cisco TrustSec device in privileged EXEC mode. Click **Show** to view the password.
Out Of Band TrustSec PAC	
Issue Date	Displays the issuing date of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device.

Field Name	Usage Guidelines
Expiration Date	Displays the expiration date of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device.
Issued By	Displays the name of the issuer (a Cisco TrustSec administrator) of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device.
Generate PAC	Click the **Generate PAC** button to generate the out-of-band Cisco TrustSec PAC for the Cisco TrustSec device.

Default Network Device Definition Settings

The following table describes the fields in the **Default Network Device** window, with which you configure a default network device that Cisco ISE can use for RADIUS or TACACS+ authentication. Choose one of the following navigation paths:

- **Administration** > **Network Resources** > **Network Devices** > **Default Device**
- **Work Centers** > **Device Administration** > **Network Resources** > **Default Devices**

Table 131: Fields in the Default Network Device Window

Field Name	Usage Guidelines
Default Network Device Status	Choose **Enable** from the **Default Network Device Status** drop-down list to enable the default network device definition. **Note** If the default device is enabled, you must enable either the RADIUS or the TACACS+ authentication settings by checking the relevant check box in the window.
Device Profile	Displays **Cisco** as the default device vendor.
RADIUS Authentication Settings	
Enable RADIUS	Check the **Enable RADIUS** check box to enable RADIUS authentication for the device.
RADIUS UDP Settings	
Shared Secret	Enter a shared secret. The shared secret can be up to 127 characters in length. The shared secret is the key that you have configured on the network device using the **radius-host** command with the **pac** keyword. **Note** The length of the shared secret must be equal to or greater than the value configured in the **Minimum RADIUS Shared Secret Length** field in the **Device Security Settings** window (**Administration** > **Network Resources** > **Network Devices** > **Device Security Settings**). By default, this value is four characters for new installations and upgraded deployments. For the RADIUS server, the best practice is to have 22 characters.
RADIUS DTLS Settings	

Field Name	Usage Guidelines
DTLS Required	If you check the **DTLS Required** check box, Cisco ISE processes only the DTLS requests from this device. If this option is disabled, Cisco ISE processes both UDP and DTLS requests from this device. RADIUS DTLS provides improved security for SSL tunnel establishment and RADIUS communication.
Shared Secret	Displays the shared secret that is used for RADIUS DTLS. This value is fixed and is used to compute the MD5 integrity checks.
Issuer CA of ISE Certificates for CoA	Choose the certificate authority to be used for RADIUS DTLS CoA from the **Issuer CA of ISE Certificates for CoA** drop-down list.
General Settings	
Enable KeyWrap	(Optional) Check the **Enable KeyWrap** check box only if KeyWrap algorithms are supported on the network device, which increases RADIUS security through an AES KeyWrap algorithm.
Key Encryption Key	Enter an encryption key to be used for session encryption (secrecy) when you enable KeyWrap.
Message Authenticator Code Key	Enter the key that is used for keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages when you enable KeyWrap.
Key Input Format	Choose one of the following formats by clicking the corresponding radio button, and enter values in the **Key Encryption Key** and **Message Authenticator Code Key** fields: • **ASCII**: The **Key Encryption Key** must be 16 characters (bytes) in length, and the **Message Authenticator Code Key** must be 20 characters (bytes) in length. • **Hexadecimal**: The **Key Encryption Key** must be 32 bytes in length, and the **Message Authenticator Code Key** must be 40 bytes in length. Specify the key input format that you want to use to enter the Key Encryption Key and Message Authenticator Code Key so that it matches the configuration on the network device. The value that you specify must be the correct (full) length for the key. Shorter values are not permitted.
TACACS Authentication Settings	
Shared Secret	Enter a string of text to assign to a network device when the TACACS+ protocol is enabled. Note that a user must enter the text before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
Retired Shared Secret is Active	Displayed when the retirement period is active.

Field Name	Usage Guidelines
Retire	Retires an existing shared secret instead of ending it. When you click **Retire**, a dialog box is displayed. Click **Yes** or **No**.
Remaining Retired Period	(Optional) Available only if you click **Yes** in the **Retire** dialog box. Displays the default value that is specified in the **Work Centers** > **Device Administration** > **Settings** > **Connection Settings** > **Default Shared Secret Retirement Period** window. You can change the default values. This allows a new shared secret to be entered. The old shared secret remains active for the specified number of days.
End	(Optional) Available only if you select **Yes** in the **Remaining Retired Period** dialog box. Ends the retirement period and terminates the old shared secret.
Enable Single Connect Mode	Check the **Enable Single Connect Mode** check box to use a single TCP connection for all TACACS+ communication with the network device. Click one of the following the radio buttons: • **Legacy Cisco Devices** • **TACACS Draft Compliance Single Connect Support**. **Note** If you disable this field, Cisco ISE uses a new TCP connection for every TACACS+ request.

Network Device Import Settings

The following table describes the fields in the **Import Network Devices** window, which you can use to import network device details into Cisco ISE. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Devices**. In the **Network Devices** window, click **Import**.

Table 132: Import Network Devices Settings

Field Name	Usage Guidelines
Generate a Template	Click **Generate a Template** to create a comma-separated value (CSV) template file. Update the template with network devices information in the CSV format and save it locally. Then, use the edited template to import network devices into any Cisco ISE deployment.
File	Click **Choose File** to choose the CSV file that you have recently created, or previously exported from a Cisco ISE deployment. You can import network devices into another Cisco ISE deployment with new and updated network devices information, by using the **Import** option.
Overwrite Existing Data with New Data	Check the **Overwrite Existing Data with New Data** check box to replace the existing network devices with the devices in your import file. If you do not check this check box, new network device definitions that are available in the import file are added to the network device repository. Duplicate entries are ignored.

Field Name	Usage Guidelines
Stop Import on First Error	Check the **Stop Import on First Error** check box if you want Cisco ISE to discontinue import when it encounters an error during import. Cisco ISE imports network devices until the time of an error. If this check box is not checked and an error is encountered, the error is reported and Cisco ISE continues to import the remaining devices.

Add a Network Device in Cisco ISE

You can add a network device in Cisco ISE or use the default network device.

You can also add a network device in the **Network Devices** (**Work Centers** > **Device Administration** > **Network Resources** > **Network Devices**) window.

Before you begin

The AAA function must be enabled on the network device to be added. See Command to Enable AAA Functions, on page 1332.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Devices**.

Step 2 Click **Add**.

Step 3 Enter the corresponding values in the **Name**, **Description**, and **IP Address** fields.

Step 4 Choose the required values from the **Device Profile**, **Model Name**, **Software Version**, and **Network Device Group** drop-down lists.

Step 5 (Optional) Check the **RADIUS Authentication Settings** check box to configure the RADIUS protocol for authentication.

Step 6 (Optional) Check the **TACACS Authentication Settings** check box to configure the TACACS protocol for authentication.

Step 7 (Optional) Check the **SNMP Settings** check box to configure SNMP for the Cisco ISE profiling service to collect information from the network device.

Step 8 (Optional) Check the **Advanced Trustsec Settings** check box to configure a Cisco TrustSec-enabled device.

Step 9 Click **Submit**.

Import Network Devices into Cisco ISE

To enable Cisco ISE to communicate with network devices, you must add device definitions of the network devices in Cisco ISE. Import device definitions of network devices into Cisco ISE through the **Network Devices** window (From the main menu, choose **Administration** > **Network Resources** > **Network Devices**).

Import a list of device definitions into a Cisco ISE node using a comma-separated value (CSV) file. A CSV template file is available when you click **Import** in the **Network Devices** window. Download this file, enter the required device definitions, and then upload the edited file through the **Import** window.

You cannot execute multiple imports of the same resource type at the same time. For example, you cannot concurrently import network devices from two different import files.

When you import a CSV file of device definitions, you can either create new records or update existing records by clicking the **Overwrite Existing Data with New Data** option.

Import templates may vary in each Cisco ISE. Do not import CSV files of network devices that have exported from a different Cisco ISE release. Enter the details of the network devices in the CSV template file for your release, and import this file into Cisco ISE.

Note You can import the network devices with IP ranges in all the octets.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **Network Devices**.

Step 2 Click **Import**.

Step 3 In the **Import Network Devices** window that is displayed, click **Generate A Template** to download a CSV file that you can edit and then import it into Cisco ISE with the required details.

Step 4 Click **Choose File** to choose the CSV file from the system that is running the client browser.

Step 5 (Optional) Check the for **Overwrite Existing Data with New Data** and **Stop Import on First Error**check boxes, as required.

Step 6 Click **Import**.

After the file import is complete, Cisco ISE displays a summary message. This message includes the import status (successful or unsuccessful), number of errors encountered, if any, and the total processing time taken for the file import process.

Export Network Devices from Cisco ISE

Export the device definitions of the network devices that are available in a Cisco ISE node in the form of a CSV file. You can then import this CSV file into another Cisco ISE node so that the device definitions are available to the required Cisco ISE nodes.

Note You can export the network devices with IP ranges in all the octets.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration** > **Network Resources** > **Network Devices**.

Step 2 Click **Export**.

Step 3 Export the device definitions for the network devices added to the Cisco ISE node by performing one of the following actions.

- Check the check boxes next to the devices that you want to export, choose **Export Selected** from the **Export** drop-down list.
- Choose **Export All** from the **Export** drop-down list to export all the network devices that are added to the Cisco ISE node.

Step 4 In both cases, a CSV file of device definitions downloads to your system.

Troubleshoot Network Device Configuration Issues

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **Evaluate Configuration Validator**.

Step 2 Enter the IP address of the network device that you want to evaluate in the **Network Device IP** field.

Step 3 Check the check boxes and click the radio buttons next to the configuration options you want to compare against the recommended template.

Step 4 Click **Run**.

Step 5 In the **Progress Details...** area, click **Click Here to Enter Credentials**.

Step 6 In the **Credentials Window** dialog box, enter the connection parameters and credentials that are required to establish a connection with the network devices.

Step 7 Click **Submit**.

Step 8 (Optional) To cancel the workflow, click **Click Here to Cancel the Running Workflow** in the **Progress Details...** window.

Step 9 (Optional) Check the check boxes next to the interfaces that you want to analyze, and click **Submit**.

Step 10 (Optional) Click **Show Results Summary** for details of the configuration evaluation.

The Execute Network Device Command Diagnostic Tool

The Execute Network Device Command diagnostic tool allows you to run the **show** command on any network device.

The results that are displayed are the same as what you would see on a console. The tool enables you to identify problems, if any, in a device configuration.

Use this tool to validate the configuration of any network device, or if you are want to know how a network device is configured.

To access the Execute Network Device Command diagnostic tool, choose one of the following navigation paths:

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **Execute Network Device Command**.In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Profiler** > **Troubleshoot** > **Execute Network Device Command**.
2. In the **Execute Network Device Command** window that is displayed, enter the IP address of the network device and the **show** command that you want to run in the corresponding fields.
3. Click **Run**.

Third-Party Network Device Support in Cisco ISE

Cisco ISE supports third-party network access devices (NADs) by using network device profiles. A NAD profile defines the capabilities of a third-party device with a simplified policy configuration, regardless of the vendor-side implementation. A network device profile contains the following:

- The protocols that the network device supports, such as RADIUS, TACACS+, and Cisco TrustSec. You can import into Cisco ISE any vendor-specific RADIUS dictionaries that exist for the network device.
- The attributes and values that the device uses for various authentication flows such as Wired MAB and 802.1X. These attributes and values allow Cisco ISE to detect the right authentication flow for your device according to the attributes that the network device uses.
- The Change of Authorization (CoA) capabilities of the network device. While the RADIUS protocol RFC 5176 defines a CoA request, the attributes used in a CoA request vary depending on the network device. Most non-Cisco devices with RFC 5176 support the *Push* and *Disconnect* functions. For devices that do not support the RADIUS CoA type, Cisco ISE also supports SNMP CoA.
- The attributes and protocols that the network device uses for MAB flows. Network devices from different vendors perform MAB authentication differently.
- The VLAN and ACL permissions that are used by the device. When you save the profile, Cisco ISE automatically generates authorization profiles for each configured permission.
- URL redirection technique information. URL redirection is necessary for advanced flows such as Bring Your Own Device (BYOD), guest access, and posture services. Two types of URL redirections are found on a network device—static and dynamic. For static URL redirection, you can copy and paste the Cisco ISE portal URL into the configuration. For dynamic URL redirection, Cisco ISE uses a RADIUS attribute to tell the network device where to redirect to.

  If the network device does not support both dynamic and static URL redirects, Cisco ISE provides an Auth VLAN configuration by which URL redirect is simulated. The Auth VLAN configuration is based on DHCP and DNS services running in Cisco ISE.

After you have defined your network devices in Cisco ISE, configure these device profiles or use the preconfigured device profiles that are offered by Cisco ISE to define the capabilities that Cisco ISE uses to enable basic authentication flows, and advanced flows such as Profiler, Guest, BYOD, MAB, and Posture.

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.

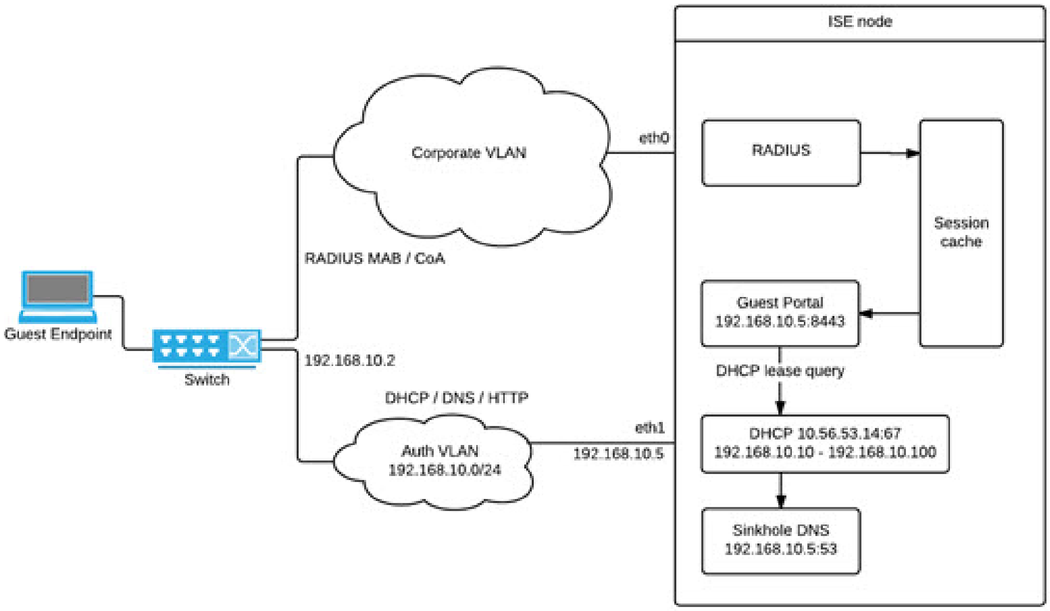
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

Multiple VLANs may be connected to one network interface card by configuring a VLAN IP helper from the NAD configuration. For more information about configuring an IP helper, see the administration guide for the network device for instructions. For guest access flows that include VLANs with IP helpers, define a guest portal, and select that portal in an authorization profile that is bound to MAB authorization. For more information about guest portals, see Cisco ISE Guest Services, on page 477.

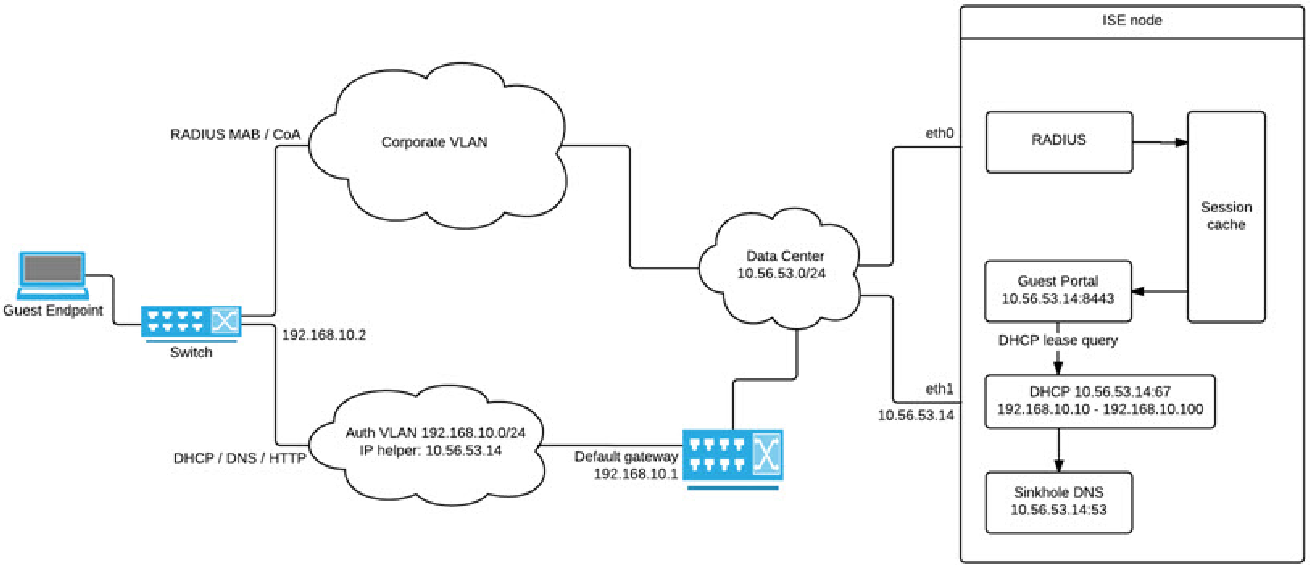
The following diagram displays a basic network setup when an Auth VLAN is defined (the Auth VLAN is connected directly to a Cisco ISE node).

Figure 31: Auth VLAN Connected to Cisco ISE Node


ISE node
Corporate VLAN
eth0
RADIUS
Session cache
RADIUS MAB / CoA
Guest Endpoint
Switch
192.168.10.2
Guest Portal 192.168.10.5:8443
DHCP lease query
DHCP / DNS / HTTP
eth1
Auth VLAN 192.168.10.0/24
192.168.10.5
DHCP 10.56.53.14:67 192.168.10.10 - 192.168.10.100
Sinkhole DNS 192.168.10.5:53

The following diagram displays a network with Auth VLAN and an IP helper.

Figure 32: Auth VLAN Configured with IP Helper


ISE node
RADIUS MAB / CoA
Corporate VLAN
eth0
RADIUS
Session cache
Guest Endpoint
Switch
192.168.10.2
Data Center 10.56.53.0/24
Guest Portal 10.56.53.14:8443
DHCP lease query
eth1
10.56.53.14
DHCP 10.56.53.14:67 192.168.10.10 - 192.168.10.100
DHCP / DNS / HTTP
Auth VLAN 192.168.10.0/24 IP helper: 10.56.53.14
Default gateway 192.168.10.1
Sinkhole DNS 10.56.53.14:53

CoA Types

Cisco ISE supports both RADIUS and SNMP CoA types. RADIUS or SNMP CoA type support is required for the NAD to work in complex flows, while it is not mandatory for basic flows.

Define the RADIUS and SNMP settings that the network device supports when you configure the NAD in Cisco ISE. Indicate the CoA type to be used for a specific flow when configuring the NAD profile. For more information about defining protocols for your NADs, see Network Device Definition Settings, on page 905. Check with your third-party supplier to verify which CoA type your NAD supports before creating the device profile and NAD profile in Cisco ISE.

Network Device Profiles

Cisco ISE supports some third-party NADs by using network device profiles. These profiles define the capabilities that Cisco ISE uses to enable basic flows, and advanced flows such as Guest, BYOD, MAB, and Posture.

Cisco ISE includes predefined profiles for network devices from several vendors. Cisco ISE 2.1 and later releases have been tested with the network devices listed in the following table.

Table 133: Vendor Devices Tested with Cisco ISE 2.1 and Later Releases

Device Type	Vendor	CoA Type	URL Redirect Type	Supported or Validated Use Cases				
				802.1X and MAB Flows	Profiler without CoA	Profiler with CoA	Posture	Guest and BYOD Flows

Wireless	Aruba 7000, InstantAP	RADIUS	Static URL	Yes	Yes	Yes	Yes	Yes
	Motorola RFS 4000	RADIUS	Dynamic URL	Yes	Yes	Yes	Yes	Yes
	HP 830	RADIUS	Static URL	Yes	Yes	Yes	Yes	Yes
	Ruckus ZD 1200	RADIUS	—	Yes	Yes	Yes	Yes	Yes
Wired	HP A5500	RADIUS	Auth VLAN provided by ISE	Yes	Yes	Yes	Yes	Yes
	HP 3800 and 2920 (ProCurve)	RADIUS	Auth VLAN provided by ISE	Yes	Yes	Yes	Yes	Yes
	Alcatel 6850	SNMP	Dynamic URL	Yes	Yes	Yes	Yes	Yes
	Brocade ICX 6610	RADIUS	Auth VLAN provided by ISE	Yes	Yes	Yes	Yes	Yes
	Juniper EX3300-24p	RADIUS	Auth VLAN provided by ISE	Yes	Yes	Yes	Yes	Yes
For other third-party NADs, you must identify the device properties and capabilities, and create custom NAD profiles in Cisco ISE.				Yes	Yes	Requires CoA support	Requires CoA support. If a wired device does not support URL redirect, Cisco ISE uses Auth VLAN. Wireless devices have not been tested with Auth VLAN.	

You must create custom NAD profiles for other third-party network devices that do not have a predefined profile. For advanced workflows such as Guest, BYOD, and Posture, the network device must support the RADIUS protocol RFC 5176, which pertains to CoA support for these flows. See the device's administration guide for information on the attributes that are required to create network device profiles in Cisco ISE.

> ISE Community Resource
>
> For information about third-party NAD profiles, see ISE Third-Party NAD Profiles and Configs.

Configure a Third-Party Network Device in Cisco ISE

Cisco ISE supports third-party NADs by using network device profiles. These profiles define the capabilities that Cisco ISE uses to enable flows such as Guest, BYOD, MAB, and Posture.

Before you begin

See Network Device Profiles, on page 922.

Step 1 Add the third-party network device to Cisco ISE (See Import Network Devices into Cisco ISE, on page 917. If you are configuring Guest, BYOD, or Posture workflows, ensure that CoA is defined and the NAD's URL redirect mechanism is configured to point to the relevant Cisco ISE portal. To configure the URL redirect, copy the Cisco ISE portal URL from the portal's landing page. For more information about configuring CoA types and URL redirects for the NAD in Cisco ISE, see Network Device Definition Settings, on page 905. In addition, see the third-party device's administration guide for instructions.

Step 2 Ensure that an appropriate NAD profile for your device is available in Cisco ISE. To view the existing profiles, choose **Administration** > **Network Resources** > **Network Device Profiles**. If an appropriate profile does not exist in Cisco ISE, create a custom profile. See Create a Network Device Profile, on page 924 for information on how to create custom profiles.

Step 3 Assign a NAD profile to the NAD that you want to configure. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Devices**. Open the device to which you want to assign a profile, and from the **Device Profile** drop-down list, choose the profile that you want to assign.

Step 4 When you configure your policy rules, set the authorization profile to the NAD profile in step 1, or **Any** if you are just using VLAN or ACL, or if you have different devices from different vendors in your network. To set the NAD profile for the authorization profile, choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**. Open the relevant authorization profile and from the **Network Device Profile** drop-down list, choose the relevant NAD profile. When using Auth VLAN for Guest flows, you should also define a guest portal and select that portal in an Authorization profile that is bound to MAB authorization—similar to regular Guest flows. For more information about guest portals, see the "Cisco ISE Guest Services" section in see Cisco ISE Guest Services, on page 477.

Create a Network Device Profile

Before you begin

- Most NADs have a vendor-specific RADIUS dictionary that provides several vendor-specific attributes, apart from the standard IETF RADIUS attributes. If the network device has a vendor-specific RADIUS dictionary, import it into Cisco ISE. See the third-party device's administration guide for instructions on which RADIUS dictionary is required. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Dictionaries** > **System** > **Radius** > **RADIUS Vendors**. To import RADIUS dictionaries, see Create RADIUS-Vendor Dictionaries, on page 1009.
- For complex flows such as Guest and Posture, the network device must support the CoA types that are defined in RFC 5176
- For information about the fields and possible values for creating a network device profile, see Network Device Profiles Settings, on page 1296.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Device Profiles**.

Step 2 Click **Add**.

Step 3 In the **New Network Device Profile** window that is displayed, enter the corresponding values in the **Name** and **Description** fields for the network device.

Step 4 From the **Vendor** drop-down list, choose the vendor of the network device.

Step 5 In the **Icon** area, click **Change Icon...** to upload an icon for the network device from your system.

Alternatively, in the **Icon** area, click **Set To Default** to use the default icon provided by Cisco ISE.

Step 6 In the **Supported Protocols** area, check the check boxes for the protocols that the device supports. Check the check boxes only for the protocols that you want to actually use. If the network device supports the RADIUS protocol, choose the RADIUS dictionary to be used in the device from **RADIUS Dictionaries** drop-down list.

Step 7 In the **Templates** area, enter relevant details:

a) Click **Authentication/Authorization** to configure the network device's default settings for flow types, attribute aliasing, and host lookup. In the new **Flow Type Conditions** area that is displayed, enter the attributes and values that your device uses for various authentication and authorization flows such as Wired MAB or 802.1X. This enables Cisco ISE to detect the correct flow type for your device according to the attributes it uses. There is no IETF standard for MAB, and different vendors use different values for Service Type. See the device's user guide or use a sniffer trace of a MAB authentication to determine the correct settings. In the **Attribute Aliasing** area, map device-specific attribute names to common names to simplify policy rules. Currently, only the Service Set Identifier (SSID) is defined. If the network device has the concept of wireless SSID, then set this to the attribute it uses. Cisco ISE maps this to an attribute called SSID in the Normalized RADIUS dictionary. This simplifies policy rule configuration because you can refer to SSID in one rule, and it works for multiple devices even if the underlying attributes are different. In the **Host Lookup** area, check the **Process Host Lookup** check box and select the relevant MAB protocols and attributes for your device, based on the instructions provided by the third-party device vendor.

b) Click **Permissions** to configure the network device's default settings for VLAN and ACL. These are automatically mapped based on the authorization profiles that you create in Cisco ISE.

c) Click **Change of Authorization (CoA)** to configure the network device's CoA capabilities.

If you choose **RADIUS** from the **CoA By** drop-down list, in the configurations area that is displayed, you must choose only static attributes. Dynamic attributes are not supported.

d) Click **Redirect** to configure the network device's URL-redirect capabilities. URL redirection is necessary for guest, BYOD, and posture services.

Step 8 Click **Submit**.

Related Topics

How to Create ISE Network Access Device Profiles

Export Network Device Profiles from Cisco ISE

Export single or multiple network device profiles that are configured in Cisco ISE in the form of an XML file. The XML file can then be edited and imported into Cisco ISE file as new network profiles.

Before you begin

See How to Create ISE Network Access Device Profiles.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Device Profiles**.

Step 2 Check the check boxes next to the devices that you want to export, and click **Export Selected**.

Step 3 A file that is named **DeviceProfiles.xml** downloads to your local hard disk.

Import Network Device Profiles into Cisco ISE

Import a single or multiple network device profiles into Cisco ISE using a single XML file with the Cisco ISE XML structure. You cannot concurrently import network device profiles from multiple import files.

Typically, you must first export an existing profile from the Cisco ISE administrator portal to use as a template. Enter your device profile details in the file, and save it as an XML file. Then, import the edited file back into Cisco ISE. To work with multiple network device profiles, export multiple profiles that are structured together as a single XML file, edit the file, and then import the profiles together to create multiple profiles in Cisco ISE.

When you import network device profiles, you can only create new records. You cannot overwrite an existing profile. To update an existing network device profile, export the existing profile from Cisco ISE, delete the profile from Cisco ISE, and then import the profile after you edit it accordingly.

Before you begin

See How to Create ISE Network Access Device Profiles.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Device Profiles**.

Step 2 Click **Import**.

Step 3 Click **Choose File** to choose the XML file from the system that is running the client browser.

Step 4 Click **Import**.

Manage Network Device Groups

The following windows enable you to configure and manage network device groups.

Network Device Group Settings

The following table describes the fields in the **Network Device Groups** window that you use to create network device groups. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Device Groups** > **All Groups**.

You can also create network device groups in the **Work Centers** > **Device Administration** > **Network Resources** > **Network Device Groups** > **All Groups** window.

Table 134: Fields in the Network Device Group Window

Field Name	Usage Guidelines
Name	Enter a name for the root network device group. For all subsequent child network device groups added to this root network device group, enter the name of this newly created network device group. You can have a maximum of six nodes in a network device group hierarchy, including the root node. Each network device group name can have a maximum of 32 characters.
Description	Enter a description for the root or the child network device group.
No. of Network Devices	The number of network devices in the network group is displayed in this column.

Network Device Group Import Settings

The following table describes the fields in the **Import** dialog box in the **Network Device Group** window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Device Groups**.

Table 135: Fields in the Network Device Groups Import Window

Field Name	Usage Guidelines
Generate a Template	Click this link to download a CSV template file. Update the template with network device group information in the same format. Save the template locally to import the network device groups into any Cisco ISE deployment.
File	Click **Choose File** and navigate to the location of the CSV file that you want to upload. The file may be new or a file that was exported from another Cisco ISE deployment. You can import network device groups from one Cisco ISE deployment to another, with new and updated network device groups information.
Overwrite Existing Data with New Data	Check this check box if you want to replace the existing network device groups with the device groups in your import file. If you do not check this check box, only the new network device groups in the import file are added to the network device group repository. Duplicate entries are ignored.
Stop Import on First Error	Check this check box to discontinue import at the first instance of encountering an error during the import. If this check box is not checked and an error is encountered, Cisco ISE reports the error and continues importing the rest of the device groups.

Network Device Groups

Cisco ISE allows you to create hierarchical network device groups. Use network device groups to logically group network devices based on various criteria, such as geographic location, device type, or its relative place in the network (such as Access Layer or Data Center).

To view the Network Device Groups window, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Device Groups**.

For example, to organize your network devices based on geographic location, group them by continent, region, or country:

- **Africa** > **Southern** > **Namibia**
- **Africa** > **Southern** > **South Africa**
- **Africa** > **Southern** > **Botswana**

Group the network devices based on the device type:

- **Africa** > **Southern** > **Botswana** > **Firewalls**
- **Africa** > **Southern** > **Botswana** > **Routers**
- **Africa** > **Southern** > **Botswana** > **Switches**

Assign network devices to one or more hierarchical network device groups. When Cisco ISE processes the ordered list of configured network device groups to determine the appropriate group to assign to a particular device, it may find that the same device profile applies to multiple device groups. In this case, Cisco ISE applies the first device group that is matched.

There is no limit on the maximum number of network device groups that you can create. You can create up to six levels of hierarchy (including the parent group) for the network device groups.

The device group hierarchy is displayed in two views, **Tree Table** and **Flat Table**. Click **Tree Table** or **Flat Table** above the list of network device groups to organize the list into the corresponding view.

In the **Tree Table** view, the root node appears at the top of the tree followed by the child groups in hierarchical order. Click **Expand All** to view all the device groups in each root group. Click **Collapse All** to view a list of only the root groups.

In the **Flat Table** view, the hierarchy of each device group is displayed in the **Group Hierarchy** column.

In both views, the number of network devices that are assigned to each child group is displayed in the corresponding **No. of Network Devices** column. Click the number to launch a dialog box that lists all the network devices that are assigned to that device group. The dialog box that is displayed also contains two buttons to move network devices from one group to another. Click **Move Devices to Another Group** to move network devices from the current group to another. Click **Add Devices to Group** to move a network device into the chosen network device group.

To add a network device group in the **Network Device Groups** window, click **Add**. In the **Parent Group** drop-down list, choose the parent group to which the network device group must be added, or choose the **Add As Root Group** option to add the new network device group as the parent group.

Note You cannot delete a device group if any devices are assigned to that device group. Before deleting a device group, you must move all the existing devices to another device group.

Root Network Device Groups

Cisco ISE includes two predefined root network device groups, **All Device Types** and **All Locations**. You cannot edit, duplicate, or delete these predefined network device groups, but you can add new device groups under them.

You can create a root Network Device Group (network device group), and then create child network device groups under the root group in the **Network Device Groups** window, as described earlier.

Network Device Attributes Used by Cisco ISE in Policy Evaluation

When you create a new network device group, a new network device attribute is added to the **Device** dictionary in **System Dictionaries** (**Policy** > **Policy Elements** > **Dictionaries**). The added device attributes are then used in policy definitions.

Cisco ISE allows you to configure authentication and authorization policies using **Device** dictionary attributes such as the device type, location, model name, or software version that is running on the network device.

Import Network Device Groups into Cisco ISE

You can import network device groups into a Cisco ISE node using a comma-separated value (CSV) file. Not that you cannot concurrently import network device groups from two different import files.

Download a CSV template from the Cisco ISE administrator portal. Enter your network device group details in the template, save the template as a CSV file, and then import the edited file into Cisco ISE.

When importing device groups, you can create new records or update existing records. When you import device groups, you can also define whether you want Cisco ISE to overwrite the existing device groups with the new groups or stop the import process when Cisco ISE encounters the first error.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Device Groups**.

Step 2 Click **Import**.

Step 3 In the dialog box, click **Choose File** to choose the CSV file from the system that is running the client browser.

To download a CSV template file for adding network device groups, click **Generate a Template**.

Step 4 To overwrite the existing network device groups, check the **Overwrite Existing Data with New Data** check box.

Step 5 Check the **Stop Import on First Error** check box.

Step 6 Click **Import**.

Export Network Device Groups from Cisco ISE

You can export network device groups that are configured in Cisco ISE in the form of a CSV file. You can then import these network device groups into another Cisco ISE node.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Device Groups** > **All Groups**.

Step 2 To export the network device groups, you can do one of the following:

- Check the check boxes next to the device groups that you want to export, and choose **Export** > **Export Selected**.
- Choose **Export** > **Export All** to export all the network device groups that are defined.

A CSV file is downloaded into your local hard disk.

Manage Network Device Groups

The following windows enable you to configure and manage network device groups.

Network Device Group Settings

The following table describes the fields in the **Network Device Groups** window that you use to create network device groups. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Device Groups** > **All Groups**.

You can also create network device groups in the **Work Centers** > **Device Administration** > **Network Resources** > **Network Device Groups** > **All Groups** window.

Table 136: Fields in the Network Device Group Window

Field Name	Usage Guidelines
Name	Enter a name for the root network device group. For all subsequent child network device groups added to this root network device group, enter the name of this newly created network device group. You can have a maximum of six nodes in a network device group hierarchy, including the root node. Each network device group name can have a maximum of 32 characters.
Description	Enter a description for the root or the child network device group.
No. of Network Devices	The number of network devices in the network group is displayed in this column.

Network Device Group Import Settings

The following table describes the fields in the **Import** dialog box in the **Network Device Group** window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Device Groups**.

Table 137: Fields in the Network Device Groups Import Window

Field Name	Usage Guidelines
Generate a Template	Click this link to download a CSV template file. Update the template with network device group information in the same format. Save the template locally to import the network device groups into any Cisco ISE deployment.
File	Click **Choose File** and navigate to the location of the CSV file that you want to upload. The file may be new or a file that was exported from another Cisco ISE deployment. You can import network device groups from one Cisco ISE deployment to another, with new and updated network device groups information.
Overwrite Existing Data with New Data	Check this check box if you want to replace the existing network device groups with the device groups in your import file. If you do not check this check box, only the new network device groups in the import file are added to the network device group repository. Duplicate entries are ignored.
Stop Import on First Error	Check this check box to discontinue import at the first instance of encountering an error during the import. If this check box is not checked and an error is encountered, Cisco ISE reports the error and continues importing the rest of the device groups.

Import Templates in Cisco ISE

Cisco ISE allows you to import a large number of network devices and network device groups using CSV files. The template contains a header row that defines the format of the fields. You must not edit this header row except to add columns mentioned in the table below.

Use the **Generate a Template** link in the relevant import flow for network devices and network device groups to download a CSV file to your local system.

Network Devices Import Template Format

The following table lists and describes the fields in the header of the import network device CSV template file.

Table 138: CSV Template Fields and Descriptions for Network Devices

Field	Usage Guidelines
Name:String(32)	Enter a name for the network device. The name must be an alphanumeric string with a maximum of 32 characters.
Description:String(256)	(Optional) Enter a description for the network device with a maximum of 256 characters.

Field	Usage Guidelines
IP Address:Subnets(a.b.c.d/m|...)	Enter the IP address and subnet mask of the network device. You can enter more than one value separated by a pipe (|) symbol. IPv4 and IPv6 addresses are supported for network device (TACACS and RADIUS) configurations and for external RADIUS server configurations. When you enter an IPv4 address, you can use ranges and subnet masks. Ranges are not supported for IPv6.
Model Name:String(32)	Enter the network device's model name with a maximum of 32 characters.
Software Version:String(32)	Enter the network device's software version with a maximum of 32 characters.
Network Device Groups:String(100)	Enter the names of existing network device groups. If it is a subgroup, it must include both the parent and subgroup, separated by a space. The string must be a maximum of 100 characters, for example, *Location>All Location>US*.
Authentication:Protocol:String(6)	Enter the authentication protocol that you want to use. The only valid value is **RADIUS** (not case-sensitive).
Authentication:Shared Secret:String(128)	(Required only if you enter a value in the **Authentication:Protocol:String(6)** field) Enter a string with a maximum of 128 characters.
EnableKeyWrap:Boolean(true|false)	This field is enabled only if KeyWrap is supported in the network device. Enter **true** or **false**.
EncryptionKey:String(ascii:16|hexa:32)	(Required if you enable KeyWrap) Enter the encryption key that is used for session encryption. ASCII values: 16 characters (bytes) long. Hexadecimal values: 32 characters (bytes) long.
AuthenticationKey:String(ascii:20|hexa:40)	(Required if you enable KeyWrap.) Enter the keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages. ASCII values: 20 characters (bytes) long. Hexadecimal values: 40 characters (bytes) long.
InputFormat:String(32)	Enter the encryption and authentication keys input format. ASCII and hexadecimal values are accepted.
SNMP:Version:Enumeration (|2c|3)	Enter the version of the SNMP protocol that the profiler service must use—1, 2c, or 3.
SNMP:RO Community:String(32)	(Required if you enter a value in the **SNMP:Version:Enumeration (|2c|3)** field). Enter a string for Read Only Community with a maximum of 32 characters
SNMP:RW Community:String(32)	(Required if you enter a value in the **SNMP:Version:Enumeration (|2c|3)** field). Enter a string for Read Write Community with a maximum of 32 characters.
SNMP:Username:String(32)	Enter a string with a maximum of 32 characters.

Field	Usage Guidelines
	(Required if you enter SNMP version 3 in the **SNMP:Version:Enumeration (|2c|3)** field) Enter **Auth**, **No Auth**, or **Priv**.
SNMP:Authentication Protocol:Enumeration(MD5|SHA)	(Required if you have entered **Auth** or **Priv** for the SNMP security level.) Enter **MD5** or **SHA**.
SNMP:Authentication Password:String(32)	(Required if you have entered **Auth** in the **SNMP:Security Level:Enumeration(Auth|No Auth|Priv)** field.) Enter a string with a maximum of 32 characters.
SNMP:Privacy Protocol:Enumeration(DES|AES128|AES192|AES256|3DES)	(Required if you have entered **Priv** in the **SNMP:Security Level:Enumeration(Auth|No Auth|Priv)** field.) Enter **DES**, **AES128**, **AES192**, **AES256**, or **3DES**.
SNMP:Privacy Password:String(32)	(Required if you have entered **Priv** in the **SNMP:Security Level:Enumeration(Auth|No Auth|Priv)** field.) Enter a string with a maximum of 32 characters.
SNMP:Polling Interval:Integer:600-86400 seconds	Enter the SNMP polling interval, in seconds. A valid value is an integer from 600 to 86400.
SNMP:Is Link Trap Query:Boolean(true|false)	Enable or disable the SNMP link trap by entering **true** or **false**.
SNMP:Is MAC Trap Query:Boolean(true|false)	Enable or disable the SNMP MAC trap by entering **true** or **false**.
SNMP:Originating Policy Services Node:String(32)	Indicate which Cisco ISE server must be used to poll for SNMP data. It is automatic by default, but you can overwrite the setting by assigning different values in this field.
Trustsec:Device Id:String(32)	Enter a Cisco Trustsec device ID, which is a string with a maximum of 32 characters.
Trustsec:Device Password:String(256)	(Required if you have entered a Cisco TrustSec device ID.) Enter a Cisco TrustSec device password, which is a string with a maximum of 256 characters.
Trustsec:Environment Data Download Interval:Integer:1-2147040000 seconds	Enter the Cisco TrustSec environment data download interval. A valid value is an integer from 1 to 2147040000.
Trustsec:Peer Authorization Policy Download Interval:Integer:1-2147040000 seconds	Enter the Cisco TrustSec peer authorization policy download interval. A valid value is an integer from 1 to 2147040000.
Trustsec:Reauthentication Interval:Integer:1-2147040000 seconds	Enter the Cisco TrustSec reauthentication interval. A valid value is an integer from 1 to 2147040000.
Trustsec:SGACL List Download Interval:Integer:1-2147040000 seconds	Enter the Cisco TrustSec security group ACL list download interval. A valid value is an integer from 1 to 2147040000.
Trustsec:Is Other Trustsec Devices Trusted:Boolean(true|false)	Indicate whether a Cisco TrustSec device is trusted by entering **true** or **false**.

Field	Usage Guidelines
Trustsec:Notify this device about Trustsec configuration changes:String(ENABLE_ALL|DISABLE_ALL)	Notify Cisco TrustSec configuration changes to the Cisco TrustSec device by entering **ENABLE_ALL** or **DISABLE_ALL** .
Trustsec:Include this device when deploying Security Group Tag Mapping Updates:Boolean(true|false)	Indicate if the Cisco TrustSec device is included in security group tag by entering **true** or **false**.
Deployment:Execution Mode Username:String(32)	Enter the user name that has privileges to edit the network device configuration. It is a string with a maximum of 32 characters.
Deployment:Execution Mode Password:String(32)	Enter the device password, which is a string with a maximum of 32 characters.
Deployment:Enable Mode Password:String(32)	Enter the password of the device that allows you to edit its configuration. It is a string with a maximum of 32 characters.
Trustsec:PAC issue date:Date	Enter the issuing date of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device.
Trustsec:PAC expiration date:Date	Etner the expiration date of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device.
Trustsec:PAC issued by:String	Enter the name of the issuer (a Cisco TrustSec administrator) of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device. It must be a string value.

Network Device Groups Import Template Format

The following table lists the fields in the template header and provides a description of the fields in the Network Device Group CSV file.

Table 139: CSV Template Fields and Descriptions for Network Device Groups

Field	Description
Name:String(100):	(Required) This field is the network device group name. It is a string with a maximum of 100 characters in length. The full name of an NDG can have a maximum of 100 characters in length. For example, if you create a subgroup India under the parent groups Global > Asia, then the full name of the NDG that you create would be Global#Asia#India. The full name cannot exceed 100 characters in length. If the full name of the NDG exceeds 100 characters in length, the NDG creation fails.
Description:String(1024)	This is an optional field. It is a string, with a maximum of 1024 characters in length.
Type:String(64):	(Required) This field is the network device group type. It is a string, with a maximum of 64 characters in length.
Is Root:Boolean(true|false):	(Required) This is a field that determines if the specific network device group is a root group. Valid value is true or false.

IPsec Security to Secure Communication Between Cisco ISE and NAD

IPsec is a set of protocols that provides security to IP. The RADIUS, and TACACS+ protocols use the MD5 hashing algorithm. For greater security, Cisco ISE offers the IPsec feature. IPsec provides secure communication by authenticating the sender, discovering any changes in data during transmission, and encrypting the data that is sent.

Cisco ISE supports IPsec in tunnel and transport modes. When you enable IPsec on a Cisco ISE interface and configure the peers, an IPsec tunnel is created between Cisco ISE and the NAD to secure the communication.

You can define a pre-shared key or use X.509 certificates for IPsec authentication. IPsec can be enabled on Gigabit Ethernet 1 through Gigabit Ethernet 5 interfaces. You can configure IPsec on only one Cisco ISE interface per PSN.

Smart licensing is enabled by default on Gigabit Ethernet 2 (e0/2—> eth2) interface. Hence, if you want to enable IP security on this interface, you must configure a different interface for smart licensing.

Note Gigabit Ethernet 0 and Bond 0 (when Gigabit Ethernet 0 and Gigabit Ethernet 1 interfaces are bonded) are management interfaces in the Cisco ISE CLI. IPsec is not supported on Gigabit Ethernet 0 and Bond 0.

Cisco ISE Releases 2.2 and later support IPsec.

Note the following points while configuring IPsec on Cisco ISE:

- Cisco ISE Releases 2.2 and later support IPsec.
- Cisco IOS Software, C5921 ESR Software (C5921_I86-UNIVERSALK9-M): The ESR 5921 configuration, by default, supports IPsec in tunnel and transport modes. Diffie-Hellman Group 14 and Group 16 are supported.

  Note The C5921 ESR software is bundled with Cisco ISE, Releases 2.2 and later. You need an ESR license to enable it. See Cisco 5921 Embedded Services Router Integration Guide for ESR licensing information.

For more information on IPsec configuration, restrictions, and support, see the Security Configuration Guide, Cisco IOS XE Cupertino 17.7.x (Catalyst 9300 Switches).

Configure RADIUS IPSec on Cisco ISE

To configure RADIUS IPSec on Cisco ISE, you must:

Step 1 Configure IP address on the interface from the Cisco ISE CLI.

Gigabit Ethernet 1 through Gigabit Ethernet 5 interfaces (Bond 1 and Bond 2) support IPSec. However, IPSec can be configured only on one interface in a Cisco ISE node.

Step 2 Add a directly connected network device to the IPSec network device group.

Note RADIUS IPSec requires the static route gateway to be directly connected through an interface of the device.

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Devices**.
b) In the **Network Devices** window, click **Add**.
c) Enter the name and IP address and subnet of the network device that you want to add in the corresponding fields.
d) From the IPSEC drop-down list, choose **Yes**.
e) Check the **RADIUS Authentication Settings** check box.
f) In the **Shared Secret** field, enter the shared secret key that you have configured on the network device.
g) Click **Save**.

Step 3 Add a separate management interface to interact with the Cisco Smart Software Manager (CSSM). See Smart Software Manager satellite for information on Embedded Services Router (ESR). To do this, from the Cisco ISE CLI, run the following command to select the corresponding management interface (Gigabit Ethernet 1 to 5 (or Bond 1 or 2)):

ise/admin# **license esr smart** {*interface*}

This interface must be able to reach Cisco.com to access the Cisco online licensing server.

To disable ise/admin# **license esr smart** on an existing interface:

- Add a new management interface.
- In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Protocols** > **IPSec**. **Enable** and **Disable** IPSec on the new interface.

Step 4 Add a network device to a directly connected gateway from the Cisco ISE CLI.

ip route [*destination network*] [*network mask*] **gateway** [*next-hop address*]

Step 5 Activate IPSec on Cisco ISE nodes.

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Protocols** > **IPSec**..

   All the Cisco ISE nodes in the deployment are listed in this window.

b) Check the check box next to the Cisco ISE node on which you want to activate IPSec, and then click the **Enable** radio button.
c) Choose the interface that you want to use for IPSec communication from the **IPSec Interface for selected nodes:** drop-down list.
d) Click the radio button for one the following authentication type for the selected Cisco ISE node:

   - **Pre-shared Key**: If you choose this option, you must enter the pre-shared key and configure the same key on the network device. Use alphanumeric characters for the pre-shared key. Special characters are not supported. For instructions on how to configure the pre-shared key on the network device, see the network device documentation. For an example of the pre-shared key configuration output, see Example: Output of Pre-shared Key Configuration on Cisco Catalyst 3850 Series Switches, on page 944.
   - **X.509 Certificates**: If you choose this option, from the Cisco ISE CLI, go to the ESR shell and configure and install X.509 Certificates for ESR 5921. Then, configure the network device for IPSec. For instructions, see Configure and Install X.509 Certificates on ESR-5921, on page 939.

e) Click **Save**.

Note You cannot modify IPSec configurations directly. To modify the IPSec tunnel or authentication when IPSec is enabled, disable the current IPSec tunnel, modify the IPSec configuration, and then re-enable the IPSec tunnel with a different configuration.

Note When enabled, IPSec removes the IP address from the Cisco ISE interface and shuts down the interface. When the user logs in from Cisco ISE CLI, the interface is displayed with no IP address and in shutdown state. This IP address will be configured on the ESR-5921 interface.

Step 6 Type **esr** to enter into the ESR shell.

```
ise/admin# esr
% Entering ESR 5921 shell
% Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE SOFTWARE
 (fc3)
% Technical Support: http://www.cisco.com/techsupport
% Copyright (c) 1986-2015 Cisco Systems, Inc.

Press RETURN to get started, CTRL-C to exit

ise-esr5921>
ise-esr5921>
```

Note For FIPS compliance, you must configure a secret password that is at least eight characters in length. Enter the **Enable secret level 1** command to specify the password:

```
ise-esr5921(config)#enable secret level 1 ?
0 Specifies an UNENCRYPTED password will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
LINE The UNENCRYPTED (cleartext) 'enable' secret
```

Note If you configure customized RADIUS ports from the GUI (other than 1645, 1646, 1812, and 1813), you must enter the following CLI command in the ESR shell to accept the configured RADIUS ports:

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

Step 7 Verify IPSec tunnel and RADIUS authentication over IPSec tunnel.

a) Add a user in Cisco ISE and assign the user to a user group (In the Cisco ISE GUI, click the **Menu** icon (☰) and choose**Administration** > **Identity Management** > **Identities** > **Users**).

b) Carry out the following steps to verify if the IPSec tunnel is established between Cisco ISE and the NAD:

1. Use the **ping** command to test if Cisco ISE is connected to the NAD.
2. Run the following command from the ESR shell or the NAD CLI to verify if the connection is in the active state:

   show crypto isakmp sa

```
ise-esr5921#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.30.1    192.168.30.3    QM_IDLE           1001 ACTIVE
```

3. Run the following command from the ESR shell or the NAD CLI to verify if the tunnel is established:

   show crypto ipsec sa

```
ise-esr5921#show crypto ipsec sa

interface: Ethernet0/0
```

```
    Crypto map tag: radius, local addr 192.168.30.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.30.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (192.168.30.2/255.255.255.255/0/0)
   current_peer 192.168.30.2 port 500
     PERMIT, flags={}
    #pkts encaps: 52, #pkts encrypt: 52, #pkts digest: 52
    #pkts decaps: 57, #pkts decrypt: 57, #pkts verify: 57
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.30.1, remote crypto endpt.: 192.168.30.2
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0x393783B6(959939510)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x8EA0F6EE(2392913646)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 99, flow_id: SW:99, sibling_flags 80000040, crypto map: radius
        sa timing: remaining key lifetime (k/sec): (4237963/2229)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x393783B6(959939510)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 100, flow_id: SW:100, sibling_flags 80000040, crypto map: radius
        sa timing: remaining key lifetime (k/sec): (4237970/2229)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

c) Verify the RADIUS authentication using one of the following methods:

- Log in to the network device using the credentials of the user that you created in Step 8 (a). The RADIUS authentication request is sent to the Cisco ISE node. View the details in the **Live Authentications** window.
- Connect the end host with the network device and configure 802.1X authentication. Log in to the end host using the credentials of the user that you created in Step 8 (a). The RADIUS authentication request is sent to the Cisco ISE node. View the details in the **Live Authentications** window.

Configure and Install X.509 Certificates on ESR-5921

Step 1 Type **esr** to enter into the ESR shell.

```
ise/admin# esr
% Entering ESR 5921 shell
% Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE SOFTWARE
 (fc3)
% Technical Support: http://www.cisco.com/techsupport
% Copyright (c) 1986-2015 Cisco Systems, Inc.

Press RETURN to get started, CTRL-C to exit

ise-esr5921>
ise-esr5921>
```

Note For FIPS compliance, you must configure a secret password that is at least eight characters in length. Enter the **Enable secret level 1** command to specify the password:

```
ise-esr5921(config)#enable secret level 1 ?
0 Specifies an UNENCRYPTED password will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
LINE The UNENCRYPTED (cleartext) 'enable' secret
```

Note If you configure customized RADIUS ports from the GUI (other than 1645, 1646, 1812, and 1813), you must enter the following CLI command in the ESR shell to accept the RADIUS ports that are configured:

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

Step 2 Generate an RSA key pair using the following command:

Example:

```
crypto key generate rsa label rsa2048 exportable modulus 2048
```

Step 3 Create a trustpoint using the following command:

Example:

```
crypto pki trustpoint trustpoint-name

enrollment terminal
serial-number none
fqdn none
ip-address none
subject-name cn=networkdevicename.cisco.com
revocation-check none
rsakeypair rsa2048
```

Step 4 Generate a certificate signing request using the following command:

Example:

```
crypto pki enroll rsaca-mytrustpoint

Display Certificate Request to terminal? [yes/no]: yes
```

Step 5 Copy the output of the certificate signing request to a text file, submit it to an external CA for signing, and obtain the signed certificate and the CA certificate.

Step 6 Import the Certificate Authority (CA) certificate using the following command:

Example:

```
crypto pki authenticate rsaca-mytrustpoint
```

Copy and paste the contents of the CA certificate, including the "**—BEGIN—**" and "**—-End—**" lines.

Step 7 Import the signed certificate using the following command:

Example:

```
crypto pki import rsaca-mytrustpoint
```

Copy and paste the contents of the signed certificate, including the "**—BEGIN—**" and "**—-End—**" lines.

The following is an example of the output that is displayed when you configure and install X.509 Certificates on Cisco 5921 ESR:

```
ise-esr5921#show running-config
!
hostname ise-esr5921
!
boot-start-marker
boot host unix:default-config
boot-end-marker
!
no aaa new-model
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email address
to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
  active
  destination transport-method http
  no destination transport-method email
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
!
crypto pki trustpoint rsaca-mytrustpoint
enrollment terminal
serial-number none
fqdn none
ip-address none
subject-name cn=ise-5921.cisco.com
revocation-check none
rsakeypair rsa2048
!
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
        quit
crypto pki certificate chain rsaca-mytrustpoint
certificate 39
  30820386 3082026E A0030201 02020139 300D0609 2A864886 F70D0101 0B050030
  61310B30 09060355 04061302 5553310B 30090603 5504080C 024E4331 0C300A06
  03550407 0C035254 50310E30 0C060355 040A0C05 43495343 4F310C30 0A060355
  040B0C03 53544F31 19301706 03550403 0C107273 6163612E 65726368 616F2E63
  6F6D301E 170D3136 30393031 32313037 34335A17 0D313730 39303132 31303734
  335A301D 311B3019 06035504 03131269 73652D35 3932312E 63697363 6F2E636F
  6D308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201 0A028201
  0100EE87 CABFBA18 7E0405A8 ACAAAB23 E7CB6109 2CF98BAE 8EE93536 BF1EBBD3
  73E60BE7 F430B5AF EBF8B0C5 969B2828 A6783BB4 64E333E4 29C8744E 6E783617
  194AF1B0 7F04B4EA B89FD6EB F9C4F2DD 196DC6E0 CAA49B8B 665B6E0D 2FBC1D2F
  8E8181B9 60FAE126 D1B2E4E4 1F321A97 10C1B76A C2BB3174 361B13FA 2CB7BDFE
  22C0C33F 2792D714 C41E2237 00B1AE49 6593DCC3 A799D526 D81F9706 A71DA14E
  5ED76038 7A2C84B4 C668E35C 337BA1DC 9CA56AC2 C8E0059F 660CE39C 925310A0
  F9A21FFB 3C3C507A 20B924F7 E0125D60 6552321C 35736079 42449401 15E68DA6
  B4776DAA FB5AFDF8 59E31373 263175E3 1F14416A 24C21D69 A46173B6 96CC84FB
  5B9D0203 010001A3 818C3081 89300906 03551D13 04023000 302C0609 60864801
  86F84201 0D041F16 1D4F7065 6E53534C 2047656E 65726174 65642043 65727469
  66696361 7465301D 0603551D 0E041604 146DD31C 03690B98 330B67FA 6EDC7B20
  F99FB924 60301F06 03551D23 04183016 8014966A 0C21AF96 3E827690 423599CC
  EE8087A1 2909300E 0603551D 0F0101FF 04040302 05A0300D 06092A86 4886F70D
  01010B05 00038201 0100C0B9 D2845D97 6FFC16DB 01559659 BC1DECA6 E1A01965
  1F6CD459 E03D7ABE 91179FEB 08BF5B9B 84B62C36 236F528E E30C921C 81DA29E1
  EA3DFDC1 B0B0EEBA 14EADAEC 078576E4 D643A0EF 7D8E0880 C5FC3965 811B08C0
  5696DBF5 FADA4092 ACF549B8 2257F508 636D52AA 6CDC9596 AB43313F 6C33C9C1
  2CFDDBE3 EA9D407C 8D1B0F49 BBACD0CD 2832AC12 CD3FEFC8 501E1639 A4EFDC27
  69CA0147 971A1B2D DB2758E6 A84AFC86 4F9A4942 3D7EDBCC 7BDCC1BB 61F69B31
  BF13E39B 10AAC31C 55E73C8B C30BE516 7C506FF4 AC367D94 814A6880 EF201A6D
  CD2E1A95 7BBEC982 01CE867D 931F56E1 1EF1C457 9DC9A0BE 9DB2DC9B 19873585
  89AE82F6 A37E51D6 EECD
        quit
certificate ca 008DD3A81106B14664
  308203A2 3082028A A0030201 02020900 8DD3A811 06B14664 300D0609 2A864886
  F70D0101 05050030 61310B30 09060355 04061302 5553310B 30090603 5504080C
  024E4331 0C300A06 03550407 0C035254 50310E30 0C060355 040A0C05 43495343
  4F310C30 0A060355 040B0C03 53544F31 19301706 03550403 0C107273 6163612E
  65726368 616F2E63 6F6D301E 170D3135 31303231 32313135 34335A17 0D323531
  30313832 31313534 335A3061 310B3009 06035504 06130255 53310B30 09060355
  04080C02 4E43310C 300A0603 5504070C 03525450 310E300C 06035504 0A0C0543
  4953434F 310C300A 06035504 0B0C0353 544F3119 30170603 5504030C 10727361
  63612E65 72636861 6F2E636F 6D308201 22300D06 092A8648 86F70D01 01010500
  0382010F 00308201 0A028201 0100CB82 2AECEE38 1BCB27B9 FA5F2FBD 8609B190
  16A6F741 5BEC18B8 8B260CAF 190EA1CE 063BC558 556DC085 6FAC5425 14AFE225
  0E9E3A12 05F3DA7E D17E03F2 7FFE92FB 38D67027 DBC5C175 EB53E96B 66C20D11
  B4C32D38 AE04385C 8FD4CB74 31A97824 CA1CAFD5 091806C3 6F9CBF8D DC42DD5B
  D985703D F3BB9ED1 7DE99614 422D765C 86AB25CD E80008C5 22049BE8 66D1CA27
  E1EB6D4F 4FD3CC18 E091BBF0 6FE0EB52 B33F231A 6D6B7190 4196C929 D22E2C42
  B9CD2BBD 24550E82 8CD8838F C41B4DAD 2FA1636A 5787BBB2 F21E4718 335B005B
  DFBE6EA7 56EBE30B D52DE85F FFAF0189 E372CBFC 44BFF235 4DA7C9EF DAAC6D0A
  A196DA5A 1B525175 C26B3581 EA4B0203 010001A3 5D305B30 1D060355 1D0E0416
  0414966A 0C21AF96 3E827690 423599CC EE8087A1 2909301F 0603551D 23041830
  16801496 6A0C21AF 963E8276 90423599 CCEE8087 A1290930 0C060355 1D130405
  30030101 FF300B06 03551D0F 04040302 02A4300D 06092A86 4886F70D 01010505
  00038201 01002334 A3F0E5D3 4D229985 67A07754 73EC52E3 05B7D05F 926CC863
  220F849B 861C36B2 EF7C3485 474D4EF0 73895879 CAE08BBB 183B7CFA A20C4354
  86C6D9DF D445DACE C252C608 236F6673 F3F3C329 474B22E8 660BF91E 41054B8D
  43B80E44 AE69C164 2C9F41A2 8284F577 21FFAB8E A6771A5E DD34EBE4 A0DC2EAD
  95702010 02964566 478DA90F 5E134643 81A5F5EA 362D0394 1F9F23D1 DEE50B07
  12938299 1AF11A36 82DAFC6A 164B2F66 8B0AB7CC 9A723EBC B50E740B 0A9270E3
  60E2ED42 7F10D1A6 F6735144 AE93BF86 3D5A0502 6811D2BD 6E694693 28DE84C5
  3747CF0A D2B8D6C9 6CBEBA0A D1137CF8 E31CBF6B 437D82DD D74A4A9F 3557B3D9
  D0BD055F 65A8
        quit
license udi pid CISCO5921-K9 sn 9XG4481W768
username lab password 0 lab
!
redundancy
!
crypto keyring MVPN-spokes
rsa-pubkey address 0.0.0.0
  address 0.0.0.0
  key-string
  quit
!
crypto isakmp policy 10
encr aes
hash sha256
group 16
!
crypto isakmp policy 20
encr aes
hash sha256
group 14
crypto isakmp profile MVPN-profile
   description LAN-to-LAN for spoke router(s) connection
   keyring MVPN-spokes
   match identity address 0.0.0.0
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
mode tunnel
crypto ipsec transform-set radius-2 esp-aes esp-sha256-hmac
mode transport
!
crypto dynamic-map MVPN-dynmap 10
set transform-set radius radius-2
!
crypto map radius 10 ipsec-isakmp dynamic MVPN-dynmap
!
interface Ethernet0/0
description e0/0->connection to external NAD
ip address 192.168.20.1 255.255.255.0
ip nat outside
ip virtual-reassembly in
```

```
no ip route-cache
crypto map radius
!
interface Ethernet0/1
description e0/1->tap0 internal connection to ISE
ip address 10.1.1.1 255.255.255.252
ip nat inside
ip virtual-reassembly in
no ip route-cache
!
interface Ethernet0/2
no ip address
shutdown
!
interface Ethernet0/3
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip nat inside source list 1 interface Ethernet0/0 overload
ip nat inside source static udp 10.1.1.2 1645 interface Ethernet0/0 1645
ip nat inside source static udp 10.1.1.2 1646 interface Ethernet0/0 1646
ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813
!
access-list 1 permit 10.1.1.0 0.0.0.3
!
control-plane
!
line con 0
logging synchronous
line aux 0
line vty 0 4
login
transport input none
!
end
```

The following is an example of the output that is displayed when you configure and install X.509 certificates on Cisco Catalyst 3850 Series Switches:

```
cat3850#show running-config

enable password lab
!
username lab password 0 lab
aaa new-model

!

aaa group server radius ise
server name ise-vm
deadtime 60
!
aaa authentication login default group radius local

aaa authentication enable default group radius enable

!

crypto isakmp policy 10
```

```
encr aes

hash sha256
authentication rsa-sig
group 16
!
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
mode tunnel

!

crypto ipsec profile radius-profile

!

crypto map radius 10 ipsec-isakmp
set peer 192.168.20.1
set transform-set radius

match address 100

!

interface GigabitEthernet1/0/1
no switchport
ip address 192.168.20.2 255.255.255.0

crypto map radius

!
access-list 100 permit ip host 192.168.20.2 host 192.168.20.1
!
snmp-server community public RO
snmp-server community private RW
!
radius server rad-ise
address ipv4 192.168.20.1 auth-port 1645 acct-port 1646

key secret
```

Example: Output of Pre-shared Key Configuration on Cisco Catalyst 3850 Series Switches

The following is an example of the output that is displayed when you configure the pre-shared key on Cisco Catalyst 3850 Series Switches:

```
cat3850#show running-config

enable password lab
 !
 username lab password 0 lab
 aaa new-model
 !
 aaa group server radius ise
 server name ise-vm
 deadtime 60
 !
 aaa authentication login default group radius local

 aaa authentication enable default group radius enable
```

```
!

crypto isakmp policy 10

 encr aes

 hash sha256
 authentication pre-share
 group 16
 crypto isakmp key 123456789 address 0.0.0.0
 !
 crypto ipsec security-association lifetime seconds 86400
 !
 crypto ipsec transform-set radius esp-aes esp-sha256-hmac
 mode tunnel
 !
 crypto ipsec profile radius-profile
 !
 crypto map radius 10 ipsec-isakmp
 set peer 192.168.20.1
 set transform-set radius
 match address 100
!
interface GigabitEthernet1/0/1
 no switchport
 ip address 192.168.20.2 255.255.255.0

 crypto map radius
!
 access-list 100 permit ip host 192.168.20.2 host 192.168.20.1
 !
 snmp-server community public RO
 snmp-server community private RW
 !
 radius server rad-ise
 address ipv4 192.168.20.1 auth-port 1645 acct-port 1646

 key secret
```

Mobile Device Manager Interoperability with Cisco ISE

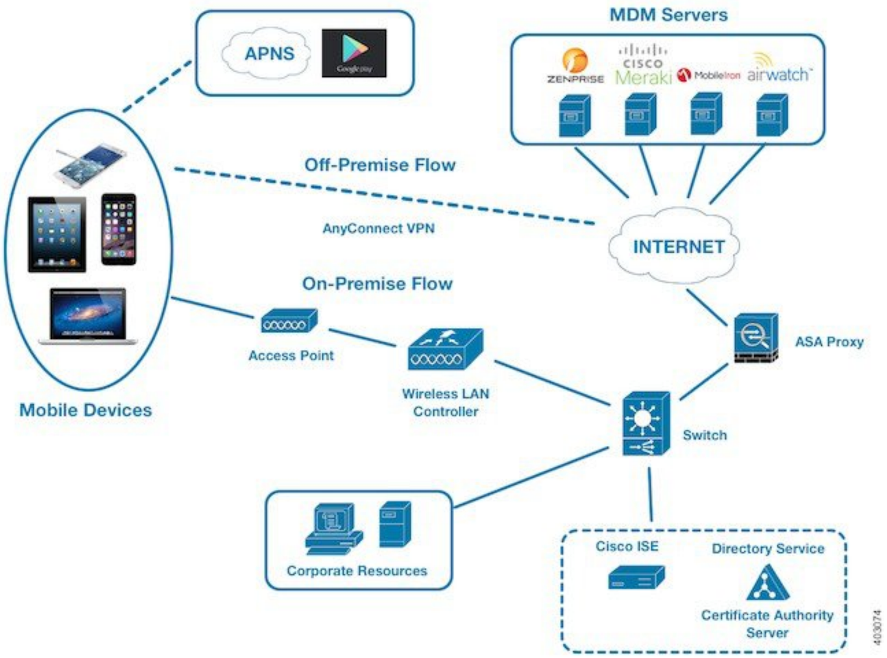
Mobile Device Management (MDM) servers secure, monitor, manage, and support mobile devices that are deployed across mobile operators, service providers, and enterprises. Traditionally, MDM servers have only supported mobile devices. Some MDM servers now manage all types of devices in a network (mobile phones, tablets, laptops, and desktops) and are called Unified Endpoint Management (UEM) servers. MDM servers act as a policy server that controls the use of some applications on a mobile device (for example, an email application) in the deployed environment. Cisco ISE queries a connected MDM server for information about various attributes that you can use to create network authorization policies.

You can run multiple active MDM servers on your network, from different vendors. This allows you to route different endpoints to different MDM servers based on device factors such as location or device type.

Cisco ISE also integrates with MDM servers using the Cisco MDM Server Info APIs, Version 2 and later versions, to allow devices to access the network over VPN via Cisco AnyConnect 4.1 and Cisco Adaptive Security Appliances 9.3.2 or later.

In the following illustration, Cisco ISE is the enforcement point and the MDM policy server is the policy information point. Cisco ISE obtains data from the MDM server to provide a complete solution.

Figure 33: MDM Interoperability with Cisco ISE


APNS
MDM Servers
ZENPRISE
CISCO Meraki
MobileIron
airwatch
Off-Premise Flow
AnyConnect VPN
INTERNET
On-Premise Flow
Access Point
Wireless LAN Controller
ASA Proxy
Mobile Devices
Switch
Corporate Resources
Cisco ISE
Directory Service
Certificate Authority Server
403074

Configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. Cisco ISE applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network.

For a list of the MDM vendors supported by Cisco ISE, see Supported Unified Endpoint Management and Mobile Device Management Servers, on page 950.

Supported Mobile Device Management Use Cases

Cisco ISE performs the following functions with external MDM servers:

- Manages device registration: Unregistered endpoints that access the network are redirected to a registration page that is hosted on the MDM server. Device registration includes the user role, device type, and so on.
- Handles device remediation: Endpoints are granted restricted access during remediation.
- Augments endpoint data: The endpoint database is updated with information from the MDM server that you cannot gather using the Cisco ISE profiling services. Cisco ISE uses multiple device attributes that you can view in the **Endpoints** page. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Identities** > **Endpoints**.

  The following are examples of the device attributes available.

- MDMImei: xx xxxxxx xxxxxx x
- MDMManufacturer: Apple

- MDMModel: iPhone
- MDMOSVersion: iOS 6.0.0
- MDMPhoneNumber: 5550100
- MDMSerialNumber: DNPGQZGUDTFx

- Polls the MDM server every four hours for device compliance data. Configure the polling interval in the **External MDM Servers** page. (To view this page, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Network Resources** > **External MDM Servers**.
- Issues device instructions through the MDM server: Cisco ISE issues remote actions for user devices through the MDM server. Initiate remote actions from the Cisco ISE administration portal through the **Endpoints** page. To view this page, click the **Menu** icon (☰) and choose **Context Visibility** > **Endpoints**. Check the check box next to the MDM server and click **MDM Actions**. Choose the required action from the drop-down list displayed.

Vendor MDM Attributes

When you configure an MDM server in Cisco ISE, Cisco ISE queries the MDM server for device attribute information and adds the information to the MDM system dictionary. The following attributes are used for registration status, and are commonly supported by MDM vendors.

Cisco ISE uses APIs to query MDM servers for the required device attributes. Cisco ISE Release 3.1 and later releases support MDM APIs Version 3. The Version 3 APIs include APIs that allow Cisco ISE to send queries to MDM servers for device attributes that help Cisco ISE identify endpoints that use MAC address randomization. Cisco ISE queries the MDM server for the following attributes:

- GUID: A unique device identifier that replaces the use of MAC address to identify a device.
- MAC addresses: The list of MAC addresses that a UEM or MDM server has recorded for a particular device. A maximum of five MAC addresses are shared for a device.

If an MDM server does not provide values for the required attributes, Cisco ISE fills the attributes fields with the default values that are mentioned in the following table.

Table 140: MDM Attributes and Values

Attribute Name	Attribute Dictionary	Default Value	Data That is Expected From UEM or MDM Servers	Data That is Expected From Microsoft SCCM Servers
DaysSinceLastCheckin Supported from MDM API Version 3	MDM	None	The number of days since a user has last checked in or synchronized a device with the UEM or MDM server. The valid range is 1–365 days.	The number of days since a user has last checked in or synchronized a device with the SCCM server. The valid range is 1–365 days.
DeviceCompliantStatus	MDM	NonCompliant	**Compliant** or **NonCompliant**.	**Compliant** or **NonCompliant**.

Attribute Name	Attribute Dictionary	Default Value	Data That is Expected From UEM or MDM Servers	Data That is Expected From Microsoft SCCM Servers
DeviceRegisterStatus	MDM	UnRegistered	**Registered** or **UnRegistered**.	**Registered** or **UnRegistered**.
DiskEncryptionStatus	MDM	Off	**On** or **Off**.	**On** or **Off**.
IMEI	MDM	None	The IMEI number of the device.	Not applicable.
JailBrokenStatus	MDM	Unbroken	**Reachable** or **UnReachable**.	**Reachable** or **UnReachable**.
MDMFailureReason	MDM	None	The device failure reason.	The device failure reason.
MDMServerName	MDM	None	The name of the server.	The name of the server.
MDMServerReachable	MDM	Reachable	**Reachable** or **UnReachable**.	**Reachable** or **UnReachable**.
MEID	MDM	None	The MEID value of the device.	Not applicable.
Manufacturer	MDM	None	The name of the device manufacturer.	Not applicable.
Model	MDM	None	The name of the device model.	Not applicable.
OsVersion	MDM	None	The operating system version of the device.	Not applicable.
PhoneNumber	MDM	None	The phone number of the device.	Not applicable.
PinLockStatus	MDM	Off	**On** or **Off**.	Not applicable.
SerialNumber	MDM	None	The serial number of the device.	Not applicable.
ServerType	MDM	None	**MDM** for a Mobile Device Manager server. **DM** for Desktop Device Manager server.	**DM** for Desktop Device Manager server.
UDID	MDM	None	The UDID number of the device.	Not applicable.
UserNotified	MDM	No	**Yes** or **No**	Not applicable.

Attribute Name	Attribute Dictionary	Default Value	Data That is Expected From UEM or MDM Servers	Data That is Expected From Microsoft SCCM Servers
GUID Supported from MDM API Version 3	Not a Dictionary attribute	None	The GUID is a unique device identifier that is used to identify a device instead of the device's MAC address, UDID, MEID, or IMEI values. The GUID template is **ID:MDMServer:GUID:{{DeviceId}}** The GUID value is generated and provided by the MDM server, not by Cisco ISE.	Not applicable.
Macaddresses Supported from MDM API Version 3	Not a Dictionary attribute	None	The list of MAC addresses that the UEM or MDM server has recorded for a particular device. A maximum of five MAC addresses can be shared for a device. The Macaddresses values are generated and provided by the MDM server, not by Cisco ISE.	Not applicable.

If a vendor's unique attributes are not supported, you may be able to use ERS APIs to exchange vendor-specific attributes. Check the vendor's documentation for information on the ERS APIs that are supported.

The new MDM dictionary attributes are available for use in authorization policies.

Manage Allowed Values in MDM System Dictionary

In an MDM system dictionary, you can enable an attribute value to be used multiple times in authorization profiles. You can view these values in the **Allowed Values** area of the **Policy** > **Policy Elements** > **Dictionaries** > **MDM** page.

When you remove an MDM server integration from the **Administration** > **Network Resources** > **External MDM** page, the values received from the deleted MDM server are not automatically removed from the **Allowed Values** list in the MDM system dictionary.

To remove an entry from the **Allowed Values** list, all the MDM servers integrated with Cisco ISE must be removed from the External MDM page.

Supported Unified Endpoint Management and Mobile Device Management Servers

Supported MDM servers include products from the following vendors:

- Absolute
- Blackberry - BES
- Blackberry - Good Secure EMM
- Cisco Meraki Systems Manager
- Citrix XenMobile 10.x (On-prem)
- Globo
- IBM MaaS360
- Ivanti (previously MobileIron UEM), core and cloud UEM services

  For the use case of handling random and changing MAC Addresses in Cisco ISE 3.1, you must integrate MobileIron Core 11.3.0.0 Build 24 and later releases to receive GUID values.

Note Some versions of MobileIron do not work with Cisco ISE. MobileIron is aware of this problem, and have a fix. Contact MobileIron for more information.

- JAMF Casper Suite
- Microsoft Endpoint Configuration Manager
- Microsoft Endpoint Manager Intune
- Mosyle
- SAP Afaria
- Sophos
- SOTI MobiControl
- Symantec
- Tangoe
- VMware Workspace ONE (earlier known as AirWatch)
- 42Gears

For the configurations that you must perform in your endpoint management servers to integrate the servers with Cisco ISE, see Integrate UEM and MDM Servers With Cisco ISE.

ISE Community Resource

How To: Meraki EMM / MDM Integration with ISE

Ports Used by the Mobile Device Management Server

The following table lists the ports that must be open between Cisco ISE and an MDM server to enable them to communicate with each other. See the documentation from the MDM vendor for a list of ports that must be open on the MDM agent and server.

Table 141: Ports Used by the MDM Server

MDM Server	Ports
MobileIron	443
Citrix XenMobile 10.x (On-prem)	443
Blackberry - Good Secure EMM	19005
VMware Workspace ONE (earlier known as AirWatch)	443
SAP Afaria	443
IBM MaaS360	443
Cisco Meraki	443
Microsoft Intune	80 and 443
Microsoft SCCM	80 and 443

Mobile Device Management Integration Process Flow

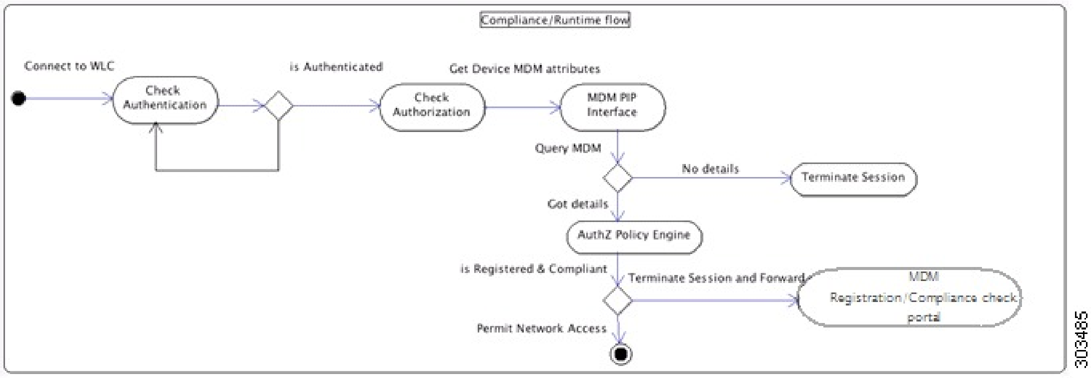
1. The user associates a device with an SSID.
2. Cisco ISE makes an API call to the MDM server.
3. This API call returns a list of devices for the user and the posture statuses for the devices.

Note The input parameter is the MAC address of the endpoint device. For off-premise Apple iOS devices (any device that connects to Cisco ISE through a VPN), the input parameter is the UDID.

4. If the user’s device is not on this list, it means that the device is not registered. Cisco ISE sends an authorization request to the NAD to redirect to Cisco ISE. The user is presented with the MDM server page.
5. Cisco ISE uses MDM to provision the device and presents the appropriate window for the user to register the device.
6. The user registers the device in the MDM server, and the MDM server redirects the request to Cisco ISE through automatic redirection or manual browser refresh.

7. Cisco ISE queries the MDM server again for the posture status.
8. If the user’s device is not compliant with the posture (compliance) policies that are configured on the MDM server, the user is notified that the device is out of compliance. The user must take the necessary action to ensure that the device is compliant.
9. When the user’s device is compliant, the MDM server updates the device's state in its internal tables.
10. If the user refreshes the browser now, the control is transferred back to Cisco ISE.
11. Cisco ISE polls the MDM server every four hours to get compliance information and issues the appropriate Change of Authorization (CoA). You can configure the polling interval. Cisco ISE also checks the MDM server every five minutes to make sure that it is available.

Figure 34: The MDM Process Flow in Cisco ISE


Compliance/Runtime flow
Connect to WLC
Check Authentication
is Authenticated
Check Authorization
Get Device MDM attributes
MDM PIP Interface
Query MDM
No details
Terminate Session
Got details
AuthZ Policy Engine
is Registered & Compliant
Terminate Session and Forward
MDM Registration/Compliance check portal
Permit Network Access
303485

Note A device can only be enrolled in a single MDM server at a time. If you want to enroll the same device to an MDM service from another vendor, the previous vendor's profiles must be removed from the device. The MDM service usually offers a "corporate wipe", which only deletes the vendor's configuration from the device (not the whole device). The user can also remove the files. For example, on an iOS device, the user can go to the **Settings** > **General** > **Device management** window, and click **Remove Management**. Or the user can go to the MyDevices portal in Cisco ISE and click **Corporate Wipe**.

Handle Random and Changing MAC Addresses with Mobile Device Management Servers

Configure Cisco ISE to identify endpoints that are connected to an MDM server by a unique device identifier instead of a MAC address, to avoid issues that are caused by the use of random and changing MAC addresses. As a privacy measure, mobile devices increasingly use random and changing MAC addresses for each SSID that they connect to. Some desktop operating systems offer users the ability to randomize MAC addresses at regular intervals as well. This means that an endpoint presents different MAC addresses to the MDM server and Cisco ISE. As a result, when the MDM server and Cisco ISE are integrated and an action is initiated for an endpoint, issues arise because of the difference in the endpoint identity in the two systems.

To work around this issue, you can configure Cisco ISE to use a unique device identifier instead of MAC addresses. When an endpoint enrolls with an MDM server, the MDM server sends a certificate with a GUID value to the endpoint. The endpoint uses this certificate for authentication with Cisco ISE. Cisco ISE receives the GUID for the endpoint from the certificate. All communications between Cisco ISE and the MDM server now use the GUID to identify the endpoint, ensuring accuracy and consistency between the two systems.

Note that GUID is available only in certificate-based authentication methods. You must configure the certificates issued by the MDM or UEM server to include the GUID in the SAN URI or CN fields. We recommend configuring the SAN URI field for GUID. If the same certificate is used to authenticate an endpoint connected to Active Directory, the presence of GUID in the CN field might cause issues.

Basic authentication methods that only use username and password will not be able to leverage the GUID-based solution.

The Cisco ISE MDM APIs have been updated (Cisco ISE MDM APIs Version 3) to facilitate the gathering and management of GUID data.

Configure GUID for Connected MDM Servers

To check if an MDM server you have already connected to Cisco ISE supports the latest Cisco ISE MDM APIs and can send GUID information, carry out the following steps:

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **External MDM**.
2. In the **MDM Servers** window, check the check box for the MDM server you want to update, and click **Edit**.
3. Click **Test Connection**.
4. If the MDM server supports Cisco ISE MDM APIs Version 3, a new section called **Device Identifiers** is displayed.

   Check the check boxes for one or more of the following options that you want to enable:

   - **Cert - SAN URI, GUID**
   - **Cert - CN, GUID**
   - **Legacy MAC Address**

   You can drag and drop the options to organize them in the order of preference. For example, if you place **Cert - SAN URI, GUID** first and then **Cert - CN, GUID**, Cisco ISE first queries the MDM server for the SAN URI and GUID attributes of an endpoint. If the requested attributes are not available, Cisco ISE queries for the common name and GUID attributes of the endpoint.
5. Click **Save**.

Sharing GUID Through pxGrid

Cisco ISE can share this GUID information through the pxGrid with other Cisco solutions. For example, you can share the GUID received from MDM servers with a Catalyst Center in your deployment through pxGrid topics.

Set Up Mobile Device Management Servers with Cisco ISE

To set up MDM servers with Cisco ISE, you must perform the following high-level tasks:

Step 1 Import the MDM server certificate into Cisco ISE, except for Intune, where you import the Policy Administration node's (PAN) certificate into Azure.

Step 2 Create mobile device manager definitions.

Step 3 Configure ACLs on the Cisco WLCs.

Step 4 Configure an authorization profile that redirects nonregistered devices to the MDM server.

Step 5 If there are multiple MDM servers on the network, configure separate authorization profiles for each vendor.

Step 6 Configure authorization policy rules for the MDM use cases.

Import Mobile Device Management Server Certificate into Cisco ISE

For Cisco ISE to connect with the MDM server, you must import the MDM server certificate into the Cisco ISE Trusted Certificates store. If your MDM server has a CA-signed certificate, you must import the root certificate into the Cisco ISE Trusted Certificates store.

Note For Microsoft Azure, import the Cisco ISE certificate into Azure. See Connect Microsoft Intune to Cisco ISE as a Mobile Device Management Server.

Step 1 Export the MDM server certificate from your MDM server and save it on your local machine.

Step 2 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Trusted Certificate** > **Import**.

Step 3 In the **Import a new Certificate into the Certificate Store** window, click **Choose File** to select the MDM server certificate that you obtained from the MDM server.

Step 4 Add a name for the certificate in the **Friendly Name** field.

Step 5 Check the **Trust for authentication within ISE** check box.

Step 6 Click **Submit**.

Step 7 Verify that the **Trust Certificates** window lists the newly added MDM server certificate.

Define Device Management Servers in Cisco ISE

Define mobile and desktop device management servers in Cisco ISE to allow Cisco ISE to communicate with the required servers. You can configure the authentication type that is used to communicate with the servers, the frequency at which Cisco ISE requests device information from a device management server, and so on.

To define a mobile management server, see Configure Mobile Device Management Servers in Cisco ISE, on page 955.

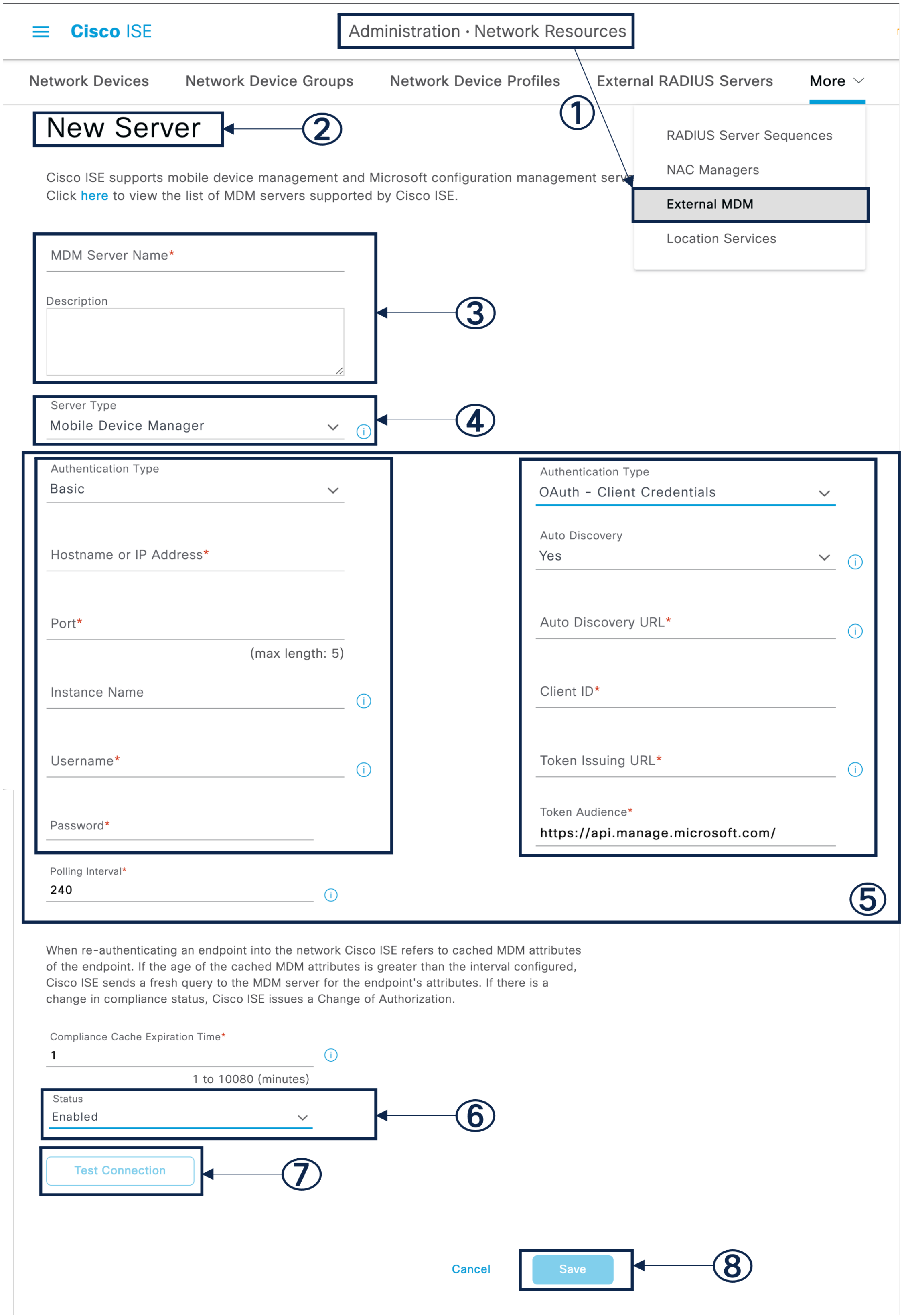
To define a Microsoft System Center Configuration Manager (SCCM) server, see Select Configuration Baseline Policies for Endpoint Compliance from Desktop Device Manager Server.

Configure Mobile Device Management Servers in Cisco ISE

The first MDM server that provides an endpoint's information to Cisco ISE is displayed in the endpoint information in the **Context Visibility** > **Endpoints** window. The MDM server information is not automatically updated when an endpoint connects with a different MDM server. You must delete the endpoint from the **Context Visibility** window, and then the endpoint must reconnect with an MDM server, for the **Context Visibility** window to display the updated information.

The following image displays the Cisco ISE GUI fields that you must work with during this task. The numbers in the image correspond to the step numbers in the following task.

Figure 35: Add an MDM Server in Cisco ISE


Cisco ISE
Administration · Network Resources
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
More
RADIUS Server Sequences
NAC Managers
External MDM
Location Services
①
New Server
②
MDM Server Name*
Description
③
④
Hostname or IP Address*
Port*
(max length: 5)
Instance Name
Username*
Password*
Auto Discovery URL*
Client ID*
Token Issuing URL*
⑤
1 to 10080 (minutes)
⑥
Test Connection
⑦
Cancel
Save
⑧

Cisco ISE supports mobile device management and Microsoft configuration management serv

Click here to view the list of MDM servers supported by Cisco ISE.

Server Type: Mobile Device Manager

Authentication Type: Basic

Authentication Type: OAuth - Client Credentials

Auto Discovery: Yes

Token Audience*: https://api.manage.microsoft.com/

Polling Interval*: 240

When re-authenticating an endpoint into the network Cisco ISE refers to cached MDM attributes of the endpoint. If the age of the cached MDM attributes is greater than the interval configured, Cisco ISE sends a fresh query to the MDM server for the endpoint's attributes. If there is a change in compliance status, Cisco ISE issues a Change of Authorization.

Compliance Cache Expiration Time*: 1

Status: Enabled

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **External MDM**.

Step 2 In the **MDM Servers** window, click **Add**.

Step 3 Enter the name and description of the MDM server that you want to add in the corresponding fields.

Step 4 From the **Server Type** drop-down list, choose **Mobile Device Manager**.

Step 5 From the **Authentication Type** drop-down list, choose either **Basic** or **OAuth - Client Credentials**.

If you choose the **Basic** authentication type, the following fields are displayed:

- **Host Name / IP Address**: Enter the hostname or IP address of the MDM server.
- **Port**: Specify the port to be used when connecting to the MDM server, which is usually 443.
- **Instance Name**: If this MDM server has several instances, enter the instance that you want to connect to.
- **Username**: Enter the username that must be used to connect to the MDM server.
- **Password**: Enter the password that must be used to connect to the MDM server.

If you choose the **OAuth - Client Credentials** authentication type, the following fields are displayed:

- From the **Auto Discovery** drop-down list, choose **Yes** or **No**.
- **Auto Discovery URL**: Enter the value of Microsoft Azure AD Graph API Endpoint from the Microsoft Azure management portal. This URL is the endpoint at which an application can access directory data in your Microsoft Entra ID using the Graph API. For more information, see Integrate MDM and UEM Servers with Cisco ISE.
- **Client ID**: The unique identifier for your application. Use this attribute if your application accesses data in another application, such as the Microsoft Azure AD Graph API, Microsoft Intune API, and so on.
- **Token Issuing URL**: Enter the value of the Oauth2.0 Authorization Endpoint. This is the endpoint from which Cisco ISE obtains an access token using OAuth2.0.
- **Token Audience**: The recipient resource that the token is intended for, which is a public, well-known **APP ID URL** to the Microsoft Intune API.

Time Interval For Compliance Device ReAuth Query: When an endpoint is authenticated or reauthenticated, Cisco ISE uses a cache to get the MDM variables for that endpoint. If the age of the cached value is greater than the value configured in this field, Cisco ISE sends a new device query to the MDM server to get new values. If the compliance status has changed, then Cisco ISE triggers the appropriate CoA. The valid range is from 1 to 10080 minutes. The default value is one minute.

Polling Interval: Enter the polling interval, in minutes, for Cisco ISE to poll the MDM server for noncompliant endpoints. Set this value to match the polling interval on your MDM server. The valid range is from 15 to 1440 minutes. The default value is 240 minutes. We recommend that you set the polling interval more than 60 minutes in production environments to minimize any performance impact that might occur due to large numbers of noncompliant endpoints.

ISE retrieves list of non compliant devices information through MAC Address/GUID based non compliant API calls (Eg:)

Since this is a bulk retrieval API, ISE uses paging info provided by MDM Server.

ISE updates endpoint records compliance information based on the non compliance API response. If ISE finds active sessions on these non compliance devices, then it will reauthorize.

ISE limits the non compliance API calls to maximum of 200 requests or 20,000 endpoint records, whichever happens first.

If you set the polling interval to 0, Cisco ISE disables polling with the MDM server.

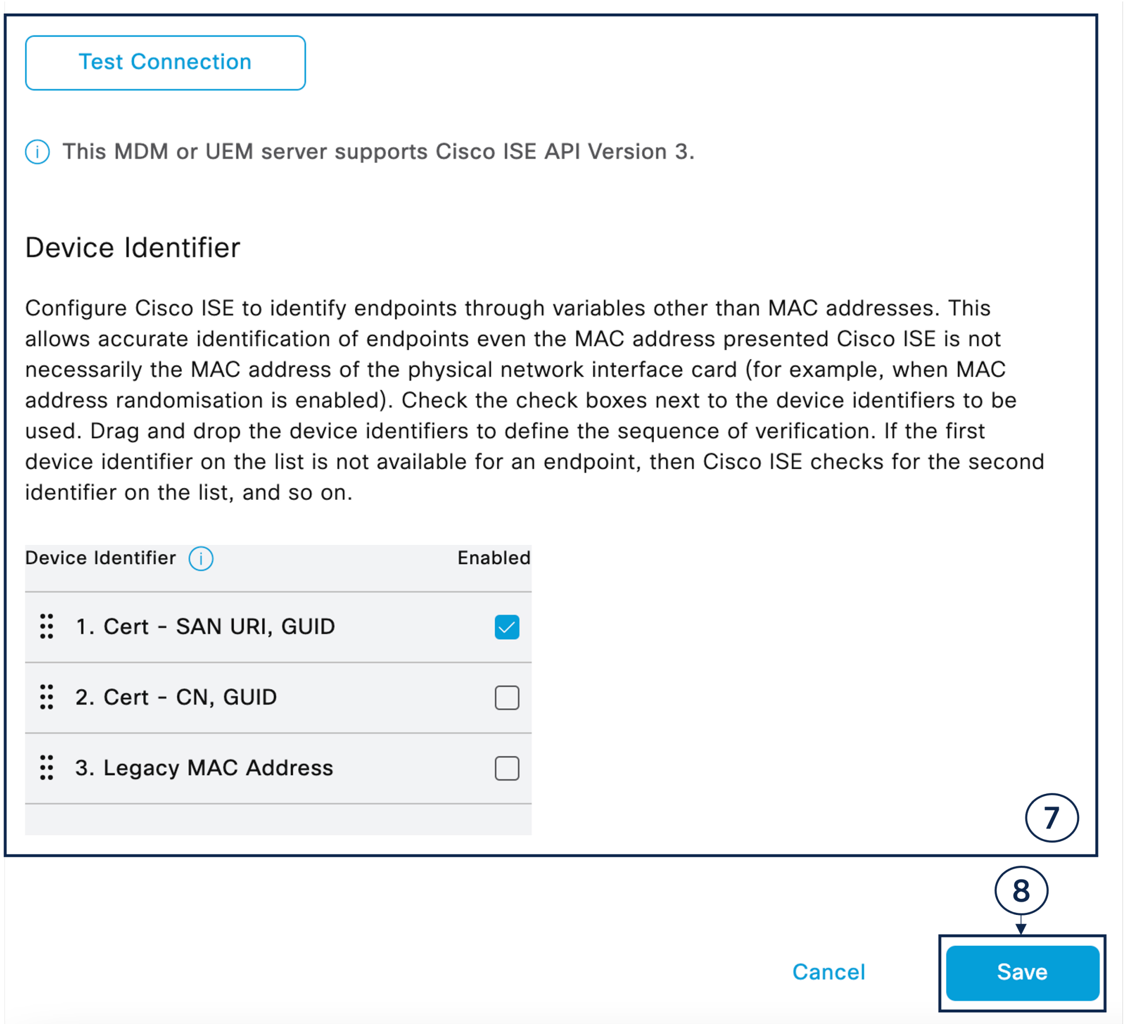
Note Cisco ISE limits API calls from noncompliant endpoints to 200. If the external MDM server receives requests from more than 20000 noncompliant endpoints, the external MDM server polling interval is automatically set to 0. You also receive the following alarm on Cisco ISE:

```
MDM Compliance Polling Disabled: Reason is Periodic Compliance Polling received huge
non-compliance device information.
```

Step 6 From the **Status** drop-down list, choose **Enabled**.

Step 7 To verify whether the MDM server is connected to Cisco ISE, click **Test Connection**. Note that **Test Connection** is not intended to check permissions for all the use cases (get baselines, get device information, and so on). These are validated when the server is added to Cisco ISE.

Figure 36: Add an MDM Server in Cisco ISE



This MDM or UEM server supports Cisco ISE API Version 3.

Device Identifier

Configure Cisco ISE to identify endpoints through variables other than MAC addresses. This allows accurate identification of endpoints even the MAC address presented Cisco ISE is not necessarily the MAC address of the physical network interface card (for example, when MAC address randomisation is enabled). Check the check boxes next to the device identifiers to be used. Drag and drop the device identifiers to define the sequence of verification. If the first device identifier on the list is not available for an endpoint, then Cisco ISE checks for the second identifier on the list, and so on.

Device Identifier	Enabled
1. Cert - SAN URI, GUID	☑
2. Cert - CN, GUID	☐
3. Legacy MAC Address	☐

If the MDM server you are configuring supports Cisco ISE MDM API Version 3 and can share the attribute GUID with Cisco ISE, the **Device Identifiers** area is displayed. For more information, see Handle Random and Changing MAC Addresses with Mobile Device Management Servers, on page 952.

Check the check boxes for one or more of the following options that you want to enable, and arrange them in the order of preference by dragging and dropping each option in its place:

- **Cert - SAN URI, GUID**
- **Cert - CN, GUID**
- **Legacy MAC Address**

Step 8 Click **Save**.

Cisco ISE MDM Support for Microsoft Intune and Microsoft SCCM

- **Microsoft Intune**: Cisco ISE supports Microsoft Intune device management as a partner MDM server to manage mobile devices.

  Configure Cisco ISE as an OAuth 2.0 client application with the Microsoft Intune server managing mobile devices. Cisco ISE gets a token from Azure to establish a session with the Cisco ISE Intune application.

  For information about how Microsoft Intune communicates with a client application, see https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx.

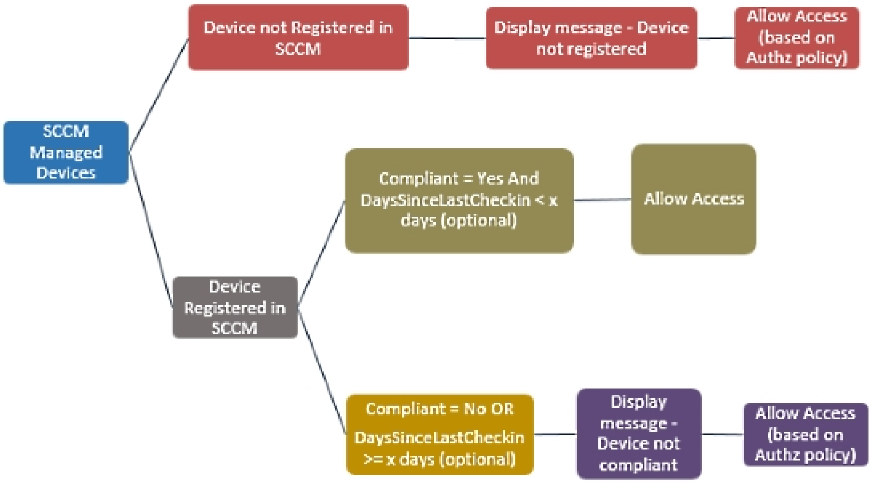
- **Desktop Device Manager (Microsoft SCCM)**: Cisco ISE supports the Microsoft System Center Configuration Manager (SCCM) as a partner MDM server for managing Windows computers.

  For performance and scalability information for Microsoft SCCM integrations, see Size and Scale Numbers for Configuration Manager. Microsoft uses Windows Management Instrumentation (WMI) interfaces based on the Component Object Model (COM), which results in scalability limitations.

Microsoft SCCM Workflow

Cisco ISE retrieves information from the Microsoft SCCM server about whether a device is registered. If the endpoint is registered, Cisco ISE checks for its compliance status. The following diagram shows the workflow for devices that Microsoft SCCM manages.

Figure 37: SCCM Workflow


SCCM Managed Devices
Device not Registered in SCCM
Display message - Device not registered
Allow Access (based on Authz policy)
Device Registered in SCCM
Compliant = Yes And DaysSinceLastCheckin < x days (optional)
Allow Access
Compliant = No OR DaysSinceLastCheckin >= x days (optional)
Display message - Device not compliant
Allow Access (based on Authz policy)

When a device connects to the network and a Microsoft SCCM policy matches, Cisco ISE queries the relevant SCCM server to retrieve compliance and last login (check-in) time. With this information, Cisco ISE updates the compliance status and the lastCheckinTimeStamp of the device in the **Endpoint** list.

If the device is not compliant or not registered with the Microsoft SCCM server, and the authorization policy uses a redirect profile, a message is displayed to the user that the device is not compliant, or is not registered with the Microsoft SCCM. After the user acknowledges the message, Cisco ISE can issue a CoA to the Microsoft SCCM registration site. Users are granted access based on the authorization policy and profile.

Microsoft SCCM Server Connection Monitoring

You cannot configure polling intervals for Microsoft SCCM.

Cisco ISE runs an MDM HeartBeat job that verifies connection with the Microsoft SCCM server, and raises alarms if Cisco ISE loses the connection to the Microsoft SCCM server. The HeartBeat job interval cannot be configured.

Policy Set Example for Microsoft System Center Configuration Manager

The following new dictionary entries are used in policies to support Microsoft SCCM.

- **MDM.DaysSinceLastCheckin**: The number of days since a user last checked in or synchronized a device with Microsoft SCCM. The value may range from 1 to 365 days.
- **MDM.UserNotified**: The valid values are **Y** or **N**. The value indicates whether the user was notified that their device is not registered. You can then allow the user limited access to the network and then redirect them to the registration portal, or deny them access to the network.
- **MDM.ServerType**: The valid value is **MDM** for MDM servers and **DM** for desktop device management.

The following is an example of a policy set that supports Microsoft SCCM.

Policy Name	If	Then
SCCM_Comp	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceRegisterStatus EQUALS Registered	PermitAccess
SCCM_NonComp_Notify	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:UserNotified EQUALS 28	PermitAccess
SCCM_NonComp_Days	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:MDMDeviceCompliantStatus EQUALS Registered AND MDM:DaysSinceLastCheckin EQUALS 28	SCCMRedirect
SCCM_NonComp	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:DeviceRegisterStatus EQUALS Registered	SCCMRedirect
SCCM_UnReg_Notify	Wireless_802.1X AND MDM:DeviceRegisterStatus EQUALS Registered AND MDM:UserNotified EQUALS Yes	PermitAccess

Configure the Microsoft System Center Configuration Manager Server for Cisco ISE

Cisco ISE communicates with the Microsoft SCCM server using Windows Management Instrumentation (WMI). Configure WMI on the Windows server running Microsoft SCCM.

Note The user account that you use for Cisco ISE integration must either:

- Be a member of the SMS Admins user group.
- Have the same permissions as the SMS object under the WMI namespace:

  `root\sms\site_<sitecode>`

  where *sitecode* is the Microsoft SCCM site.

Set Permissions when Microsoft Active Directory Users are in Domain Admin Group

For Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2, the Domain Admin group does not have full control of certain registry keys in the Windows operating system by default. The Microsoft Active Directory administrator must give the Microsoft Active Directory user full control permissions on the following registry keys:

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

The following Microsoft Active Directory versions require no registry changes:

- Windows 2003
- Windows 2003R2
- Windows 2008

To grant full control, the Microsoft Active Directory admin must first take ownership of the key:

Step 1 Right-click the key icon and choose the **Owner** tab.

Step 2 Click **Permissions**.

Step 3 Click **Advanced**.

Permissions for Microsoft Active Directory Users Not in Domain Admin Group

For Windows Server 2012 R2, give the Microsoft AD user full control permissions on the following registry keys:

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

Use the following commands in Windows PowerShell to check if full permission is given to the registry keys:

-
  ```
  get-acl -path
  "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}"
  | format-list
  ```

- `get-acl -path "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" | format-list`

The following permissions are required when a Microsoft AD user is not in the Domain Admin group, but is in the Domain Users group:

- Add registry keys to allow Cisco ISE to connect to the domain controller.
- Permissions to Use DCOM on the Domain Controller, on page 678
- Set Permissions for Access to WMI Root and CIMv2 Namespace, on page 966

These permissions are only required for the following Microsoft AD versions:

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

Add Registry Keys to Allow Cisco ISE to Connect to the Domain Controller

You must manually add some registry keys to the domain controller to allow Cisco ISE to connect as a domain user, and retrieve login authentication events. An agent is not required on the domain controllers or on any machines in the domain.

The following registry script shows the keys to add. You can copy and paste this into a text file, save the file with a .reg extension, and double click the file to make the registry changes. To add registry keys, the user must be an owner of the root key.

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "
```

Make sure that you include two spaces in the value of the DllSurrogate key. If the registry is manually updated, you must include only the two spaces and do not include the quotes. While updating the registry manually, ensure that quotes are not included for AppID, DllSurrogate, and its values.

Retain the empty lines as shown in the preceding script, including the empty line at the end of the file.

Use the following commands in the Windows command prompt to confirm if the registry keys are created and have the correct values:

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`
- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`
- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`

Permissions to Use DCOM on the Domain Controller

The Microsoft Active Directory user who is used for Cisco ISE Passive Identity service must have the permissions to use DCOM on the domain controller server. Configure permissions with the **dcomcnfg** command line tool.

Step 1 Run the **dcomcnfg** tool from the command line.

Step 2 Expand `Component Services`.

Step 3 Expand **Computers** > **My Computer**.

Step 4 Choose **Action** from the menu bar, click **Properties**, and click **COM Security**.

Step 5 The account that Cisco ISE uses for both access and launch must have Allow permissions. Add the Microsoft Active Directory user to all the four options, **Edit Limits** and **Edit Default** for both **Access Permissions** and **Launch and Activation Permissions**.

Step 6 Allow all local and remote accesses for both **Access Permissions** and **Launch and Activation Permissions**.

Figure 38: Local and Remote Accesses for Access Permissions

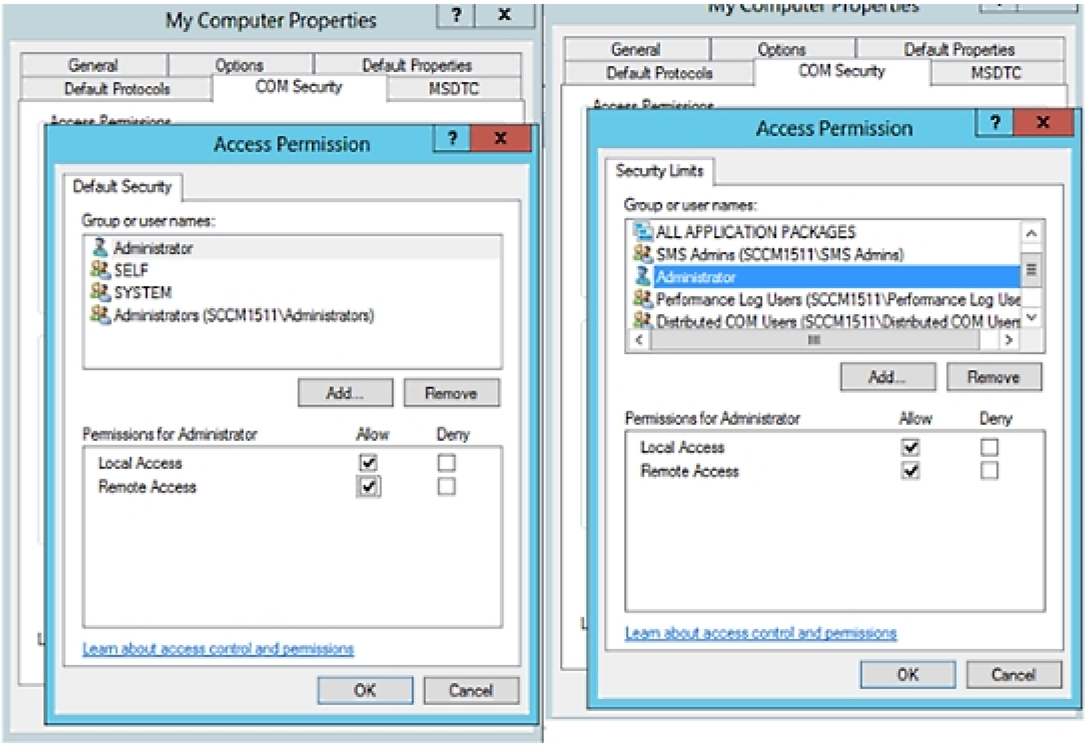
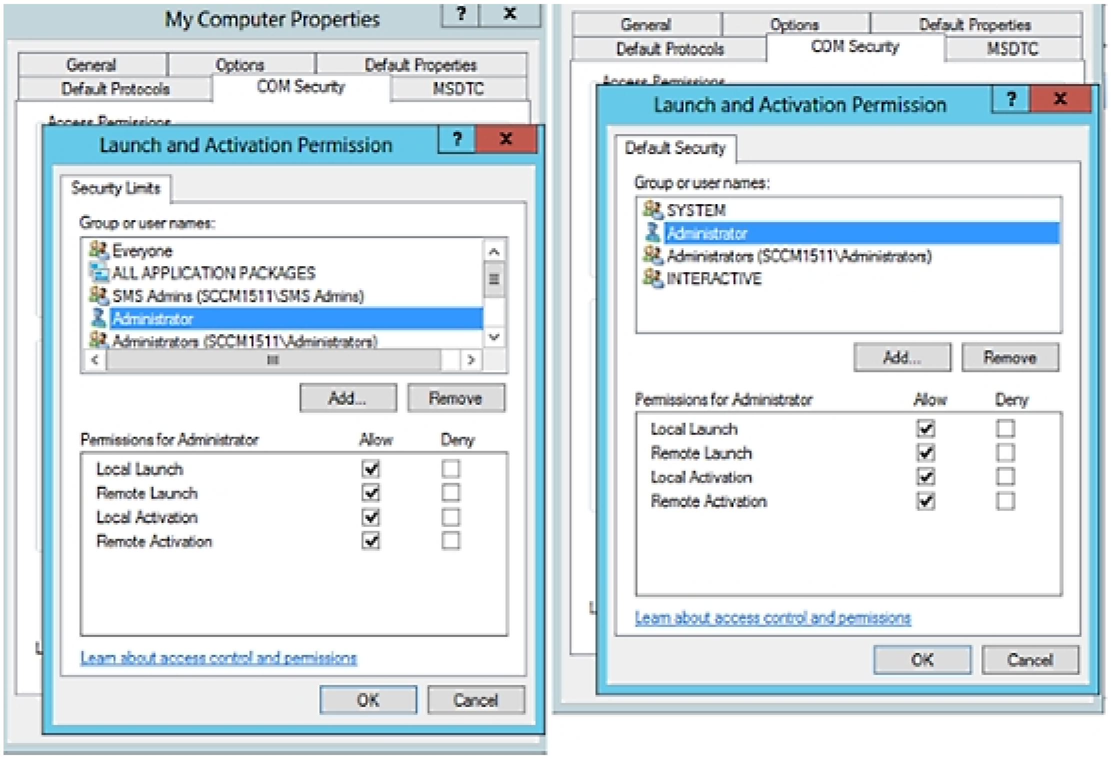

My Computer Properties
General
Options
Default Properties
Default Protocols
COM Security
MSDTC
Access Permission
Default Security
Group or user names:
Administrator
SELF
SYSTEM
Administrators (SCCM1511\Administrators)
Add...
Remove
Permissions for Administrator
Allow
Deny
Local Access ☑ ☐
Remote Access ☑ ☐
Learn about access control and permissions
OK
Cancel
My Computer Properties
Access Permission
Security Limits
Group or user names:
ALL APPLICATION PACKAGES
SMS Admins (SCCM1511\SMS Admins)
Administrator
Performance Log Users (SCCM1511\Performance Log Use
Distributed COM Users (SCCM1511\Distributed COM Users
Add...
Remove
Permissions for Administrator
Allow
Deny
Local Access ☑ ☐
Remote Access ☑ ☐
Learn about access control and permissions
OK
Cancel

Figure 39: Local and Remote Accesses for Launch and Activation Permissions



My Computer Properties
General
Options
Default Properties
Default Protocols
COM Security
MSDTC
Access Permissions
Launch and Activation Permission
Security Limits
Group or user names:
Everyone
ALL APPLICATION PACKAGES
SMS Admins (SCCM1511\SMS Admins)
Administrator
Administrators (SCCM1511\Administrators)
Add...
Remove
Learn about access control and permissions
OK
Cancel
Default Security
Group or user names:
SYSTEM
Administrator
Administrators (SCCM1511\Administrators)
INTERACTIVE
Add...
Remove
Learn about access control and permissions
OK
Cancel

Permissions for Administrator	Allow	Deny
Local Launch	☑	☐
Remote Launch	☑	☐
Local Activation	☑	☐
Remote Activation	☑	☐

Set Permissions for Access to WMI Root and CIMv2 Namespace

By default, Microsoft Active Directory users do not have permissions for the Execute Methods and Remote Enable. You can grant access using the wmimgmt.msc MMC console.

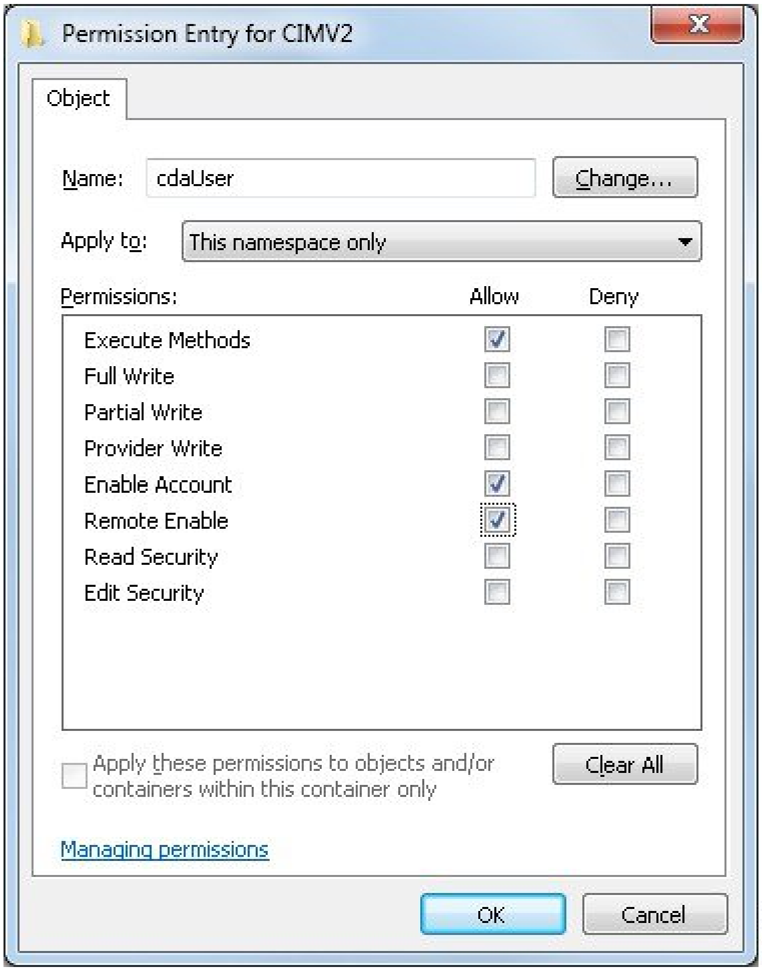
Step 1 Choose **Start** > **Run** and enter `wmimgmt.msc`.

Step 2 Right-click **WMI Control** and click **Properties**.

Step 3 Under the **Security** tab, expand **Root** and choose **CIMV2**.

Step 4 Click **Security**.

Step 5 Add the Microsoft Active Directory user, and configure the required permissions as shown in the following image.



Name: cdaUser

Apply to: This namespace only

Permissions:	Allow	Deny
Execute Methods	☑	☐
Full Write	☐	☐
Partial Write	☐	☐
Provider Write	☐	☐
Enable Account	☑	☐
Remote Enable	☑	☐
Read Security	☐	☐
Edit Security	☐	☐

☐ Apply these permissions to objects and/or containers within this container only

Open Firewall Ports for WMI Access

The firewall software on the Microsoft Active Directory domain controller may block access to WMI. You can either turn off the firewall, or allow access on a specific IP address (Cisco ISE IP address) to the following ports:

- TCP 135: General RPC Port. When performing asynchronous RPC calls, the service listening on this port tells the client which port the component servicing this request is using.
- UDP 138: NetBIOS Datagram Service
- TCP 139: NetBIOS Session Service
- TCP 445: Server Message Block (SMB)

Note Cisco ISE supports SMB 2.0.

Higher ports are assigned dynamically, or you can configure them manually. We recommend that you add *%SystemRoot%\System32\dllhost.exe* as a target. This program manages ports dynamically.

All firewall rules can be assigned to a specific IP address (Cisco ISE IP).

Select Configuration Baseline Policies for Endpoint Compliance from Desktop Device Manager Server

You can view the baseline policies available in a Desktop Device Manager server (for example, a Microsoft SCCM server) added to Cisco ISE, and choose specific baseline policies to check for endpoint compliance for network access. The configuration baseline policies that are enabled and deployed in the Desktop Device Manager server can be viewed in the Cisco ISE administration portal.

Note Check your user privileges in your desktop device management server to ensure you have the required security permissions to allow baseline policies and compliance information to be sent to Cisco ISE. An administrator must be added in the **Security > Administrator Users** folder of the desktop device manager.

To view the baseline policies in a Desktop Device Manager server in the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **External MDM** > **MDM Servers**.

Add a New Desktop Device Manager Server to Cisco ISE, and Select Configuration Baseline Policies

1. In the **MDM Servers** window, click **Add**.
2. Choose **Desktop Device Manager** from the **Server Type** drop-down list.
3. Enter the required details for the following fields:
    - **Host Name / IP Address**: Enter the hostname or IP address of the Microsoft SCCM server.
    - **Instance Name**: If the Microsoft SCCM server has several instances, enter the instance that you want to connect to.
    - **Username**: Enter the username that must be used to connect to the Microsoft SCCM server.
    - **Password**: Enter the password that must be used to connect to the Microsoft SCCM server.
    - **Time Interval For Compliance Device ReAuth Query**: When an endpoint is authenticated or reauthenticated, Cisco ISE uses a cache to get the MDM variables for that endpoint. If the age of the cached value is higher than the value configured in this field, Cisco ISE sends a new device query to the MDM server to get new values. If the compliance status has changed, then Cisco ISE triggers the appropriate CoA.

      The valid range is from 1 to 10080 minutes. The default value is one minute.
4. Choose **Enabled** from the **Status** drop-down list.

To verify that the server is connected to Cisco ISE, click the **Test Connection** button. To view the configuration baseline policies available in this server, click **Save & Continue**. A new window is displayed with a list of names and IDs of the baseline policies.

Select Configuration Baseline Policies from an Existing Desktop Device Manager Server

In the **MDM Servers** window, check the check box for the desired server and click **Edit**. Click the **Configuration Baselines** tab for the list of the baseline policies available in this server.

By default, all the baseline policies are selected. Uncheck the check box next to **Name** to deselect all the baseline policies. Select the required baseline policies by checking the check boxes next to their names. Click **Save**.

Endpoint compliance is checked based on the selected configuration baseline policies.

If there are any changes in the configuration baseline policies in a Desktop Device Manager server, click the **Update Now** button in the **Configuration Baselines** tab for the changes to be updated in Cisco ISE.

Configure Device Identifiers for Windows Endpoints

A Desktop Device Manager server uses certain attributes as identifiers to verify endpoints connecting to the network. The endpoint MAC address is the most popularly used identifier. However, MAC addresses are not the most reliable identifiers when dongles, docking stations, or MAC address randomization techniques are in use.

You can now choose to use hostnames as identifiers. The hostnames are derived from common name (CN) or SAN-DNS attributes available in certificates. Certificate-based authentication of endpoints is mandatory to check for baseline policy compliance using hostnames.

To configure device identifiers for a Desktop Device Manager server, go to its **Server Configuration** tab. From the main menu, choose **Administration** > **Network Resources** > **External MDM** > **MDM Servers** > **Edit**.

In the **Device Identifier Configurations** section, the following identifiers are enabled by default, in this order:

1. **Legacy MAC Address**
2. **Cert – CN, Hostname**
3. **Cert – SAN-DNS, Hostname**

To deselect an identifier, uncheck the check box against the identifier. You can drag the attributes to rearrange the order in which the server must use them for verification.

Verify Configuration of Device Identifiers

When hostnames are used for verification, a GUID is assigned to the endpoint by Cisco ISE. See the **Live Logs** window (In the Cisco ISE GUI, click the **Menu** icon (☰) and choose**Operations** > **RADIUS** > **Live Logs**), and check the GUID entry for details.

Configure an Authorization Profile for Redirecting Nonregistered Devices

You must configure an authorization profile in Cisco ISE to redirect nonregistered devices for each external MDM server.

Before you begin

- Ensure that you have created an MDM server definition in Cisco ISE. Only after you successfully integrate Cisco ISE with the MDM server is the MDM dictionary populated. You can then create an authorization policy using the MDM dictionary attributes.

- Configure ACLs on the Cisco WLC for redirecting unregistered devices.
- If you are using a proxy for Internet connection and the MDM server is part of the internal network, then you have to put the MDM server name or its IP address in the Proxy-Bypass list. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Proxy** to perform this action.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles** > **Add**.

Step 2 Create an authorization profile for redirecting nonregistered devices that are not compliant or registered.

Step 3 Enter a name for the authorization profile that matches the MDM server name, in the **Name** field.

Step 4 Choose **ACCESS_ACCEPT** from the **Access Type** drop-down list.

Step 5 In the **Common Tasks** section, check the **Web Redirection** check box and choose **MDM Redirect** from the drop-down list.

Step 6 Choose the name of the ACL that you configured on the wireless LAN controller from the **ACL** drop-down list.

Step 7 Choose the MDM portal from the **Value** drop-down list.

Step 8 Choose the MDM server that you want to use from the **MDM Server** drop-down list.

Step 9 Click **Submit**.

What to do next

Configure Authorization Policy Rules for the MDM Use Cases.

Configure Authorization Policy Rules for the MDM Use Cases

Configure authorization policy rules in Cisco ISE to complete the MDM configuration.

Before you begin

- Add the MDM server certificate to the Cisco ISE certificate store.
- Ensure that you have created the MDM server definition in Cisco ISE. Only after you successfully integrate Cisco ISE with the MDM server does the MDM dictionary get populated, and you can create an authorization policy using the MDM dictionary attributes.
- Configure ACLs on the Cisco WLC for redirecting unregistered or noncompliant devices.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Sets**, and expand the policy set to view the authorization policy rules.

Step 2 Add the following rules:

- **MDM_Un_Registered_Non_Compliant**: For devices that are not yet registered with an MDM server or noncompliant with MDM policies. When a request matches this rule, the Cisco ISE MDM window is displayed to a user, with information on registering the device with the MDM server.

Note Do not use the **MDM.MDMServerName** condition in this policy. When this condition is used, an endpoint matches the policy only if the endpoint is registered with the MDM server.

- **PERMIT**: If the device is registered with Cisco ISE, registered with MDM, and is compliant with Cisco ISE and MDM policies, it is granted access to the network based on the access control policies configured in Cisco ISE.

Step 3 Click **Save**.

Configure ACLs on Wireless Controllers for MDM Interoperability

Configure ACLs on the Wireless Controller for use in an authorization policy to redirect nonregistered devices and certificate provisioning. Your ACLs must be in the following sequence.

Step 1 Allow all outbound traffic from the server to the client.

Step 2 (Optional) Allow ICMP inbound traffic from the client to the server for troubleshooting.

Step 3 Allow access to the MDM server for unregistered and noncompliant devices to download the MDM agent and proceed with compliance checks.

Step 4 Allow all inbound traffic from the client to the server to Cisco ISE for the web portal and supplicant, and certificate provisioning flows.

Step 5 Allow inbound Domain Name System (DNS) traffic from the client to the server for name resolution.

Step 6 Allow inbound DHCP traffic from the client to the server for IP addresses.

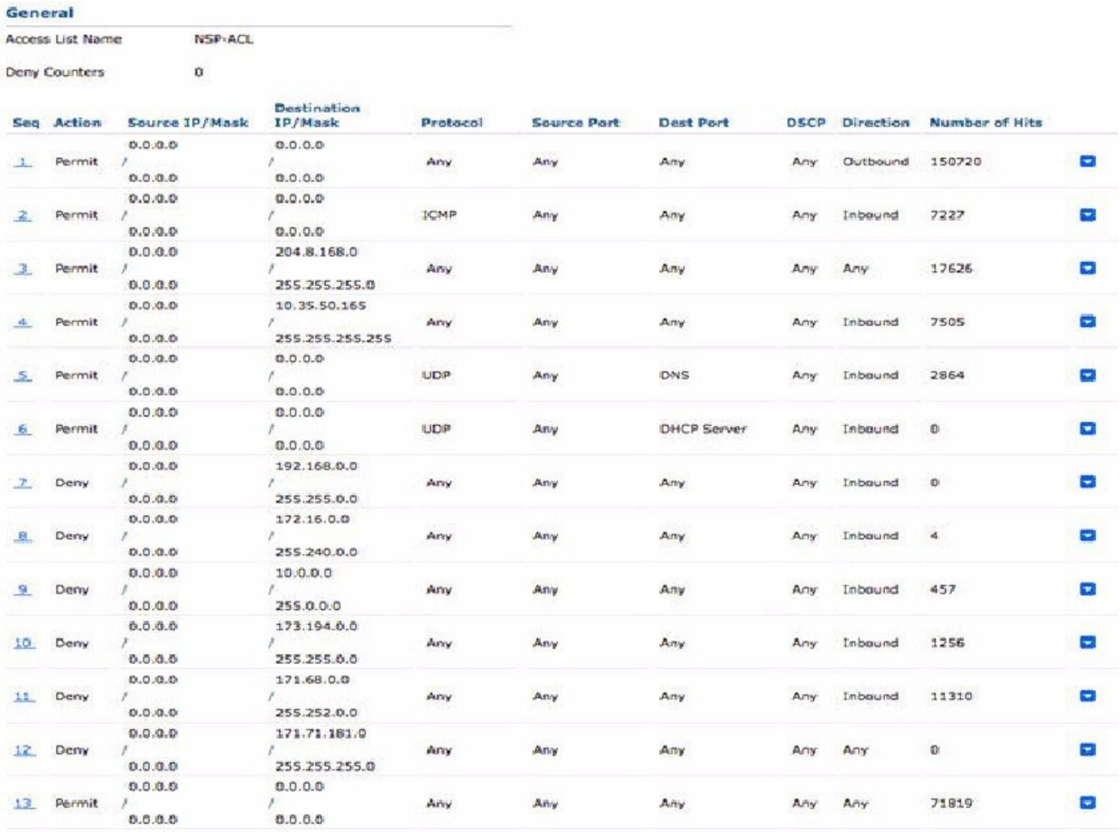
Step 7 Deny all inbound traffic from the client to the server to corporate resources for redirection to Cisco ISE (as per your company policy).

Step 8 (Optional) Permit the rest of the traffic.

Example

The following example shows the ACLs for redirecting a nonregistered device to the BYOD flow. In this example, the Cisco ISE IP address is 10.35.50.165, the internal corporate network IP addresses are 192.168.0.0 and 172.16.0.0 (to redirect), and the MDM server subnet is 204.8.168.0.

Figure 40: ACLs for Redirecting Nonregistered Device



General

Access List Name NSP-ACL

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819

Wipe or Lock a Device

Cisco ISE allows you to wipe or enable a pin lock for a lost device. You can configure this from the **Endpoints** window.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Identities** > **Endpoints**.

Step 2 Check the check box next to the device that you want to wipe or lock.

Step 3 From the **MDM Actions** drop-down list, choose one of the following options:

- **Full Wipe**: Depending on the MDM vendor, this option either removes the corporate apps or resets the device to the factory settings.
- **Corporate Wipe**: This option removes applications that you have configured in the MDM server policies.
- **PIN Lock**: This option locks the device.

Step 4 Click **Yes** to wipe or lock the device.

View Mobile Device Management Reports

Cisco ISE records all additions, updates, and deletions of MDM server definitions. You can view these events in the **Change Configuration Audit** report, which displays all the configuration changes from any system administrator for a selected time period.

In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Operations** > **Reports** > **Reports** > **Audit** > **Change Configuration Audit**. Check the entries in the **Object Type** and **Object Name** columns for the MDM server that you want to review, and click the corresponding **Event** value to view the details of the configuration event.

View Mobile Device Management Logs

You can use the **Debug Wizard** window to view mobile device management log messages. In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Operations** > **Troubleshoot** > **Degug Wizard** > **Debug Log Configuration**. Click the radio button next to a Cisco ISE node and click **Edit**. In the new window displayed, click the radio button next to the component name **external-mdm**, and click **Edit**. The default log level for this component is **INFO**. Choose **DEBUG** or **TRACE** from the corresponding **Log Level** drop-down list, and click **Save**.

CHAPTER 12

Segmentation

- Policy Sets, on page 975
- Policy Set Configuration Settings, on page 977
- Authentication Policies, on page 978
- Authorization Policies, on page 987
- Policy Conditions, on page 1001
- Special Network Access Conditions , on page 1020
- Policy Set Protocol Settings, on page 1024
- Enable MAB from Non-Cisco Devices, on page 1068
- Enable MAB from Cisco Devices, on page 1069
- TrustSec Architecture, on page 1071
- Integration with Cisco Catalyst Center, on page 1074
- TrustSec Dashboard, on page 1075
- Configure TrustSec Global Settings, on page 1078
- Configure TrustSec Matrix Settings, on page 1082
- Configure TrustSec Devices, on page 1084
- Configure Cisco TrustSec AAA Servers, on page 1086
- TrustSec HTTPS Servers, on page 1087
- Security Groups Configuration, on page 1089
- Egress Policy, on page 1096
- SGT Assignment, on page 1110
- TrustSec Configuration and Policy Push, on page 1112
- Security Group Tag Exchange Protocol , on page 1120
- Add an SXP Domain Filter, on page 1122
- Configure SXP Settings, on page 1123
- Connect Cisco Application Centric Infrastructure with Cisco ISE, on page 1124
- Configure ACI Settings, on page 1125
- Cisco ACI and Cisco SD-Access Integration with Virtual Network Awareness, on page 1127
- Run Top N RBACL Drops by User Report, on page 1137

Policy Sets

Cisco ISE is a policy-based, network-access-control solution, which offers network access policy sets, allowing you to manage several different network access use cases such as wireless, wired, guest, and client provisioning.

Policy sets (both network access and device administration sets) enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type, and similar parameters. When you install Cisco ISE, there is always one policy set defined, which is the default policy set, and the default policy set contains within it, predefined and default authentication, authorization and exception policy rules.

When creating policy sets, you can configure these rules (configured with conditions and results) in order to choose the network access services on the policy set level, the identity sources on the authentication policy level, and network permissions on the authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE-supported dictionaries for different vendors. Cisco ISE allows you to create conditions as individual resuable policy elements.

The network access service to be used per policy set to communicate with the network devices is defined at the top level of that policy set. Network access services include:

- Allowed protocols—the protocols configured to handle the initial request and protocol negotiation.
- A proxy service—sends requests to an external RADIUS server for processing.

Note From the **Work Centers** > **Device Administration** , you can also select a relevant TACACS server sequence for your policy set. Use the TACACS server sequence to configure a sequence of TACACS proxy servers for processing.

Policy sets are configured hierarchically, where the rule on the top level of the policy set, which can be viewed from the **Policy Set** table, applies to the entire set and is matched before the rules for the rest of the policies and exceptions. Thereafter, rules of the set are applied in this order:

1. Authentication policy rules
2. Local policy exceptions
3. Global policy exceptions
4. Authorization policy rules

Note Policy Sets functionality is identical for network access and for device administration policies. All processes described in this chapter can be applied when working with both the **Network Access** and the **Device Administration** work centers. This chapter specifically discusses the Network Access work center policy sets. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Policy Sets**.

ISE Community Resource

For information about using RADIUS results from a WLC, see WLC Called-Station-ID (Radius Authentication and Accounting Config) .

Policy Set Configuration Settings

The following table describes the fields in the **Policy Sets** window, from which you can configure policy sets, including authentication, exception and authorization policies. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Policy Sets** for network access policies.In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Device Admin Policy Sets** for device administration policies.

Table 142: Policy Set Configuration Settings

Field Name	Usage Guidelines
Status	Choose the status of this policy. It can be one of the following: • **Enabled**: This policy condition is active. • **Disabled**: This policy condition is inactive and will not be evaluated. • **Monitor Only**: This policy condition will not be evaluated.
Policy Set Name	Enter a unique name for this policy set.
Conditions	From a new policy row, click the plus (+) icon or from an existing policy row, click the Edit icon to open the Conditions Studio.
Description	Enter a unique description for the policy.
Allowed Protocols or Server Sequence	Choose an allowed protocol that you have already created, or click the (+) sign to **Create a New Allowed Protocol** , to **Create a New Radius Sequence**, or to **Create a TACACS Sequence**.
Conditions	From a new exceptions row, click the plus (+) icon or from an existing exception row, click the Edit icon to open the Conditions Studio.
Hits	Hits are a diagnostic tool indicating the number of times the conditions have matched. Hover over the icon to view when this was last updated, reset to zero and to view the frequency of updates.

Field Name	Usage Guidelines
Actions	Click the cog icon ⚙ from the Actions column to view and select different actions: • Insert new row above: Insert a new policy above the policy from which you opened the Actions menu. • Insert new row below: Insert a new policy below the policy from which you opened the Actions menu. • Duplicate above: Insert a duplicate policy above the policy from which you opened the Actions menu, above the original set. • Duplicate below: Insert a duplicate policy below the policy from which you opened the Actions menu, below the original set. • Delete: Delete the policy set.
View	Click the arrow icon to open the Set view of the specific policy set and view its authentication, exception, and authorization sub-policies.

Authentication Policies

Each policy set can contain multiple authentication rules that together represent the authentication policy for that set. Priority of the authentication policies is determined based on the order to those policies as they appear within the policy set itself (from the Set view page in the Authentication Policy area).

Cisco ISE dynamically chooses the network access service (either an allowed protocol a server sequence) based on the settings configured on the policy set level, and thereafter checks the identity sources and results from the authentication and authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE dictionary. Cisco ISE allows you to create conditions as individual policy elements that can be stored in the Library and then can be reused for other rule-based policies.

The identity method, which is the result of the authentication policy, can be any one of the following:

- Deny access—Access to the user is denied and no authentication is performed.
- Identity database—A single identity database that can be any one of the following:
  - Internal users
  - Guest users
  - Internal endpoints
  - Active Directory
  - Lightweight Directory Access Protocol (LDAP) database

  - RADIUS token server (RSA or SafeWord server)
  - Certificate authentication profile
- Identity source sequences—A sequence of identity databases that is used for authentication.

The default policy set implemented at initial Cisco ISE installation includes the default ISE authentication and authorization rules. The default policy set also includes additional flexible built-in rules (that are not defaults) for authentication and authorization. You can add additional rules to those policies and you can delete and change the built-in rules but you cannot remove the default rules and you cannot remove the default policy set.

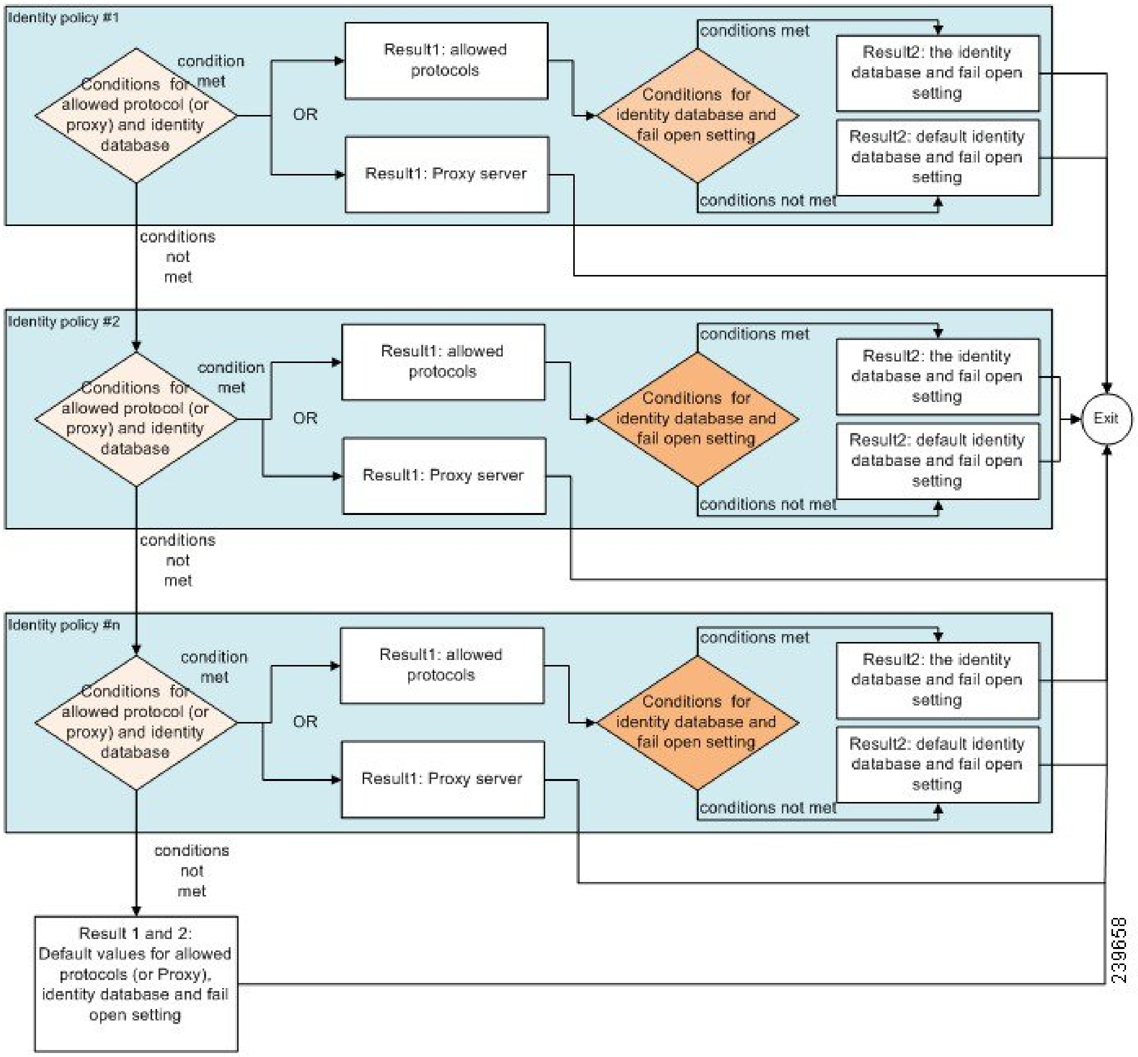
Authentication Policy Flow

In authentication policies, you can define multiple rules, which consist of conditions and results. ISE evaluates the conditions that you have specified and based on the result of the evaluation, assigns the corresponding results. The identity database is selected based on the first rule that matches the criteria.

You can also define an identity source sequence consisting of different databases. You can define the order in which you want Cisco ISE to look up these databases. Cisco ISE will access these databases in sequence until the authentication succeeds. If there are multiple instances of the same user in an external database, the authentication fails. There can only be one user record in an identity source.

We recommend that you use only three, or at most four databases in an identity source sequence.

Figure 41: Authentication Policy Flow


Identity policy #1
Conditions for allowed protocol (or proxy) and identity database
condition met
OR
Result1: allowed protocols
Result1: Proxy server
conditions met
Conditions for identity database and fail open setting
conditions not met
Result2: the identity database and fail open setting
Result2: default identity database and fail open setting
conditions not met
Identity policy #2
Identity policy #n
Exit
Result 1 and 2: Default values for allowed protocols (or Proxy), identity database and fail open setting
239658

Authentication Failures—Policy Result Options

If you choose the identity method as deny access, a reject message is sent as a response to the request. If you choose an identity database or an identity source sequence and the authentication succeeds, the processing continues to the authorization policy configured for the same policy set. Some of the authentications fail and these are classified as follows:

- Authentication failed—Received explicit response that authentication has failed such as bad credentials, disabled user, and so on. The default course of action is reject.
- User not found—No such user was found in any of the identity databases. The default course of action is reject.
- Process failed—Unable to access the identity database or databases. The default course of action is drop.

Cisco ISE allows you to configure any one of the following courses of action for authentication failures:

- Reject—A reject response is sent.
- Drop—No response is sent.
- Continue—Cisco ISE continues with the authorization policy.

Even when you choose the Continue option, there might be instances where Cisco ISE cannot continue processing the request due to restrictions on the protocol that is being used. For authentications using PEAP, LEAP, EAP-FAST, EAP-TLS, or RADIUS MSCHAP, it is not possible to continue processing the request when authentication fails or user is not found.

When authentication fails, it is possible to continue to process the authorization policy for PAP/ASCII and MAC authentication bypass (MAB or host lookup). For all other authentication protocols, when authentication fails, the following happens:

- Authentication failed—A reject response is sent.
- User or host not found—A reject response is sent.
- Process failure—No response is sent and the request is dropped.

Use Cases for Using Continue as the Course of Action for Authentication Failures

If you select the **Continue** option, Cisco ISE skips authentication and proceeds to evaluate the authorization policy in the following cases:

- Lookup (MAB)- Cisco ISE proceeds with authorization policy evaluation even if the ‘User not found’ result is displayed.
- PAP or ASCII
- CHAP
- EAP-MD5
- EAP-TLS - Cisco ISE proceeds with authorization policy evaluation even if the user or certificate validation has failed in AD or LDAP.
- PEAP (EAP-TLS) - Cisco ISE proceeds with authorization policy evaluation even if the user or certificate validation has failed in AD or LDAP.
- TEAP (EAP-TLS) - Cisco ISE proceeds with authorization policy evaluation even if the user or certificate validation has failed in AD or LDAP.
- EAP-FAST (EAP-TLS) - Cisco ISE proceeds with authorization policy evaluation even if the user or certificate validation has failed in AD or LDAP.
- EAP-chaining TEAP (EAP-TLS, EAP-MS-CHAPv2) - Cisco ISE proceeds with authorization policy evaluation even if the user or certificate validation has failed in AD or LDAP. Note that the Continue option is only applicable for the EAP-TLS inner method.

If there is an authentication failure in the following authentication protocols, all the chosen **Advanced** options are ignored, and Cisco ISE sends an **Access-Reject** response.

- MS-CHAPv1
- MS-CHAPv2

- LEAP
- PEAP (EAP-MS-CHAPv2)
- TEAP (EAP-MS-CHAPv2)
- EAP-FAST (EAP-MS-CHAPv2)
- EAP-TTLS (PAP\ASCII)
- EAP-TTLS (MS-CHAPv1)
- EAP-TTLS (MS-CHAPv2)
- EAP-TTLS (EAP-MD5)
- EAP-TTLS (CHAP)
- EAP-TTLS (EAP-MS-CHAPv2)
- EAP-FAST (EAP-GTC)
- PEAP (EAP-GTC)

Configure Authentication Policies

Define an authentication policy per policy set by configuring and maintaining multiple authentication rules, as necessary.

Before you begin

To perform the following task, you must be a Super Admin or Policy Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Policy Sets** for network access policies. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Device Admin Policy Sets** for device administration policies.

Step 2 From the row for the policy set from which you would like to add or update an authentication policy, click › from the View column in the Policy Sets table, in order to access all of the policy set details and to create authentication and authorization policies as well as policy exceptions.

Step 3 Click the arrow icon next to the Authentication Policy part of the page to expand and view all of the Authentication Policy rules in the table.

Step 4 From the **Actions** column on any row, click the cog icon. From the dropdown menu, insert a new authentication policy rule by selecting any of the insert or duplicate options, as necessary.
A new row appears in the Authentication Policy table.

Step 5 From the **Status** column, click the current **Status** icon and from the dropdown list update the status for the policy set as necessary. For more information about status, seeAuthentication Policy Configuration Settings, on page 983 .

Step 6 For any rule in the table, click in the **Rule Name** or **Description** cells to make any free-text changes necessary.

Step 7 To add or change conditions, hover over the cell in the **Conditions** column and click ✎. The Conditions Studio opens. For more information, see Special Network Access Conditions , on page 1020.

Not all attributes you select will include the “Equals”, “Not Equals", "In", "Not In", “Matches", “Starts With" or “Not Starts With” operator options.

The “Matches” operator supports and uses regular expressions (REGEX) not wildcards.

Note You must use the “equals” operator for straight forward comparison. “Contains” operator can be used for multi-value attributes. “Matches” operator should be used for regular expression comparison. When “Matches” operator is used, regular expression will be interpreted for both static and dynamic values. In case of lists, the "in" operator checks whether a particular value exists in a list. In case of a single string the "in" operator checks whether the strings are same like the "equals" operator.

Step 8 Organize the policies within the table according to the order by which they are to be checked and matched. To change the order of the rules, drag and drop the rows in to their correct position.

Step 9 Click **Save** to save and implement your changes.

What to do next

1. Configure authorization policies

Authentication Policy Configuration Settings

The following table describes the fields in the **Authentication Policy** section of the **Policy Sets** window, from which you can configure authentication subpolicies as part of your policy sets.In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Policy Sets** for network access policies. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Device Admin Policy Sets**for device administration policies. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy Sets** > **View** > **Authentication Policy**

Table 143: Authentication Policy Configuration Settings

Field Name	Usage Guidelines
Status	Choose the status of this policy. It can be one of the following: • **Enabled**: This policy condition is active. • **Disabled**: This policy condition is inactive and will not be evaluated. • **Monitor Only**: This policy condition will be evaluated, but the result will not be enforced. You can view the results of this policy condition in the Live Log authentication page. In this, see the detailed report which will have the monitored step and attribute. For example, you may want to add a new policy condition, but are not sure if the condition would provide you with the correct results. In this situation, you can create the policy condition in monitored mode to view the results and then enable it if you are satisfied with the results.
Rule Name	Enter a name for this authentication policy.
Conditions	From a new policy row, click the plus (+) icon or from an existing policy row, click the Edit icon to open the **Conditions Studio**.
Use	Choose the identity source that you want to use for authentication. You can also choose an identity source sequence if you have configured it. You can edit the default identity source that you want Cisco ISE to use in case none of the identity sources defined in this rule match the request.
Options	Define a further course of action for authentication failure, user not found, or process failure events. You can choose one of the following options: • **Reject**: A reject response is sent. • **Drop**: No response is sent. • **Continue**: Cisco ISE proceeds with the authorization policy.
Hits	Hits are a diagnostic tool indicating the number of times the conditions have matched.

Field Name	Usage Guidelines
Actions	Click the cog icon ⚙ from the Actions column to view and select different actions: • Insert new row above: Insert a new authentication policy above the policy from which you opened the Actions menu. • Insert new row below: Insert a new authentication policy below the policy from which you opened the Actions menu. • Duplicate above: Insert a duplicate authentication policy above the policy from which you opened the Actions menu, above the original set. • Duplicate below: Insert a duplicate authentication policy below the policy from which you opened the Actions menu, below the original set. • Delete: Delete the policy set.

Password-Based Authentication

Authentication verifies user information to confirm user identity. Traditional authentication uses a name and a fixed password. This is the most popular, simplest, and least-expensive method of authentication. The disadvantage is that this information can be told to someone else, guessed, or captured. An approach that uses simple, unencrypted usernames and passwords is not considered a strong authentication mechanism, but it can be sufficient for low-authorization or low-privilege levels such as Internet access.

Secure Authentication Using Encrypted Passwords and Cryptographic Techniques

You should use encryption to reduce the risk of password capture on the network. Client and server access control protocols, such as RADIUS, encrypt passwords to prevent them from being captured within a network. However, RADIUS operates only between the authentication, authorization, and accounting (AAA) client and Cisco ISE. Before this point in the authentication process, unauthorized persons can obtain cleartext passwords such as in the following examples:

- In the communication between an end-user client that dials up over a phone line.
- On an ISDN line that terminates at a network access server.
- Over a Telnet session between an end-user client and the hosting device

More-secure methods use cryptographic techniques, such as those used inside the Challenge Authentication Handshake Protocol (CHAP), one-time password (OTP), and advanced EAP-based protocols. Cisco ISE supports a variety of these authentication methods.

Authentication Methods and Authorization Privileges

A fundamental implicit relationship exists between authentication and authorization. The more authorization privileges that are granted to a user, the stronger the authentication should be. Cisco ISE supports this relationship by providing various methods of authentication.

Authentication Dashlet

The Cisco ISE dashboard provides a summary of all authentications that take place in your network and for your devices. It provides at-a-glance information about authentications and authentication failures in the **Authentications** dashlet.

The **RADIUS Authentications** dashlet provides the following statistical information about the authentications that Cisco ISE has handled:

- The total number of RADIUS authentication requests that Cisco ISE has handled, including passed authentications, failed authentications, and simultaneous logins by the same user.
- The total number of failed RADIUS authentications requests that Cisco ISE has processed.

You can also view a summary of TACACS+ authentications. The TACACS+ Authentications dashlet provides statistical information for device authentications.

For more information about device administration authentications, see TACACS Live Logs, on page 449. For additional information about RADIUS Live Logs settings, see RADIUS Live Logs, on page 443.

ISE Community Resource

For information on how to troubleshoot failed authentications and authorizations, see How To: Troubleshoot ISE Failed Authentications & Authorizations.

View Authentication Results

Cisco ISE provides various ways to view real-time authentication summary.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **RADIUS** > **Live Logs** for network authentications (RADIUS). In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **TACACS** > **Live Logs** to view the real-time authentication summaries.

Step 2 You can view the authentication summary in the following ways:

- Hover your mouse cursor over the Status icon to view the results of the authentication and a brief summary. A pop-up with status details appears.
- Enter your search criteria in any one or more of the text boxes that appear at the top of the list, and press **Enter,** to filter your results.
- Click the magnifier icon in the **Details** column to view a detailed report.

Note As the **Authentication Summary** report or dashboard collects and displays the latest data corresponding to failed or passed authentications, the contents of the report appear after a delay of a few minutes.

Authentication Reports and Troubleshooting Tools

Apart from the authentication details, Cisco ISE provides various reports and troubleshooting tools that you can use to efficiently manage your network.

There are various reports that you can run to understand the authentication trend and traffic in your network. You can generate reports for historical as well as current data. The following is a list of authentication reports:

- AAA Diagnostics
- RADIUS Accounting
- RADIUS Authentication
- Authentication Summary

Note You must enable IPv6 snooping on Cisco Catalyst 4000 Series switches, otherwise IPv6 address will not be mapped to the authentication sessions and will not be displayed in the show output. Use the following commands to enable IPv6 snooping:

```
vlan config <vlan-number>
 ipv6 snooping
 end
ipv6 nd raguard policy router
 device-role router
interface <access-interface>
  ipv6 nd raguard
interface <uplink-interface>
  ipv6 nd raguard attach-policy router
  end
```

Authorization Policies

Authorization policies are a component of the Cisco ISE network authorization service. This service allows you to define authorization policies and configure authorization profiles for specific users and groups that access your network resources.

Authorization policies can contain conditional requirements that combine one or more identity groups using a compound condition that includes authorization checks that can return one or more authorization profiles. In addition, conditional requirements can exist apart from the use of a specific identity group.

Authorization profiles are used when creating authorization policies in Cisco ISE. An authorization policy is composed of authorization rules. Authorization rules have three elements: name, attributes, and permissions. The permission element maps to an authorization profile.

Cisco ISE Authorization Profiles

Authorization policies associate rules with specific user and group identities to create the corresponding profiles. Whenever these rules match the configured attributes, the corresponding authorization profile that grants permission is returned by the policy and network access is authorized accordingly.

For example, authorization profiles can include a range of permissions that are contained in the following types:

- Standard profiles
- Exception profiles
- Device-based profiles

Profiles consist of attributes chosen from a set of resources, which are stored in any of the available vendor dictionaries, and these are returned when the condition for the specific authorization policy matches. Because authorization policies can include condition mapping to a single network service rule, these can also include a list of authorization checks.

authorization verifications must comply with the authorization profiles to be returned. Authorization verifications typically comprise one or more conditions, including a user-defined name that can be added to a library, which can then be reused by other authorization policies.

Permissions for Authorization Profiles

Before you start configuring permissions for authorization profiles, make sure you:

- Understand the relationship between authorization policies and profiles.
- Are familiar with the **Authorization Profile** page.
- Know the basic guidelines to follow when configuring policies and profiles.
- Understand what comprises permissions in an authorization profile.

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** to work with authorization profiles. From the menu on the left, choose **Authorization** > **Authorization Profiles**.

Use the **Results** navigation pane as your starting point in the process for displaying, creating, modifying, deleting, duplicating, or searching policy element permissions for the different types of authorization profiles on your network. The **Results** pane initially displays Authentication, Authorization, Profiling, Posture, Client Provisioning, and Trustsec options.

Authorization profiles let you choose the attributes to be returned when a RADIUS request is accepted. Cisco ISE provides a mechanism where you can configure **Common Tasks Settings** to support commonly used attributes. You must enter the value for **Common Tasks Attributes**, which Cisco ISE translates to the underlying RADIUS values.

ISE Community Resource

For an example of how to configure Media Access Control Security (MACsec) encryption between an 802.1x supplicant (Cisco AnyConnect Mobile Security) and an authenticator (switch), see MACsec Switch-host Encryption with Cisco AnyConnect and ISE Configuration Example.

Location Based Authorization

Cisco ISE integrates with Cisco Mobility Services Engine (MSE) to introduce physical location-based authorization. Cisco ISE uses information from MSE to provide differentiated network access based on the actual location of the user, as reported by MSE.

With this feature, you can use the endpoint location information to provide network access when a user is in an appropriate zone. You can also add the endpoint location as an additional attribute for policies to define more granulated policy authorization sets based on device location. You can configure conditions within authorization rules that use location-based attributes, for example:

MSE.Location Equals LND_Campus1:Building1:Floor2:SecureZone

You can define the location hierarchy (campus/building/floor structure) and configure the secure and non-secure zones using the Cisco Prime Infrastructure application. After defining the location hierarchy, you must synchronize the location hierarchy data with the MSE servers. For more information on Cisco Prime Infrastructure, see: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html.

You can add one or multiple MSE instances to integrate MSE-based location data to the authorization process. You can retrieve the location hierarchy data from these MSEs and configure location-based authorization rules using this data.

To track the endpoint movement, check the Track Movement check box while creating an authorization profile. Cisco ISE will query the relevant MSE for the endpoint location every 5 minutes to verify if the location was changed.

Note

- When adding an MSE device to Cisco ISE, copy the certificates from the MSE device over to ISE to facilitate authorization.
- Tracking multiple users will impact the performance due to frequent updates. The Track Movement option can be used for high security locations.
- The Location Tree is created by using the location data retrieved from the MSE instances. You can select the location entries that are exposed to the authorization policy by using the Location Tree.
- You will need Cisco ISE Advantage licenses to use the Location Services.

Add an MSE server

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration > Network Resources > Location Services > Location Servers**

Step 2 Click **Add**.

Step 3 Enter the MSE server details, such as server name, hostname/IP address, password, and so on.

Step 4 Click **Test** to test MSE connectivity using the server details that you have provided.

Step 5 (Optional) Enter the MAC address of an endpoint in the **Find Location** field and click **Find** to check whether the endpoint is currently connected to this MSE.

If the endpoint location is found, it is displayed in the following format: *Campus:Building:Floor:Zone*. Sometimes, more than one entry can be displayed depending on the location hierarchy and zone settings. For example, if all the floors of a building (*building1*) in a campus named *Campus1* are defined as non-secure zones, and the Lab Area in the first floor is defined as a secure zone, the following entries will be displayed when the endpoint is located in the Lab Area:

Found in:

Campus1#building1#floor1#LabArea

Campus1#building1#floor1#NonSecureZone

Step 6 Click **Submit**.
After a new MSE is added, go to the Location Tree page and click **Get Update** to retrieve its location hierarchy and add it to the Location Tree. If there are filters defined on this tree, these filters are applied on the new MSE entries as well.

Location Tree

The Location Tree is created by using the location data retrieved from the MSE instances. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Location Services** > **Location Tree**.

If one building has multiple MSEs, Cisco ISE will collate the location details from all the MSEs and present them as a single tree.

You can select the location entries that are exposed to the authorization policy by using the Location Tree. You can also hide specific locations based on your requirements. It is recommended to update the Location Tree before hiding locations. Hidden locations will remain hidden even when the tree is updated.

If the location entries related to an authorization rule are modified or removed, you must disable the affected rules and set these locations as Unknown or select a replacement location for each affected rule. You must verify the new tree structure before applying the change or canceling the update.

Click **Get Update** to get the latest location hierarchy structure from all MSEs. After verifying the new tree structure, click Save to apply your changes.

Downloadable ACLs

Access control lists (ACLs) are lists of access control entries (ACEs), which may be applied by a Policy Enforcement Point (for example, a switch) to a resource. Each ACE identifies the permissions allowed per user for that object, such as read, write, execute and more. For example, an ACL may be configured for 2 users in the Sales area of the network, with an ACE allowing Read and Write permissions for one of the users and another ACE allowing only Read only permission for the other user.

With Cisco ISE, downloadable ACLs (DACLs) can be configured and implemented in your authorization policies for control of how the network is accessed by different users and groups of users. DACLs can also be configured using the custom user attributes and AD attributes.

Note If a DACL used in an Identity Provider (IdP) authorization policy is empty, authorization will fail.

To implement DACLs in your network authorization policy in Cisco ISE:

1. Configure a new or existing DACL from **Policy** > **Policy Elements** > **Results** > **Downloadable ACLs**. For more information, see Configure Permissions for Downloadable ACLs, on page 991.
2. Configure a new or existing authorization profile from **Policy** > **Policy Elements** > **Results** > **Authorization Profiles**, using any of the DACLs you already configured.
3. Implement the authorization profiles you have configured when creating and configuring new and existing policy sets from **Policy** > **Policy Sets**.

With RADIUS protocol, ACLs grant authorization by filtering source and destination IP addresses, transport protocols, and additional parameters. Static ACLs reside on and are directly configured from the switch and can be applied in your authorization policies from the ISE GUI.

Configure Permissions for Downloadable ACLs

Default authorization DACLs are available with installation of ISE, including the following default profiles:

- DENY_ALL_IPV4_TRAFFIC
- PERMIT_ALL_IPV4_TRAFFIC
- DENY_ALL_IPV6_TRAFFIC
- PERMIT_ALL_IPV6_TRAFFIC

When working with DACLs, these defaults cannot be changed, but you can duplicate them in order to create additional, similar, DACLs.

After configuring the DACLs that you need, you can apply those DACLs to relevant authorization policies on your network. You cannot edit or delete a DACL that is used in an authorization policy. You must first remove that DACL from the authorization policy to edit or delete that DACL. After updating the DACL, you can reapply the same DACL to the authorization policy, if needed.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Downloadable ACLs**.

Step 2 Click **Add** from the top of the **Downloadable ACLs** table or alternatively, choose any of the existing DACLs and click **Duplicate** from the top of the table.

Step 3 Enter or edit the desired values for the DACL, keeping in mind the following rules:

- Supported characters for the name field are: alphanumeric, hyphen(-), dot(.) and underscore(_)
- IP formats are handled based on the selected IP version when you choose the DACL type as follows:
  - **IPv4** to validate only IPv4 legal ACEs. You must enter a valid IPv4 format.
  - **IPv6** to validate only IPv6 legal ACEs. You must enter a valid IPv6 format.
  - DACLs upgraded from prior releases to release 2.6 shows the **Agnostic** option as DACL type in the **IP Version** field. Enter any format as required. Use **Agnostic** to create a DACL for devices not supported by Cisco. When **Agnostic** is selected, formats are not validated and you cannot check DACL syntax.
- The keyword **Any** must be the source in all ACEs in the DACL. Once the DACL is pushed, the **Any** in the source is replaced with the IP address of the client that is connecting to the switch.

Note The **IP Version** field is noneditable when DACL is mapped to any authorization profile. In this case, remove the DACL reference from **Authorization Profiles**, edit the IP version and remap the DACL in **Authorization Profiles**.

Step 4 Optionally, when you finish creating the complete list of ACEs, click **Check DACL Syntax** to validate the list. If there are validation errors, the check returns specific instructions identifying the invalid syntax in the window that opens automatically.

Step 5 Click **Submit**.

Machine Access Restriction for Active Directory User Authorization

Cisco ISE contains a Machine Access Restriction (MAR) component that provides an additional means of controlling authorization for Microsoft Active Directory-authentication users. This form of authorization is based on the machine authentication of the computer used to access the Cisco ISE network. For every successful machine authentication, Cisco ISE caches the value that was received in the RADIUS Calling-Station-ID attribute (attribute 31) as evidence of a successful machine authentication.

Cisco ISE retains each Calling-Station-ID attribute value in cache until the number of hours that was configured in the "Time to Live" parameter in the Active Directory Settings page expires. Once the parameter has expired, Cisco ISE deletes it from its cache.

When a user authenticates from an end-user client, Cisco ISE searches the cache for a Calling-Station-ID value from successful machine authentications for the Calling-Station-ID value that was received in the user authentication request. If Cisco ISE finds a matching user-authentication Calling-Station-ID value in the cache, this affects how Cisco ISE assigns permissions for the user that requests authentication in the following ways:

- If the Calling-Station-ID value matches one found in the Cisco ISE cache, then the authorization profile for a successful authorization is assigned.
- If the Calling-Station-ID value is not found to match one in the Cisco ISE cache, then the authorization profile for a successful user authentication without machine authentication is assigned.

Guidelines for Configuring Authorization Policies and Profiles

Observe the following guidelines when managing or administering authorization polices and profiles:

- Rule names you create must use only the following supported characters:
    - Symbols: plus (+), hyphen (-), underscore (_), period (.), and a space ( ).
    - Alphabetic characters: A-Z and a-z.
    - Numeric characters: 0-9.
- Identity groups default to "Any" (you can use this global default to apply to all users).
- Conditions allow you to set one or more policy values. However, conditions are optional and are not required to create an authorization policy. These are the two methods for creating conditions:
    - Choose an existing condition or attribute from a corresponding dictionary of choices.
    - Create a custom condition that allows you to select a suggested value or use a text box to enter a custom value.

- Condition names you create must use only the following supported characters:
    - Symbols: hyphen (-), underscore (_), and period (.).
    - Alphabetic characters: A-Z and a-z.
    - Numeric characters: 0-9.
- When you create or edit an authorization profile, if you choose to enable **Web Redirection (CWA, MDM, NSP, CPP)** with any other option than the **Client Provisioning (Policy)** , you will not be able to configure IPv6 address as **Static IP/Host name/FQDN** for that authorization policy. This is because IPv6 Static IP/Host name/FQDN are not supported in Central Web Auth (CWA), Mobile Device Management (MDM) redirect, and Native Supplicant Protocol (NSP).
- Permissions are important when choosing an authorization profile to use for a policy. A permission can grant access to specific resources or allow you to perform specific tasks. For example, if a user belongs to a specific identity group (such as Device Admins), and the user meets the defined conditions (such as a site in Boston), then this user is granted the permissions associated with that group (such as access to a specific set of network resources or permission to perform a specific operation on a device).
- When you use the **radius** attribute **Tunnel-Private-Group-ID** in an authorization condition, you must mention both the tag and the value in the condition when the **EQUALS** operator is being used, for example:

```
Tunnel-Private-Group-ID EQUALS (tag=0) 77
```

Configure Authorization Policies

After creating attributes and building blocks for authorization policies from the Policy menu, create authorization policies within policy sets from the Policy Sets menu.

Before you begin

Before you begin this procedure, you should have a basic understanding of the different building blocks used to create authorization policies such as identify groups and conditions.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Policy Sets** for network access policies. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Device Admin Policy Sets** for device administration policies.

Step 2 From the View column, click › to access all of the policy set details and to create authentication and authorization policies as well as policy exceptions.

Step 3 Click the arrow icon next to the Authorization Policy part of the page to expand and view the Authorization Policy table.

Step 4 From the **Actions** column on any row, click the cog icon. From the dropdown menu, insert a new authorization policy rule by selecting any of the insert or duplicate options, as necessary.
A new row appears in the Authorization Policy table.

Step 5 To set the status for a policy, click the current **Status** icon and from the dropdown list select the necessary status from the **Status** column. For more information about statuses, see Authorization Policy Settings, on page 995.

Step 6 For any policy in the table, click in the **Rule Name** cells to make any free-text changes necessary and to create a unique rule name.

Step 7 To add or change conditions, hover over the cell in the **Conditions** column and click ✎. The **Conditions Studio** opens. For more information, seePolicy Conditions, on page 1001.

Not all attributes you select will include the “Equals”, “Not Equals", "In", "Not In", “Matches", “Starts With" or “Not Starts With” operator options.

The “Matches” operator supports and uses regular expressions (REGEX) not wildcards.

Note You must use the “equals” operator for straight forward comparison. “Contains” operator can be used for multi-value attributes. “Matches” operator should be used for regular expression comparison. When “Matches” operator is used, regular expression will be interpreted for both static and dynamic values. In case of lists, the "in" operator checks whether a particular value exists in a list. In case of a single string the "in" operator checks whether the strings are same like the "equals" operator.

Step 8 For network access results profiles, select the relevant authorization profile from the **Results Profiles** dropdown list or choose or click ✚, choose **Create a New Authorization Profile** and when the **Add New Standard Profile** screen opens, perform the following steps:

a) Enter values as required to configure a new authorization profile. Keep the following in mind:

- Supported characters for the name field are: space, ! # $ % & ‘ ( ) * + , - . / ; = ? @ _ {.
- For **Common Tasks**, to enter a DACL, choose the relevant **DACL Name** option as follows and then select the necessary DACL from the dynamic dropdown list:
  - To use an IPv4 DACL, check **DACL Name**.
  - To enter an IPv6 DACL, check **IPv6 DACL Name**.
  - To enter any other DACL syntax, check either option. Agnostic DACLs appear in both the IPv4 and the IPv6 dropdown lists.

    Note If you select **DACL Name**, then the AVP type is for IPv4, even if the DACL itself is agnostic. If you select a DACL for the **IPv6 DACL Name**, then the AVP type is for IPv6, even if the DACL itself is agnostic.

- **Note** If you choose to use ACL for your policy, ensure your device is compatible with this feature. For more information, see the *Cisco Identity Services Engine Compatibility Guide*.

  For **Common Tasks**, to enter an ACL, choose the relevant **ACL (Filter-ID)** option as follows and then type the ACL name in the field:
  - To use an IPv4 ACL, check **ACL (Filter-ID)**.
  - To enter an IPv6 ACL, check **ACL IPv6 (Filter-ID)**.
- To use an ACL for Airespace devices, check **Airespace ACL Name** or **Airespace IPv6 ACL Name** as necessary, and type the ACL name in the field.
- You can double-check the authorization profile RADIUS syntax from the **Attributes Details** that dynamically appear at the bottom of the screen.

b) Click **Save** to save your changes to the Cisco ISE system database to create an authorization profile.

c) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles** to create, manage, edit, and delete profiles outside of the Policy Sets area.

Step 9 For network access results security groups, select the relevant security group from the **Results Security Groups**dropdown list or click +, choose **Create a New Security Group** and when the Create New Security Group screen opens, perform the following steps:

a) Enter a name and description (optional) for the new security group.

b) Check the **Propagate to ACI** check box if you want to propagate this SGT to Cisco ACI. The SXP mappings that are related to this SGT will be propagated to Cisco ACI only if they belong to a VPN that is selected in the Cisco ACI Settings page.

This option is disabled by default.

c) Enter a Tag Value. Tag value can be set to be entered manually or autogenerate. You can also reserve a range for the SGT. You can configure it from the In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers > TrustSec > Settings > General TrustSec Settings**

d) Click **Submit**.

For more information, see Security Groups Configuration, on page 1089.

Step 10 For TACACS+ results, select the relevant Command Sets and Shell Profiles from the **Results** drop-down lists or click + in the **Command Sets** or **Shell Profiles** column to open the **Add Commands** Screen or **Add Shell Profile** respectively. Choose **Create a New Command Set** or **Create a New Shell Profile** and enter the fields.

Step 11 Organize the order by which the policies are to be checked and matched within the table.

Step 12 Click **Save** to save your changes to the Cisco ISE system database and create this new authorization policy.

Authorization Policy Settings

The following table describes the fields in the **Authorization Policy** section of the **Policy Sets** window, from which you can configure authorization policies as part of your policy sets. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Policy Sets** for network access policies. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Device Admin Policy Sets** for device administration policies.

Table 144: Authorization Policy Configuration Settings

Field Name	Usage Guidelines
Status	Choose the status of this policy. It can be one of the following: • **Enabled**: This policy condition is active. • **Disabled**: This policy condition is inactive and will not be evaluated. • **Monitor Only**: This policy condition will be evaluated, but the result will not be enforced. You can view the results of this policy condition in the Live Log authentication page. In this, see the detailed report which will have the monitored step and attribute. For example, you may want to add a new policy condition, but are not sure if the condition would provide you with the correct results. In this situation, you can create the policy condition in monitored mode to view the results and then enable it if you are satisfied with the results.
Rule Name	Enter a unique name for this policy.
Conditions	From a new policy row, click the plus (+) icon or from an existing policy row, click the Edit icon to open the Conditions Studio.
Results or Profiles	Select the relevant authorization profile, which determines the different levels of permissions offered to the configured security group. If you have not yet configured the relevant authorization profile, you can do so inline.
Results or Security Groups	Select the relevant security group, which determines the groups of users relevant to the specific rule. If you have not yet configured the relevant security group, you can do so inline.
Results or Command Sets	Command sets enforce the specified list of commands that can be executed by a device administrator. When a device administrator issues operational commands on a network device, ISE is queried to determine whether the administrator is authorized to issue these commands. This is also referred to as command authorization.
Results or Shell Profiles	TACACS+ shell profiles control the initial login session of the device administrator.

Field Name	Usage Guidelines
Hits	Hits are a diagnostic tool indicating the number of times the conditions have matched.
Actions	Click the cog icon ⚙ from the Actions column to view and select different actions: • Insert new row above: Insert a new authorization rule above the rule from which you opened the Actions menu. • Insert new row below: Insert a new authorization rule below the rule from which you opened the Actions menu. • Duplicate above: Insert a duplicate authorization rule above the rule from which you opened the Actions menu, above the original set. • Duplicate below: Insert a duplicate authorization rule below the rule from which you opened the Actions menu, below the original set. • Delete: Delete the rule.

Authorization Profile Settings

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**, the **Authorization Profiles** window define attributes for network access.

Note When upgrading from a Cisco ISE 2.x release to a Cisco ISE 3.x release in a non-Cisco device, if an Authorization profile contains a Network Device profile with a configured ACL value, an upgrade failure may occur. This occurs because a Network Device profile is not supposed to have an ACL configured in it.

To work around this issue, you can either remove the value manually or delete the corresponding Authorization profile itself.

Authorization Profile Settings

- **Name**: Enter a name for this new authorization profile.
- **Description**: Enter a description for this authorization profile.
- **Access Type**: Choose the access type: **ACCESS_ACCEPT** or **ACCESS_REJECT**.
- **Service Template**: Enable this option to support sessions with SAnet-capable devices. Cisco ISE implements service templates in authorization profiles using a special flag that marks them as *Service Template* compatible. Since the service template is also an authorization profile, it acts as a single policy that supports both SAnet and non-SAnet devices.

- **Track Movement**: Enable this option to track user location with Cisco Mobility Services Engine (MSE).

Note This option may impact Cisco ISE performance, it is only intended for high-security locations.

- **Passive Identity Tracking**: Enable this option to use the Easy Connect feature of Passive Identity for policy enforcement and user tracking.

Common Tasks

Common tasks are specific permissions and actions that apply to network access.

- **DACL Name** : Enable this option to use a downloadable ACL. You can use the default values (**PERMIT_ALL_IPV4_TRAFFIC**, **PERMIT_ALL_IPV6_TRAFFIC**, **DENY_ALL_IPV4_TRAFFIC**, **DENY_ALL_IPV6_TRAFFIC**), or select an attribute from the following dictionaries:
    - External identity store (attributes)
    - Endpoints
    - Internal User
    - Internal Endpoint

  For more information about adding DACLs or editing and managing existing DACLs, see Downloadable ACLs, on page 990.

- **ACL (Filter-ID)**: Enable this option to configure a RADIUS filter-ID attribute. The filter-ID specifies an ACL on the NAD. Your Filter-ID is displayed in the **Attributes Details** pane. **ACL IPv6 (Filter-ID)** works the same way for IPv6 connections to the NAD.

Note From Cisco ISE 3.0 onwards, you can enter the text or select the required attributes from the Attribute Values drop-down list for **ACL Filter-ID**. If you are entering the text for **ACL Filter-ID**, you must add the ".in" suffix for Cisco devices.

- **Security Group**: Enable this option to assign a security group (SGT) part of authorization.
    - If Cisco ISE is not integrated with Cisco DNA Center, Cisco ISE assigns VLAN ID 1.
    - If Cisco ISE is integrated with Cisco DNA Center, then select the Virtual Network (VN) that Cisco DNA Center shared with Cisco ISE, select the **Data Type**, and the subnet/address pool.

  A Security Group task includes a security group and an optional VN. If you configure a security group, then you cannot configure a VLAN separately. An endpoint device can only be assigned to one virtual network.

- **VLAN**: Enable this option to specify a virtual LAN (VLAN) ID. You can enter integer or string values for the VLAN ID. The format for this entry is `Tunnel-Private-Group-ID:VLANnumber`.

- **Voice Domain Permission** : Enable this option to use a downloadable ACL. The vendor-specific attribute (VSA) of `cisco-av-pair` is associated with the value `device-traffic-class=voice`. In multidomain authorization mode, if the network switch receives this VSA, the endpoint connects to a voice domain after authorization.

- **Web Redirection (CWA, DRW, MDM, NSP, CPP)**: Enable this option to enable web redirection after authentication.
    - Select the type of redirection. The type of Web Redirection that you select displays additional options, which are described below.
    - Enter an ACL to support the redirection that Cisco ISE sends to the NAD.

      The ACL you enter to send to the NAD displays in the **Attributes Details** pane as a cisco-av pair. For example, if you enter **acl119**, it is displayed in the **Attributes Details** pane as: `cisco-av-pair = url-redirect-acl = acl119`.
    - Select the other settings for the selected web redirection type.

  Select one of the following types web redirection:

    - **Centralized Web Auth**: Redirect to the portal you select from the **Value** drop-down.
    - **Client Provisioning (Posture)**: Redirect to the client provisioning portal you select from the **Value** drop-down, to enable posture on the client.
    - **Hot Spot: Redirect**: Redirect to the hot spot portal you select from the **Value** drop-down.
    - **MDM Redirect**: Redirect to the MDM portal on the MDM server that you specify.
    - **Native Supplicant Provisioning**: Redirect to the BYOD portal you select from the **Value** drop-down.

  After selecting the web redirection type, and entering the required parameters, configure the following options:

    - **Display Certificates Renewal Message**: Enable this option to display a certificate renewal message. The URL-redirect attribute value changes and includes the number of days for which the certificate is valid. This option is only for Centralized Web Auth redirection.
    - **Static IP/Host Name/FQDN**: Enable this option to redirect a user to a different PSN. Enter the target IP address, hostname, or FQDN. If you do not configure this option, the user is redirected to the FQDN of the policy service node that received this request.
    - **Suppress Profiler CoA for endpoints in Logical Profile**: Enable this option to cancel the redirect for a certain type of endpoint device.

- **Auto SmartPort**: Enable this option to use Auto SmartPort functionality. Enter an event name, which creates a VSA cisco-av-pair with that value as `auto-smart-port=event_name`. This value is displayed in the **Attributes Details** pane.
- **Access Vulnerabilities**: Enable this option to run the Threat Centric NAC Vulnerability Assessment on this endpoint as part of authorization. Select the adapter, and when to run the scan.
- **Reauthentication**: Enable this option to keep the endpoint connected during reauthentication. You choose to maintain connectivity during reauthentication by choosing to use **RADIUS-Request** (1). The default RADIUS-Request (0) disconnects the existing session. You can also set an inactivity timer.
- **MACSec Policy**: Enable this option to use the MACSec encryption policy whenever a MACSec enabled client connects to Cisco ISE. Choose one of the following options: **must-secure**, **should-secure**, or

must-not-secure. Your settings are displayed in the **Attributes Details** pane as: `cisco-av-pair = linksec-policy=must-secure`.

- **NEAT** : Enable this option to use Network Edge Access Topology (NEAT), which extends identity recognition between networks. Checking this check box displays `cisco-av-pair = device-traffic-class=switch` in the **Attributes Details** pane.
- **Web Authentication (Local Web Auth)** : Enable this option to use local web authentication for this authorization profile. This value lets the switch recognize authorization for web authentication by Cisco ISE sending a VSA along with a DACL. The VSA is `cisco-av-pair = priv-lvl=15`, which is displayed in the **Attributes Details** pane.
- **Airespace ACL Name**: Enable this option to send an ACL name to Cisco Airespace wireless controller. The Airespace VSA uses this ACL to authorize a locally defined ACL to a connection on the WLC. For example, if you entered **rsa-1188**, it is displayed as `Airespace-ACL-Name = rsa-1188` in the **Attributes Details** pane.
- **ASA VPN**: Enable this option to assign an Adaptive Security Appliances (ASA) VPN group policy. From the drop-down list, choose a VPN group policy.
- **AVC Profile Name**: Enable this option to run application visibility on this endpoint. Enter the AVC profile to use.
- **UPN Lookup**: TBD

Advanced Attributes Settings

- **Dictionaries**: Click the down arrow icon to view the available options in the **Dictionaries** window. Select a dictionary and an attribute that should be configured in the first field.
- **Attribute Values**: Click the down-arrow icon to display the available options in the **Attribute Values** window. Select the desired attribute group and the attribute value. This value is matched with the one selected in the first field. The **Advanced Attributes** settings that you configure are displayed in the **Attribute Details** panel.
- **Attributes Details**: This pane displays the configured attribute values that you have set for **Common Tasks** and **Advanced Attributes**.

  The values that are displayed in the **Attributes Details** pane are read-only.

Note To modify or delete any of the read-only values that are displayed in the **Attributes Details** pane, modify or delete these values in the corresponding **Common Tasks** field, or in the attribute that you selected in the **Attribute Values** field in the **Advanced Attributes Settings** pane.

Related Topics

Cisco ISE Authorization Profiles, on page 988
Permissions for Authorization Profiles, on page 988
Configure an Authorization Profile for Redirecting Nonregistered Devices, on page 969
Create Authorization Profiles, on page 510

Authorization Policy Exceptions

Within each policy set, you can define regular authorization policies, as well as local exception rules (defined from the Authorization Policy Local Exceptions part in the Set view for each policy set) and global exception rules (defined from the Authorization Policy Global Exceptions part in the Set view for each policy set).

Global authorization exception policies enable you to define rules that override all authorization rules in all of your policy sets. Once you configure a global authorization exception policy, it is added to to all policy sets. Global authorization exception policies can then be updated from within any of the currently configured policy sets. Every time you update a global authorization exception policy, those updates are applied to all policy sets.

The local authorization exception rule overwrites the global exception rule. The authorization rules are processed in the following order: first the local exception rule, then the global exception rule, and finally, the regular rule of the authorization policy.

Authorization exception policy rules are configured identically to authorization policy rules. For information about authorization policies, see Configure Authorization Policies, on page 993.

Note Cisco ISE does not support the use of % character in the authorization policies to avoid security issues.

Local and Global Exceptions Configuration Settings

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Policy Sets** for network access policies. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Device Admin Policy Sets** for device administration policies. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy Sets** > **View** > **Local Exceptions Policy** or **Global Exceptions Policy**.

Authorization exception settings are identical to the Authorization policy settings and are as described in Authorization Policy Settings, on page 995.

Policy Conditions

Cisco ISE uses rule-based policies to provide network access. A policy is a set of rules and results, where the rules are made up of conditions. Cisco ISE allows you to create conditions as individual policy elements that can be stored in the system library and then reused for other rule-based policies from the Conditions Studio.

Conditions can be as simple or complex as necessary using an operator (equal to, not equal to, greater than, and so on), and a value, or by including multiple attributes, operators and complex hierarchies. At runtime, Cisco ISE evaluates a policy condition and then applies the result that you have defined based on whether the policy evaluation returns a true or a false value.

After you create a condition and assign it a unique name, you can reuse this condition multiple times across various rules and policies by selecting it from the Conditions Studio Library, for example:

```
Network Conditions.MyNetworkCondition EQUALS true
```

You cannot delete conditions from the Condition Studio that are used in a policy or are part of another condition.

Each condition defines a list of objects that can be included in policy conditions, resulting in a set of definitions that are matched against those presented in the request.

You can use the operator, `EQUALS true`, to check if the network condition evaluates to true (whether the value presented in the request matches at least one entry within the network condition) or `EQUALS false` to test whether the network condition evaluates to false (does not match any entry in the network condition).

Cisco ISE also offers predefined smart conditions that you can use in your policies separately or as building blocks in your own customized conditions, and which you can update and change based on your needs.

You can create the following unique network conditions to restrict access to the network:

- Endstation Network Conditions—Based on endstations that initiate and terminate the connection.

  Cisco ISE evaluates the remote address TO field (which is obtained based on whether it is a TACACS+ or RADIUS request) to identity whether it is the IP address, MAC address, calling line identification (CLI), or dialed number identification service (DNIS) of the endpoint.

  In a RADIUS request, this identifier is available in Attribute 31 (Calling-Station-Id).

  In a TACACS+ request, if the remote address includes a slash (/), the part before the slash is taken as the FROM value and the part after the slash is taken as the TO value. For example, if a request has CLI/DNIS, CLI is taken as the FROM value and DNIS is taken as the TO value. If a slash is not included, the entire remote address is taken as the FROM value (whether IP address, MAC address, or CLI).

- Device Network Conditions—Based on the AAA client that processes the request.

  A network device can be identified by its IP address, device name that is defined in the network device repository, or Network Device Group.

  In a RADIUS request, if Attribute 4 (NAS-IP-Address) is present, Cisco ISE obtains the IP address from this attribute. If Attribute 32 (NAS-Identifier) is present, Cisco ISE obtains the IP address from Attribute 32. If these attributes are not found, it obtains the IP address from the packet that it receives.

  The device dictionary (NDG dictionary) contains network device group attributes such as Location, Device Type, or other dynamically created attributes that represent NDGs. These attributes contain the groups that the current device is related to.

- Device Port Network Conditions—Based on the device's IP address, name, NDG, and port (physical port of the device that the endstation is connected to).

  In a RADIUS request, if Attribute 5 (NAS-Port) is present in the request, Cisco ISE obtains the value from this attribute. If Attribute 87 (NAS-Port-Id) is present in the request, Cisco ISE obtains the request from Attribute 87.

  In a TACACS+ request, Cisco ISE obtains this identifier from the port field of the start request (of every phase).

For more information about these unique conditions, see Special Network Access Conditions , on page 1020.

Dictionaries and Dictionary Attributes

Dictionaries are domain-specific catalogs of attributes and allowed values that can be used to define access policies for a domain. An individual dictionary is a homogeneous collection of attribute type. Attributes that are defined in a dictionary have the same attribute type and the type indicates the source or context of a given attribute.

Attribute types can be one of the following:

- MSG_ATTR

- ENTITY_ATTR
- PIP_ATTR

In addition to attributes and allowed values, a dictionary contains information about the attributes such as the name and description, data type, and the default values. An attribute can have one of the following data types: BOOLEAN, FLOAT, INTEGER, IPv4, IPv6, OCTET_STRING, STRING, UNIT32, and UNIT64.

Cisco ISE creates system dictionaries during installation and allows you to create user dictionaries.

Attributes are stored in different system dictionaries. Attributes are used to configure conditions. Attributes can be reused in multiple conditions.

To reuse a valid attribute when creating policy conditions, select it from a dictionary that contains the supported attributes. For example, Cisco ISE provides an attribute named AuthenticationIdentityStore, which is located in the NetworkAccess dictionary. This attribute identifies the last identity source that was accessed during the authentication of a user:

- When a single identity source is used during authentication, this attribute includes the name of the identity store in which the authentication succeeded.
- When an identity source sequence is used during authentication, this attribute includes the name of the last identity source accessed.

You can use the AuthenticationStatus attribute in combination with the AuthenticationIdentityStore attribute to define a condition that identifies the identity source to which a user has successfully been authenticated. For example, to check for a condition where a user authenticated using an LDAP directory (LDAP13) in the authorization policy, you can define the following reusable condition:

```
If NetworkAccess.AuthenticationStatus EQUALS AuthenticationPassed AND
NetworkAccess.AuthenticationIdentityStore EQUALS LDAP13
```

Note The AuthenticationIdentityStore represents a text field that allows you to enter data for the condition. Ensure that you enter or copy the name correctly into this field. If the name of the identity source changes, you must ensure to modify this condition to match the change to the identity source.

To define conditions that are based on an endpoint identity group that has been previously authenticated, Cisco ISE supports authorization that was defined during endpoint identity group 802.1X authentication status. When Cisco ISE performs 802.1X authentication, it extracts the MAC address from the “Calling-Station-ID” field in the RADIUS request and uses this value to look up and populate the session cache for the device's endpoint identity group (defined as an endpointIDgroup attribute). This process makes the endpointIDgroup attribute available for use in creating authorization policy conditions, and allows you to define an authorization policy based on endpoint identity group information using this attribute, in addition to user information.

The condition for the endpoint identity group can be defined in the ID Groups column of the authorization policy configuration page. Conditions that are based on user-related information need to be defined in the “Other Conditions” section of the authorization policy. If user information is based on internal user attributes, then use the ID Group attribute in the internal user dictionary. For example, you can enter the full value path in the identity group using a value like “User Identity Group:Employee:US”.

Supported Dictionaries for Network Access Policies

Cisco ISE supports the following system-stored dictionaries that contain the different attributes necessary when building conditions and rules for your authentication and authorization policies:

- System-defined dictionaries
    - CERTIFICATE
    - DEVICE
    - RADIUS
- RADIUS vendor dictionaries
    - Airespace
    - Cisco
    - Cisco-BBSM
    - Cisco-VPN3000
    - Microsoft
    - Network access

For authorization policy types, the verification configured in the condition must comply with the authorization profiles to be returned.

Verifications typically include one or more conditions that include a user-defined name that can then be added to a library and reused by other policies.

The following sections describe the supported attributes and dictionaries available for configuring conditions.

Attributes Supported by Dictionaries

The table lists the fixed attributes that are supported by dictionaries, which can be used in policy conditions. Not all of these attributes are available for creating all types of conditions.

For example, while creating a condition to choose the access service in authentication policies, you will only see the following network access attributes: Device IP Address, ISE Host Name, Network Device Name, Protocol, and Use Case.

You can use the attributes listed in the following table in policy conditions.

Dictionary	Attributes	Allowed Protocol Rules and Proxy	Identity Rules
Device	Device Type (predefined network device group)	Yes	Yes
	Device Location (predefined network device group)		
	Other Custom Network Device Group		
	Software Version		
	Model Name		

Dictionary	Attributes	Allowed Protocol Rules and Proxy	Identity Rules
RADIUS	All attributes	Yes	Yes
Network Access	ISE Host Name	Yes	Yes
	AuthenticationMethod	No	Yes
	AuthenticationStatus	No	No
	CTSDeviceID	No	No
	Device IP Address	Yes	Yes
	EapAuthentication (the EAP method that is used during authentication of a user of a machine)	No	Yes
	EapTunnel (the EAP method that is used for tunnel establishment)	No	Yes
	Protocol	Yes	Yes
	UseCase	Yes	Yes
	UserName	No	Yes
	WasMachineAuthenticated	No	No

Dictionary	Attributes	Allowed Protocol Rules and Proxy	Identity Rules
Certificate	Common Name	No	Yes
	Country		
	E-mail		
	LocationSubject		
	Organization		
	Organization Unit		
	Serial Number		
	State or Province		
	Subject		
	Subject Alternative Name		
	Subject Alternative Name - DNS		
	Subject Alternative Name - E-mail		
	Subject Alternative Name - Other Name		
	Subject Serial Number		
	Issuer		
	Issuer - Common Name		
	Issuer - Organization		
	Issuer - Organization Unit		
	Issuer - Location		
	Issuer - Country		
	Issuer - Email		
	Issuer - Serial Number		
	Issuer - State or Province		
	Issuer - Street Address		
	Issuer - Domain Component		
	Issuer - User ID		

System Defined Dictionaries and Dictionary Attributes

Cisco ISE creates system dictionaries during installation that you can find in the System Dictionaries page. System-defined dictionary attributes are read-only attributes. Because of their nature, you can only view existing system-defined dictionaries. You cannot create, edit, or delete system-defined values or any attributes in a system dictionary.

A system-defined dictionary attribute is displayed with the descriptive name of the attribute, an internal name as understood by the domain, and allowed values.

Cisco ISE also creates dictionary defaults for the IETF RADIUS set of attributes that are also a part of the system-defined dictionaries, which are defined by the Internet Engineering Task Force (IETF). You can edit all free IETF RADIUS attribute fields except the ID.

Display System Dictionaries and Dictionary Attributes

You cannot create, edit, or delete any system-defined attribute in a system dictionary. You can only view system-defined attributes. You can perform a quick search that is based on a dictionary name and description or an advanced search that is based on a search rule that you define.

Step 1

Step 2 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Dictionaries** > **System**.

Step 3 Choose a system dictionary in the System Dictionaries page, and click **View**.

Step 4 Click **Dictionary Attributes**.

Step 5 Choose a system dictionary attribute from the list, and click **View**.

Step 6 Click the **Dictionaries** link to return to the System Dictionaries page.

User-Defined Dictionaries and Dictionary Attributes

Cisco ISE displays the user-defined dictionaries that you create in the User Dictionaries page. You cannot modify the values for Dictionary Name or Dictionary Type for an existing user dictionary once created and saved in the system.

You can do the following in the User Dictionaries page:

- Edit and delete user dictionaries.
- Search user dictionaries based on name and description.
- Add, edit, and delete user-defined dictionary attributes in the user dictionaries.
- Delete attributes of the NMAP extension dictionary, using the NMAP scan action. When custom ports are added or deleted in the NMAP Scan Actions page, the corresponding custom ports attributes are added, deleted, or updated in the dictionary.
- Add or remove allowed values for dictionary attributes.

Create User-Defined Dictionaries

You can create, edit, or delete user-defined dictionaries.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Dictionaries** > **User**

Step 2 Click **Add**.

Step 3 Enter the name for the user dictionary, an optional description, and a version for the user dictionary.

Step 4 Choose the attribute type from the Dictionary Attribute Type drop-down list.

Step 5 Click **Submit**.

Create User-Defined Dictionary Attributes

You can add, edit, and delete user-defined dictionary attributes in user dictionaries as well as add or remove allowed values for the dictionary attributes.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Dictionaries** > **User**

Step 2 Choose a user dictionary from the User Dictionaries page, and click **Edit**.

Step 3 Click **Dictionary Attributes**.

Step 4 Click **Add**.

Step 5 Enter the name for an attribute name, an optional description, and an internal name for the dictionary attribute.

Step 6 Choose a data type from the Data Type drop-down list.

Step 7 Click **Add** to configure the name, allowed value, and set the default status in the Allowed Values table.

Step 8 Click **Submit**.

RADIUS-Vendor Dictionaries

Cisco ISE allows you to define a set of RADIUS-vendor dictionaries, and define a set of attributes for each one. Each vendor definition in the list contains the vendor name, the vendor ID, and a brief description.

Cisco ISE provides you the following RADIUS-vendor dictionaries by default:

- Airespace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft

The RADIUS protocol supports these vendor dictionaries, and the vendor-specific attributes that can be used in authorization profiles and in policy conditions.

Create RADIUS-Vendor Dictionaries

You can also create, edit, delete, export, and import RADIUS-vendor dictionaries.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Dictionaries** > **System** > **Radius** > **Radius Vendors**.

Step 2 Click **Add**.

Step 3 Enter a name for the RADIUS-vendor dictionary, an optional description, and the vendor ID as approved by the Internet Assigned Numbers Authority (IANA) for the RADIUS vendor. The vendor ID must be unique across the global IANA vendor list and cannot be in use by any existing vendor.

Step 4 Choose the number of bytes taken from the attribute value to specify the attribute type from the Vendor Attribute Type Field Length drop- down list. Valid values are 1, 2, and 4. The default value is 1.

Step 5 Choose the number of bytes taken from the attribute value to specify the attribute length from the Vendor Attribute Size Field Length drop-down list. Valid values are 0 and 1. The default value is 1.

Step 6 Click **Submit**.

Create RADIUS-Vendor Dictionary Attributes

You can create, edit, and delete RADIUS vendor attributes that Cisco ISE supports. Each RADIUS-vendor attribute has a name, data type, description, and direction, which specifies whether it is relevant to requests only, responses only, or both.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Dictionaries** > **System** > **Radius** > **Radius Vendors.**

Step 2 Choose a RADIUS-vendor dictionary from the RADIUS vendor dictionaries list, and click **Edit**.

Step 3 Click **Dictionary Attributes**, and then click **Add**.

Step 4 Enter the attribute name for the RADIUS vendor attribute and an optional description.

Step 5 Choose the data type from the Data Type drop-down list.

Step 6 Check the **Enable MAC option** check box.

Step 7 Choose the direction that applies to RADIUS requests only, RADIUS responses only, or both from the Direction drop-down list.

Step 8 Enter the vendor attribute ID in the ID field.

Step 9 Check the **Allow Tagging** check box.

Step 10 Check the **Allow multiple instances of this attribute in a profile** check box.

Step 11 Click **Add** to add the allowed value for the vendor attribute in the Allowed Values table.

Step 12 Click **Submit**.

HP RADIUS IETF Service Type Attributes

Cisco ISE introduces two new values for the RADIUS IETF Service Type attribute. The RADIUS IETF service type attribute is available in **Policy** > **Policy Elements** > **Dictionaries** > **System** > **RADIUS** > **IETF**In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Dictionaries** > **System**

> RADIUS > IETF. You can use these two values in policy conditions. These two values are specifically designed for HP devices to understand permissions of the user.

Enumeration Name	Enumeration Value
HP-Oper	252
HP-User	255

RADIUS Vendor Dictionary Attribute Settings

This section describes RADIUS vendor dictionaries used in Cisco ISE.

The following table describes the fields in the Dictionary window for RADIUS vendors, which allows you to configure dictionary attributes for the RADIUS vendors. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Dictionaries** > **System** > **RADIUS** > **RADIUS Vendors**.

Table 145: RADIUS Vendor Dictionary Attribute Settings

Field Name	Usage Guidelines
Attribute Name	Enter the vendor specific attribute name for the selected RADIUS vendor.
Description	Enter an optional description for the vendor specific attribute.
Internal Name	Enter the name for the vendor specific attribute that refers to it internally in the database.
Data Type	Choose one of the following data types for the vendor specific attribute: • STRING • OCTET_STRING • UNIT32 • UNIT64 • IPV4 • IPV6

Field Name	Usage Guidelines
Enable MAC option	Check this check box to enable the comparison of RADIUS attribute as MAC address. By default, for the RADIUS attribute calling-station-id this option is marked as enabled and you cannot disable it. For other dictionary attributes (of string types) within the RADIUS vendor dictionary, you can enable or disable this option. Once you enable this option, while setting the authentication and authorization conditions, you can define whether the comparison is clear string by selecting the Text option or whether it is MAC address by selecting the MAC address option.
Direction	Choose one of the options that applies to RADIUS messages:
ID	Enter the vendor attribute ID. The valid range is 0 to 255.
Allow Tagging	Check this check box to mark the attribute as being permitted to have a tag, as defined in RFC2868. The purpose of the tag is to allow grouping of attributes for tunnelled users. See RFC2868 for more details. The tagged attributes support ensures that all attributes pertaining to a given tunnel contain the same value in their respective tag fields, and that each set includes an appropriately-valued instance of the Tunnel-Preference attribute. This conforms to the tunnel attributes that are to be used in a multi-vendor network environment, thereby eliminating interoperability issues among Network Access Servers (NASs) manufactured by different vendors.
Allow Multiple Instances of this Attribute in a Profile	Check this check box when you want multiple instances of this RADIUS vendor specific attribute in profiles.

Related Topics

System Defined Dictionaries and Dictionary Attributes, on page 1007

User-Defined Dictionaries and Dictionary Attributes, on page 1007

RADIUS-Vendor Dictionaries, on page 1008

Create RADIUS-Vendor Dictionaries, on page 1009

Navigate the Conditions Studio

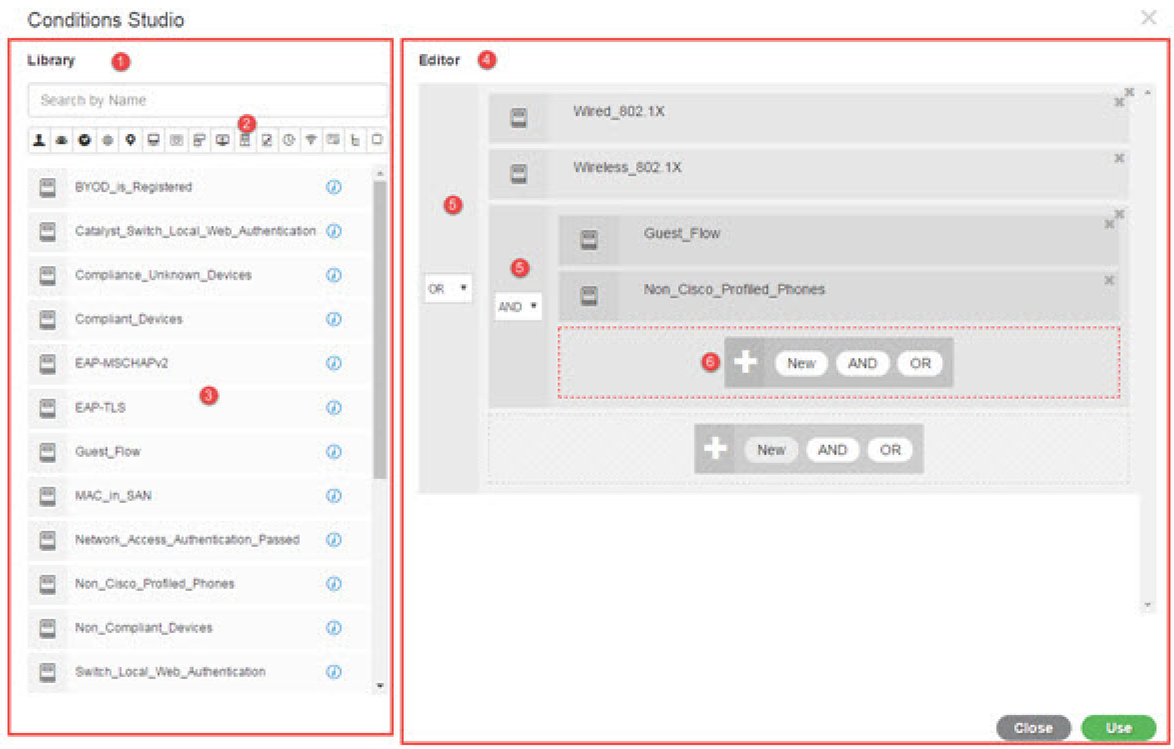
Use the Conditions Studio to create, manage and re-use conditions. Conditions can include more than one rule, and can be built with any complexity including only one level, or multiple hierarchical levels. When using the Conditions Studio to create new conditions, you can use the condition blocks that you have already stored in the Library and you can also update and change those stored condition blocks. While creating and managing conditions later, easily find the blocks and attributes that you need by using quick category filters, and more.

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Policy Sets** for network access policies. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Device Admin Policy Sets** for device administration policies.

To edit or change conditions that have already been applied to the specific rule in any of your policy sets, hover over the cell in the **Conditions** column and click ✎, or click the plus sign ✚ from the **Conditions** column in the Policy Set table in order to create a new condition, which you can then immediately apply to the same policy set or alternatively you can also save in the Library for future use.

The following figure shows the main elements of the Conditions Studio.

Figure 42: Conditions Studio


Conditions Studio
Library
1
Search by Name
2
BYOD_is_Registered
Catalyst_Switch_Local_Web_Authentication
Compliance_Unknown_Devices
Compliant_Devices
EAP-MSCHAPv2
EAP-TLS
3
Guest_Flow
MAC_in_SAN
Network_Access_Authentication_Passed
Non_Cisco_Profiled_Phones
Non_Compliant_Devices
Switch_Local_Web_Authentication
Editor
4
Wired_802.1X
Wireless_802.1X
5
OR
5
AND
Guest_Flow
Non_Cisco_Profiled_Phones
6
New
AND
OR
New
AND
OR
Close
Use

The Condition Studio is divided into two main parts: the Library and the Editor. The Library stores condition blocks for reuse while the Editor enables you to edit those saved blocks and create new ones.

The following table describes the different parts of the Conditions Studio:

Fields	**Usage Guidelines**
Library	Displays the list of all condition blocks that were created and saved in the ISE database for reuse. To use these condition blocks as part of your currently edited condition, drag and drop them from the Library to the relevant level in the Editor and update the operators as necessary. Conditions stored in the Library are all represented by the Library icon 📖, because conditions can be associated with more than one category. Next to each condition in the Library you can also find the i icon. Hover over this icon to view a full description of the condition, view the categories to which it is associated, and to delete the condition from the library entirely. You cannot delete conditions if they are used by policies. Drag and drop any of the Library conditions into the Editor in order to use it for the currently edited policy on its own or as a building block for a more complex condition to be used in the current policy or saved as a new condition in the Library. You can also drag and drop the condition in the Editor in order to make changes to that condition and then save it under the same or a new name in the Library. There are also predefined conditions upon installation. These conditions can also be changed and deleted.
Search and filter	Search conditions by name or filter them by category. In a similar manner, you can also search and filter attributes from the **Click to add an attribute** field in the Editor. The icons on the toolbar represent different attribute categories such as subject, address and so forth. Click an icon to view attributes related to the specific category and click a highlighted icon from the category toolbar in order to deselect it, thereby removing the filter.
Conditions List	The complete list of all conditions in the Library, or the list of conditions in the Library based on the search or filter results.

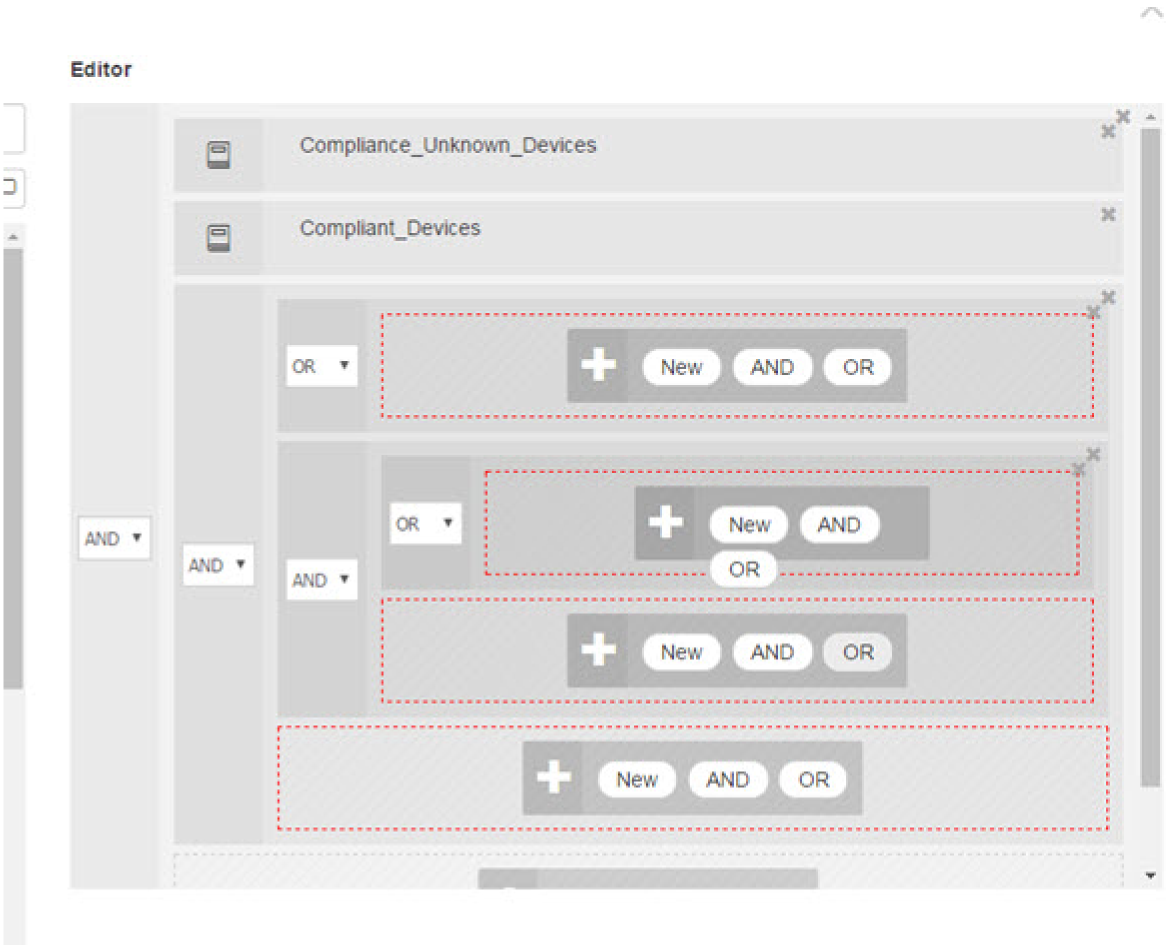
Fields	Usage Guidelines
Editor	Create new conditions to use immediately as well as to save them in the system Library for future use, and edit existing conditions and save those changes in the Library for immediate and future use. When opening the Conditions Studio in order to create a new condition (click the plus sign from any of the policy set tables), the Editor appears with only a single, empty, line to which you can add your first rule. When the Editor opens with empty fields, no operator icons appear
	The Editor is divided into different virtual columns and rows. Columns represent different hierarchical levels, and each column is indented based on its position in the hierarchy; rows represent individual rules. You can create single or multiple rules per level, and you can include multiple levels. The example in the image above displays a condition that is in the process of being built or edited and includes a hierarchy of rules, where both the first and second levels in the figure are marked with the number 5. The rules on the top parent level use the operator OR. In order to change the operator once you have selected it and created the hierarchical level, simply select the relevant option from the dropdown list that appears in this column. In addition to the operator dropdown list, each rule has a relevant icon in this column, indicating what category it belongs to. If you hover over the icon, a tooltip indicates the name of the category. Once saved to the library, all condition blocks are assigned the Library icon, replacing the category icons that appeared in the Editor. Finally, if a rule is configured to **exclude** all relevant matched items, then the Is-Not indicator also appears in this column. For example, if a location attribute with the value London is set to Is-Not then all devices from London will be denied access.

Fields	Usage Guidelines
	This area displays the options available when working with hierarchical levels as well as multiple rules within a condition. When you hover over any column or row the relevant actions appear. When you select an action, it is applied to that section and all of the children sections. For example, with five levels in Hierarchy A, if you choose AND from any rule in the third level, then a new hierarchy, Hierarchy B, is created under the original rule so that the original rule becomes the parent rule for Hierarchy B, which is embedded in Hierarchy A. When you first open the Condition Studio in order to create a new condition from scratch, the Editor area includes only one line for a single rule that you can configure, as well as the option to select relevant operators or to drag and drop relevant conditions from the Library. Additional levels can be added to the condition with the **AND** and **OR** operator options. Choose **New** to create a new rule on the same level from which you clicked the option. The **New** option only appears once you have configured at least one rule on the top level of the hieararchy.

Configure, Edit and Manage Policy Conditions

Use the Conditions Studio to create, manage and re-use conditions. Conditions can include more than one rule, and can be built with any complexity including only one level, or multiple hierarchical levels. Manage the condition hierarchy from the Editor side of the Conditions Studio as in the following image:

Figure 43: Editor—Conditions Hierarchy



When creating new conditions, you can use the condition blocks that you have already stored in the Library and you can also update and change those stored condition blocks. While creating and managing conditions, easily find the blocks and attributes that you need by using quick category filters, and more.

When creating and managing condition rules, use attributes, operators and values.

Cisco ISE also includes predefined condition blocks for some of the most common use cases. You can edit these predefined conditions to suit your requirements. Conditions saved for re-use, including the out-of-the-box blocks, are stored in the Library of the Condition Studio, as described in this task.

To perform the following task, you must be a Super Admin or Policy Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Sets**

Step 2 Access the Conditions Studio to create a new condition and to edit existing condition blocks, in order to then use those conditions as part of the rules you configure for the specific policy set (and its associated policies and rules), or in order to save to the Library for future use:

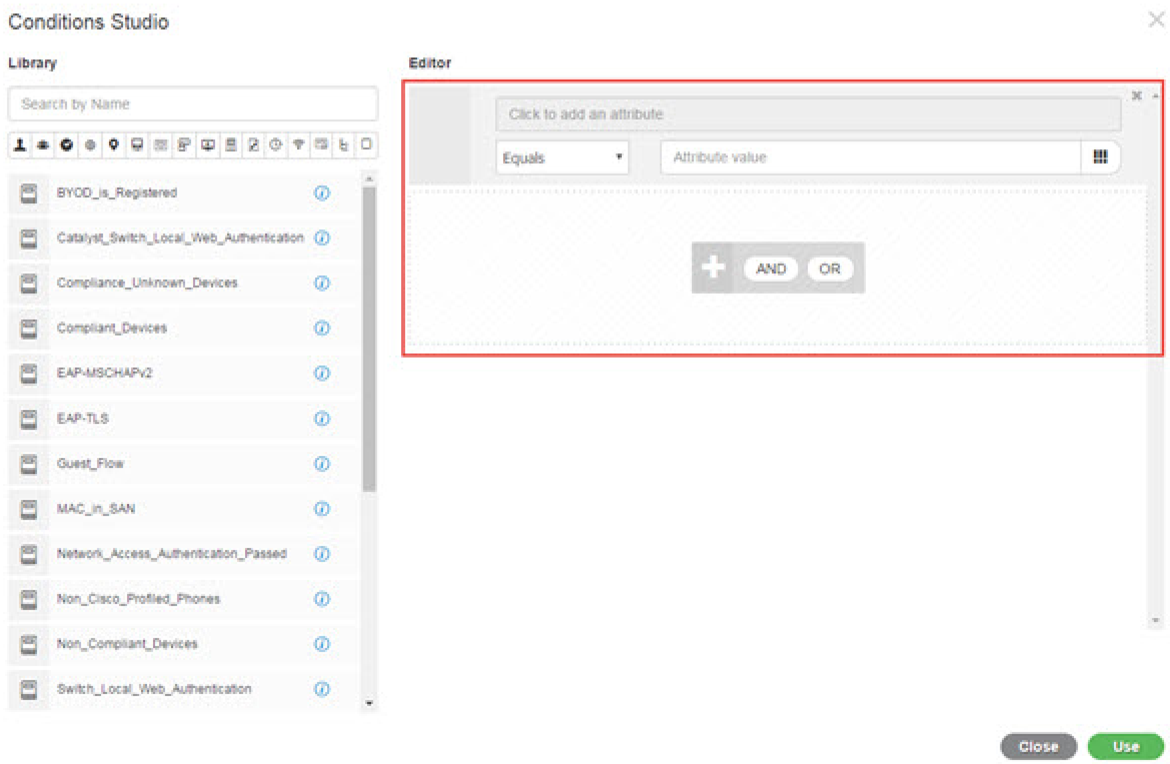
a) Click ✚ from the **Conditions** column in the Policy Set table on the main Policy Set page in order to create conditions that are relevant for the entire policy set (conditions that are checked prior to matching authentication policy rules).

b) Alternatively, click › from a specific policy set row in order to view the Set view, including all rules for authentication and authorization. From the Set view, hover over the cell in the **Conditions** column from any of the rule tables and click + to open the Conditions Studio.

c) If you are editing conditions that have already been applied to the policy set, then click ✎ to access the Conditions Studio.

The Conditions Studio opens. If you have opened it in order to create new conditions, then it appears as in the following image. For a description of the fields and to see an example of the Conditions Studio when you have opened it to edit conditions that were already applied to the policy set, see Navigate the Conditions Studio, on page 1011.

Figure 44: Conditions Studio—Creating a New Condition


Conditions Studio
Library
Editor
Search by Name
BYOD_is_Registered
Catalyst_Switch_Local_Web_Authentication
Compliance_Unknown_Devices
Compliant_Devices
EAP-MSCHAPv2
EAP-TLS
Guest_Flow
MAC_in_SAN
Network_Access_Authentication_Passed
Non_Cisco_Profiled_Phones
Non_Compliant_Devices
Switch_Local_Web_Authentication
Click to add an attribute
Equals
Attribute value
AND
OR
Close
Use

Step 3 Use an existing condition block from the Library as a rule in the condition that you are creating or editing.

a) Filter by selecting the relevant category from the category toolbar—in the Library, all blocks that contain an attribute from the selected category are displayed. Condition blocks that contain more than one rule but that use an attribute from the selected category for at least one of those rules, are also displayed. If there are additional filters added, then the results displayed include only condition blocks from the specific filter that also match the other filters that were included. For example, if you select the Ports category from the toolbar and you also enter "auth" as free text in the **Search by Name** field, then all blocks related to ports with "auth" in their names are displayed. Click the highlighted icon again from the category toolbar in order to deselect it, thereby removing that filter.

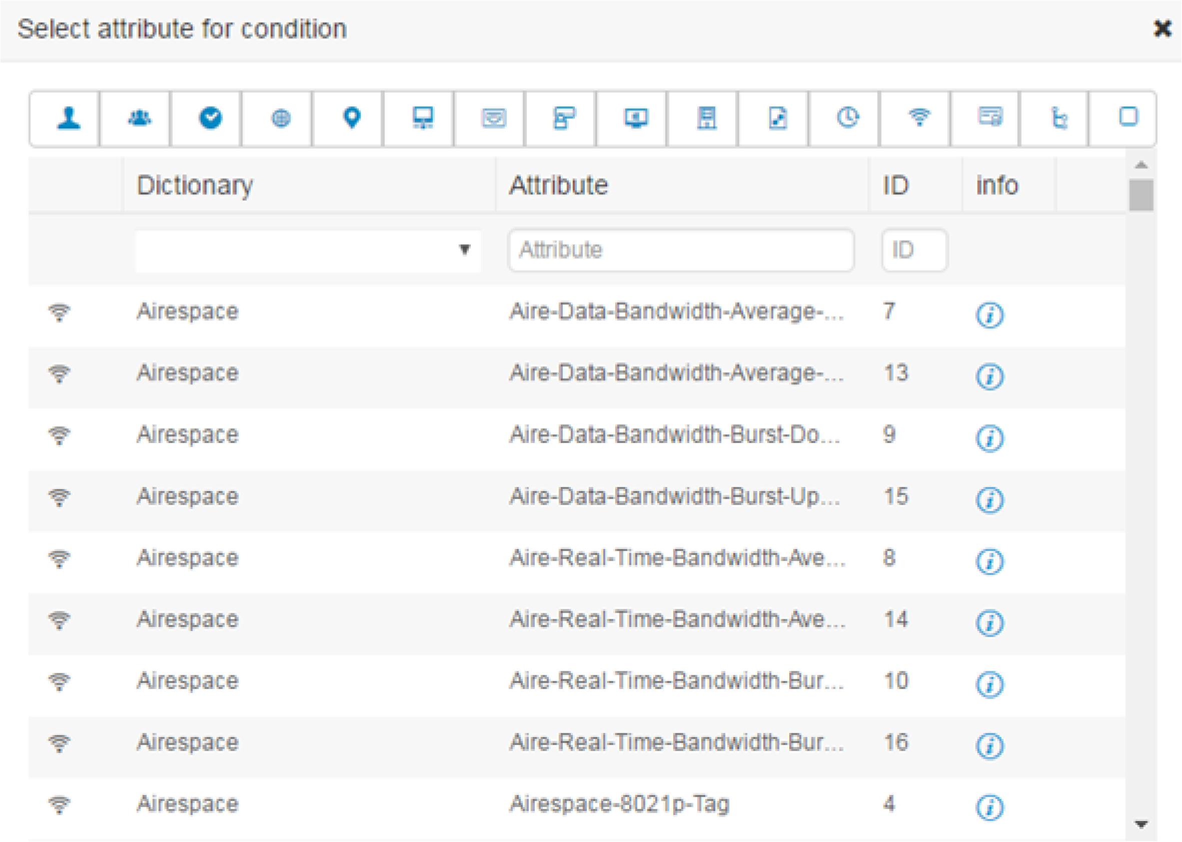
b) Search for condition blocks with free text—in the **Search by Name** free text field, enter any term, or part of a term, that appears in the name of the block for which you are searching. As you type, the system dynamically searches for relevant results in real time. If no category is selected (none of the icons are highlighted) then the results include condition blocks from all categories. If a category icon is already selected (the displayed list is already filtered), then the results displayed include only blocks in the specific category that use the specific text.

c) Once you find the condition block, drag it to the Editor and drop it in the correct level of the block that you are building. If you drop it in the incorrect location, you can drag and drop it again from within the Editor, until it is placed correctly.

d) Hover over the block from the Editor and click **Edit** to change the rule, in order make changes relevant for the condition you are working on, to overwrite the rule in the Library with those changes or alternatively to save the rule as a new block in the Library.
The block, which is read-only when dropped into the Editor can now be edited and has the same fields, structures, lists and actions as all other customized rules in the Editor. Continue to the next steps for more information in editing this rule.

Step 4 Add an operator to the current level in order to then add additional rules on the same level—choose **AND**, **OR** or **Set to 'Is not'**. **Set to 'Is not'** can also be applied to individual rules.

Step 5 Create and edit rules using the attribute dictionaries—click in the **Click to add an attribute** field. The Attribute Selector opens as in the following image:


Select attribute for condition

Dictionary	Attribute	ID	info
Airespace	Aire-Data-Bandwidth-Average-...	7	ⓘ
Airespace	Aire-Data-Bandwidth-Average-...	13	ⓘ
Airespace	Aire-Data-Bandwidth-Burst-Do...	9	ⓘ
Airespace	Aire-Data-Bandwidth-Burst-Up...	15	ⓘ
Airespace	Aire-Real-Time-Bandwidth-Ave...	8	ⓘ
Airespace	Aire-Real-Time-Bandwidth-Ave...	14	ⓘ
Airespace	Aire-Real-Time-Bandwidth-Bur...	10	ⓘ
Airespace	Aire-Real-Time-Bandwidth-Bur...	16	ⓘ
Airespace	Airespace-8021p-Tag	4	ⓘ

The parts of the Attribute Selector are as described in the following table:

Fields	Usage Guidelines
Attribute Category toolbar	Contains a unique icon for each of the different attribute categories. Choose any attribute category icon to filter the view by category. Click a highlighted icon in order to deselect it, thereby removing the filter.

Fields	Usage Guidelines
Dictionary	Indicates the name of the dictionary in which the attribute is stored. Select a specific dictionary from the dropdown in order to filter attributes by vendor dictionary.
Attribute	Indicates the name of the attribute. Filter attributes by typing free text for the attribute name in the available field. As you type, the system dynamically searches for relevant results in real time.
ID	Indicates the unique attribute identification number. Filter attributes by typing the ID number in the available field. As you type, the system dynamically searches for relevant results in real time.
Info	Hover the information icon on the relevant attribute row to view extra details about the attribute.

a) From the Attribute Selector search, filter and search for the attribute you need. When you filter or enter free text in any part of the Attribute Selector, if there are no other filters activated, then the results include all attributes relevant for the selected filter only. If more than one filter is used, then the search results that are displayed match all filters. For example, if you click the Port icon from the toolbar and type "auth" in the Attribute column, then only attributes from the Port category that have "auth" in their name are displayed. When you choose a category, the icon in the toolbar is highlighted in blue and the filtered list is displayed. Click the highlighted icon again from the category toolbar in order to deselect it, thereby removing the filter.

b) Choose the relevant attribute in order to add it to the rule.
The Attribute Selector closes and the attribute you selected is added to the **Click to add an attribute** field.

c) From the **Equals** dropdown list, select the relevant operator.

Not all attributes you select will include the “Equals,” “Not Equals,” “Matches,” “Starts With,” or “Not Starts With” operator options.

The “Matches” operator supports and uses regular expressions (REGEX) not wildcards.

You must use the “equals” operator for straight forward comparison. “Contains” operator can be used for multi-value attributes. “Matches” operator should be used for regular expression comparison. When “Matches” operator is used, regular expression will be interpreted for both static and dynamic values.

d) From the **Attribute value** field do one of the following:

- Type a free text value in the field
- Select a value from the list that dynamically loads (when relevant—depending on the attribute selected in the previous step)
- Use another attribute as the value for the condition rule—choose the table icon next to the field in order to open the Attribute Selector and then search, filter and select the relevant attribute. The Attribute Selector closes and the attribute you selected is added to the **Attribute value** field.

Step 6 Save rules in the Library as a condition block.

a) Hover over the rule or hierarchy of rules that you would like to save as a block in the Library. The **Duplicate** and **Save** buttons appear for any rule or group of rules that can be saved as a single condition block. If you would like to save a group of rules as a block, choose the action button from the bottom of the entire hierarchy in the blocked area for the entire hierarchy.

b) Click **Save**. The Save condition screen pops up.

c) Choose:

- Save to Existing Library Condition—choose this option to overwrite an existing condition block in the Library with the new rule you have created and then select the condition block that you want to overwrite from the **Select from list** dropdown list.
- Save as a new Library Condition—type a unique name in the Condition Name field for the block.

d) Optionally, enter a description in the **Description** field. This description appears when you hover over the info icon for any condition block from within the Library, enabling you to quickly identify the different condition blocks and their uses.

e) Click **Save** to save the condition block in the Library.

Step 7 To create a new rule on a new child level—click **AND** or **OR** to apply the correct operator between the existing parent hierarchy and the child hierarchy that you are creating. A new section is added to the Editor hierarchy with the selected operator, as a child of the rule or hierarchy from which you chose the operator.

Step 8 To create a new rule on a a current existing level—click **New** from the relevant level. A new empty row appears for a new rule in the same level as the level from which you began.

Step 9 Click **X** to remove any condition from the Editor and all of its children.

Step 10 Click **Duplicate** to automatically copy and paste the specific condition within the hierarchy, thereby creating additional identical children at the same level. You can duplicate individual rules with or without their children, depending on the level from which you click the **Duplicate** button.

Step 11 Click **Use** from the bottom of the page to save the condition you created in the Editor and to implement that condition in your policy set.

Note When an AD attribute is needed in any policy set, the corresponding AD condition must be configured.

Special Network Access Conditions

This section describes unique conditions that can be useful when creating your policy sets. These conditions cannot be created from the Conditions Studio and so have their own unique processes.

Configure Device Network Conditions

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Network Conditions** > **Device Network Conditions**

Step 2 Click **Add**.

Step 3 Enter a name and description for the network condition.

Step 4 Enter the following details:

- IP Addresses—You can add a list of IP addresses or subnets, one per line. The IP address/subnet can be in IPv4 or IPv6 format.

- Device Name—You can add a list of device names, one per line. You must enter the same device name that is configured in the Network Device object.
- Device Groups—You can add a list of tuples in the following order: Root NDG, comma, and an NDG (that it under the root NDG). There must be one tuple per line.

Step 5 Click **Submit**.

Configure Device Port Network Condition

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Network Conditions** > **Device Port Network Conditions**

Step 2 Click **Add**.

Step 3 Enter a name and description for the network condition.

Step 4 Enter the following details:

- IP Addresses—Enter the details in the following order: IP address or subnet, comma, and a port (that is used by the device). There must be one tuple per line.
- Devices— Enter the details in the following order: device name, comma, and a port. There must be one tuple per line. You must enter the same device name that is configured in the Network Device object.
- Device Groups— Enter the details in the following order: Root NDG, comma, NDG (that it under the root), and a port. There must be one tuple per line.

Step 5 Click **Submit**.

Configure Endstation Network Conditions

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Network Conditions** > **Endstation Network Conditions**

Step 2 Click **Add**.

Step 3 Enter a name and description for the network condition.

Step 4 Enter the following details:

- IP Addresses—You can add a list of IP addresses or subnets, one per line. The IP address/subnet can be in IPv4 or IPv6 format.
- MAC Addresses—You can enter a list of Endstation MAC addresses and Destination MAC addresses, separated by a comma. Each MAC address must include 12 hexadecimal digits and must be in one of the following formats: nn:nn:nn:nn:nn:nn, nn-nn-nn-nn-nn-nn, nnnn.nnnn.nnnn, or nnnnnnnnnnnn.

  If the Endstation MAC or the Destination MAC is not required, use the token "-ANY-" instead.

- CLI/DNIS—You can add a list of Caller IDs (CLI) and Called IDs (DNIS), separated by a comma. If the Caller ID (CLI) or the Called ID (DNIS) is not required, use the token "-ANY-" instead.

Step 5 Click **Submit**.

Create Time and Date Conditions

Use the Policy Elements Conditions page to display, create, modify, delete, duplicate, and search time and date policy element conditions. Policy elements are shared objects that define a condition that is based on specific time and date attribute settings that you configure.

Time and date conditions let you set or limit permission to access Cisco ISE system resources to specific times and days as directed by the attribute settings you make.

Before you begin

To perform the following task, you must be a Super Admin or Policy Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Common** > **Time and Date** > **Add**

Step 2 Enter appropriate values in the fields.

- In the Standard Settings area, specify the time and date to provide access.
- In the Exceptions area, specify the time and date range to limit access.

Step 3 Click **Submit**.

Use IPv6 Condition Attributes in Authorization Policies

Cisco ISE can detect, manage, and secure IPv6 traffic from endpoints.

When an IPv6-enabled endpoint connects to the Cisco ISE network, it communicates with the Network Access Device (NAD) over an IPv6 network. The NAD conveys the accounting and profiling information from the endpoint (including IPv6 values) to Cisco ISE over an IPv4 network. You can configure authorization profiles and policies in Cisco ISE using the IPv6 attributes in your rule conditions to process such requests from IPv6-enabled endpoints and ensure that the endpoint is compliant.

You can use wildcard characters in IPv6 prefix and IPv6 interface values. For example: 2001:db8:1234::/48.

Supported IPv6 address formats include:

- Full notation: Eight groups of four hexadecimal digits separated by colons. For example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- Shortened notation: Exclude leading zeros in a group; replace groups of zeros with two consecutive colons. For example: 2001:db8:85a3::8a2e:370:7334
- Dotted-quad notation (IPv4-mapped and IPv4 compatible-IPv6 addresses): For example, ::ffff:192.0.2.128

Supported IPv6 attributes include:

- NAS-IPv6-Address
- Framed-Interface-Id
- Framed-IPv6-Prefix
- Login-IPv6-Host
- Framed-IPv6-Route
- Framed-IPv6-Pool
- Delegated-IPv6-Prefix
- Framed-IPv6-Address
- DNS-Server-IPv6-Address
- Route-IPv6-Information
- Delegated-IPv6-Prefix-Pool
- Stateful-IPv6-Address-Pool

The following table lists Supported Cisco Attribute-Value pairs and their equivalent IETF attributes:

Cisco Attribute-Value Pairs	IETF Attributes
ipv6:addrv6=<ipv6 address>	Framed-ipv6-Address
ipv6:stateful-ipv6-address-pool=<name>	Stateful-IPv6-Address-Pool
ipv6:delegated-ipv6-pool=<name>	Delegated-IPv6-Prefix-Pool
ipv6:ipv6-dns-servers-addr=<ipv6 address>	DNS-Server-IPv6-Address

The RADIUS Live Logs page, RADIUS Authentication report, RADIUS Accounting report, Current Active Session report, RADIUS Error report, Misconfigured NAS report, Adaptive Network Control Audit, and Misconfigured Supplicant report support IPv6 addresses. You can view the details about these sessions from the RADIUS Live Logs page or from any of these reports. You can filter the records by IPv4, IPv6, or MAC addresses.

Note If you connect an Android device to an IPv6 enabled DHCPv6 network, it receives only the link-local IPv6 address from the DHCP server. Hence, global IPv6 address is not displayed in the Live Logs and in the Endpoints page (In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Identities** > **Endpoints**).

The following procedure describes how to configure IPv6 attributes in authorization policies.

Before you begin

Ensure that the NADs in your deployment support AAA with IPv6. See **AAA Support for IPv6** for information on how to enable AAA support for IPv6 on your NADs.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Policy Sets** for network access policies. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Device Admin Policy Sets** for device administration policies.

Step 2 Create authorization rules.

Step 3 When creating authorization rules, create a condition from the Conditon Studio. In the Condition Studio, from the RADIUS dictionary, choose the RADIUS IPv6 attribute, the operator, and the value.

Step 4 Click **Save** to save the authorization rules in the policy set.

Policy Set Protocol Settings

You must define global protocol settings in Cisco ISE before you can use these protocols to create, save and implement a policy set. You can use the Protocol Settings page to define global options for the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), and Protected Extensible Authentication Protocol (PEAP) protocols, which communicate with the other devices in your network.

Supported Network Access Policy Set Protocols

The following is a list of protocols that you can choose while defining your Network Access Policy Set policy:

- Password Authentication Protocol (PAP)
- Protected Extensible Authentication Protocol (PEAP)
- Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2)
- Extensible Authentication Protocol-Message Digest 5 (EAP-MD5)
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)
- Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS)
- Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)

Guidelines for Using EAP-FAST as Protocol

Follow these guidelines when using EAP-FAST as an authentication protocol:

- It is highly recommended to enable EAP-TLS inner method when the EAP-FAST accept client certificate is enabled on authenticated provisioning. EAP-FAST accept client certificate on authenticated provisioning is not a separate authentication method but a shorter form of client certificate authentication that uses the same certificate credentials type to authenticate a user but does not require to run an inner method.
- Accept client certificate on authenticated provisioning works with PAC-less full handshake and authenticated PAC provisioning. It does not work for PAC-less session resume, anonymous PAC provisioning, and PAC-based authentication.

- EAP attributes are displayed per identity (so in EAP chaining displayed twice) are shown in authentication details in monitoring tool in order user then machine even if authentication happens in different order.
- When EAP-FAST authorization PAC is used then EAP authentication method shown in live logs is equal to the authentication method used for full authentication (as in PEAP) and not as Lookup.
- In EAP chaining mode when tunnel PAC is expired then ISE falls back to provisioning and AC requests User and Machine authorization PACs - Machine Authorization PAC cannot be provisioned. It will be provisioned in the subsequent PAC-based authentication conversation when AC requests it.
- When Cisco ISE is configured for chaining and AC for single mode then AC response with IdentityType TLV to ISE. However, the second identity authentication fails. You can see from this conversation that client is suitable to perform chaining but currently is configured for single mode.
- Cisco ISE supports retrieval attributes and groups for both machine and user in EAP-FAST chaining only for AD. For LDAP and Internal DB ISE uses only the last identity attributes.

Note "EAP-FAST cryptobinding verification failed" message might be seen if EAP-FAST authentication protocol is used for High Sierra, Mojave, or Catalina MAC OSX devices. We recommend that you configure the Preferred EAP Protocol field in the Allowed Protocols page to use PEAP or EAP-TLS instead of EAP-FAST for these MAC OSX devices.

Configure EAP-FAST Settings

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration** > **System** > **Settings** > **Protocols** > **EAP-FAST** > **EAP Fast Settings**.

Step 2 Enter the details as required to define the EAP-FAST protocol.

Step 3 Click **Revoke** if you want to revoke all the previously generated primary keys and PACs.

Step 4 Click **Save** to save the EAP-FAST settings.

Generate the PAC for EAP-FAST

You can use the Generate PAC option in the Cisco ISE to generate a tunnel or machine PAC for the EAP-FAST protocol.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration** > **System** > **Settings**.

Step 2 From the Settings navigation pane on the left, click **Protocols**.

Step 3 Choose **EAP-FAST** > **Generate PAC**.

Step 4 Enter the details as required to generate machine PAC for the EAP-FAST protocol.

Step 5 Click **Generate PAC**.

EAP-FAST Settings

The following table describes the fields on the Protocol Settings window, which you can use to configure the EAP-FAST, EAP-TLS, and PEAP protocols. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Protocols** > **EAP-FAST** > **EAP FAST Settings**.

Table 146: Configuring EAP-FAST Settings

Field Name	Usage Guidelines
Authority Identity Info Description	Enter a user-friendly string that describes the Cisco ISE node that sends credentials to a client. The client can discover this string in the Protected Access Credentials (PAC) information for type, length, and value (TLV). The default value is Identity Services Engine.
Master Key Generation Period	Specifies the primary key generation period in seconds, minutes, hours, days, or weeks. The value must be a positive integer in the range 1 to 2147040000 seconds. The default is 604800 seconds, which is equivalent to one week.
Revoke all master keys and PACs	Click Revoke to revoke all primary keys and PACs.
Enable PAC-less Session Resume	Check this check box if you want to use EAP-FAST without the PAC files.
PAC-less Session Timeout	Specifies the time in seconds after which the PAC-less session resume times out. The default is 7200 seconds.

Related Topics

- Policy Set Protocol Settings, on page 1024
- Guidelines for Using EAP-FAST as Protocol, on page 1024
- Benefits of EAP-FAST, on page 1068
- Configure EAP-FAST Settings, on page 1025

PAC Settings

The following table describes the fields on the Generate PAC window, which you can use to configure protected access credentials for EAP-FAST authentication. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Protocols** > **EAP-FAST** > **Generate PAC**.

Table 147: Generating PAC for EAP-FAST Settings

Field Name	Usage Guidelines
Tunnel PAC	Click this radio button to generate a tunnel PAC.
Machine PAC	Click this radio button to generate a machine PAC.
Trustsec PAC	Click this radio button to generate a Trustsec PAC.
Identity	(For Tunnel and Machine PAC) Specifies the username or machine name that is presented as the “inner username” by the EAP-FAST protocol. If the identity string does not match that username, authentication fails. This is the hostname as defined on the Adaptive Security Appliance (ASA). The identity string must match the ASA hostname otherwise, ASA cannot import the PAC file that is generated. If you are generating a Trustsec PAC, the Identity field specifies the Device ID of a Trustsec network device and is provided with an initiator ID by the EAP-FAST protocol. If the Identity string entered here does not match that Device ID, authentication fails.
PAC Time to Live	(For Tunnel and Machine PAC) Enter a value in seconds that specifies the expiration time for the PAC. The default is 604800 seconds, which is equivalent to one week. This value must be a positive integer between 1 and 157680000 seconds. For the Trustsec PAC, enter a value in days, weeks, months, or years. By default, the value is one year. The minimum value is one day and the maximum is 10 years.
Encryption Key	Enter an encryption key. The length of the key must be between 8 and 256 characters. The key can contain uppercase or lowercase letters, or numbers, or a combination of alphanumeric characters.
Expiration Data	(For Trustsec PAC only) The expiration date is calculated based on the PAC Time to Live.

Related Topics

Policy Set Protocol Settings, on page 1024

Guidelines for Using EAP-FAST as Protocol, on page 1024

Generate the PAC for EAP-FAST, on page 1025

Using EAP-TTLS as Authentication Protocol

EAP-TTLS is a two-phase protocol that extends the functionality of EAP-TLS protocol. Phase 1 builds the secure tunnel and derives the session keys used in Phase 2 to securely tunnel attributes and inner method data between the server and the client. You can use the attributes tunneled during Phase 2 to perform additional authentications using a number of different mechanisms.

Cisco ISE can process authentications from a variety of TTLS supplicants including:

- Network Access Manager (NAM) on Windows
- Windows 8.1 native supplicant
- Secure W2 (also called as JoinNow on MultiOS)
- MAC OS X native supplicant
- IOS native supplicant
- Android based native supplicant
- Linux WPA supplicant

Note If cryptobinding is required, you must use EAP-FAST as the inner method.

Configure EAP-TTLS Settings

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Protocols** > **EAP-TTLS**

Step 2 Enter the required details in the EAP-TTLS Settings page.

Step 3 Click **Save**.

EAP-TTLS Settings

The following table describes the fields on the EAP-TTLS Settings window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Protocols** > **EAP-TTLS**.

Table 148: EAP-TTLS Settings

Field Name	Usage Guidelines
Enable EAP-TTLS Session Resume	If you check this check box, Cisco ISE will cache the TLS session that is created during phase one of EAP-TTLS authentication, provided the user successfully authenticates in phase two of EAP-TTLS. If a user needs to reconnect and the original EAP-TTLS session has not timed out, Cisco ISE uses the cached TLS session, resulting in faster EAP-TTLS performance and a reduced AAA server load. **Note** When the EAP-TTLS session is resumed, the inner method is skipped.
EAP-TTLS Session Timeout	Specifies the time in seconds after which the EAP-TTLS session times out. The default value is 7200 seconds.

Related Topics

Policy Set Protocol Settings, on page 1024
Using EAP-TTLS as Authentication Protocol, on page 1028
Configure EAP-TTLS Settings, on page 1028

Configure EAP-TLS Settings

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration** > **System** > **Settings** > **Protocols** > **EAP-TLS**.
Step 2 Enter the details as required to define the EAP-TLS protocol.
Step 3 Click **Save** to save the EAP-TLS settings.

EAP-TLS Settings

The following table describes the fields on the EAP-TLS Settings window, which you can use to configure the EAP-TLS protocol settings. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Protocols** > **EAP-TLS**.

Table 149: EAP-TLS Settings

Fields	Usage Guidelines
Enable EAP-TLS Session Resume	Check this check box to support an abbreviated reauthentication of a user who has passed full EAP-TLS authentication. This feature provides reauthentication of the user with only a Secure Sockets Layer (SSL) handshake and without applying the certificates. EAP-TLS session resume works only if the EAP-TLS session has not timed out.
EAP-TLS Session Timeout	Specifies the time in seconds after which the EAP-TLS session times out. The default value is 7200 seconds.
Stateless Session Resume	
Master Key Generation Period	Enter the time after which the primary key is regenerated. This value determines the duration that a primary key remains active. You can enter the value in seconds, minutes, hours, days, or weeks.
Revoke	Click **Revoke** to cancel all previously generated primary keys and tickets. This option is disabled on the secondary node.

Related Topics

Policy Set Protocol Settings, on page 1024

Configure EAP-TLS Settings, on page 1029

Configure PEAP Settings

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration** > **System** > **Settings**.

Step 2 From the Settings navigation pane on the left, click **Protocols**.

Step 3 Choose **PEAP**.

Step 4 Enter the details as required to define the PEAP protocol.

Step 5 Click **Save** to save the PEAP settings.

PEAP Settings

The following table describes the fields on the PEAP Settings window, which you can use to configure the PEAP protocol settings. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Protocols** > **PEAP**.

Table 150: PEAP Settings

Field Name	Usage Guidelines
Enable PEAP Session Resume	Check this check box for the Cisco ISE to cache the TLS session that is created during phase one of PEAP authentication, provided the user successfully authenticates in phase two of PEAP. If a user needs to reconnect and the original PEAP session has not timed out, the Cisco ISE uses the cached TLS session, resulting in faster PEAP performance and a reduced AAA server load. You must specify a PEAP session timeout value for the PEAP session resume features to work.
PEAP Session Timeout	Specifies the time in seconds after which the PEAP session times out. The default value is 7200 seconds.
Enable Fast Reconnect	Check this check box to allow a PEAP session to resume in the Cisco ISE without checking user credentials when the session resume feature is enabled.

Related Topics

Policy Set Protocol Settings, on page 1024
Configure PEAP Settings, on page 1030
Advantages of Using PEAP, on page 1066
Supported Supplicants for the PEAP Protocol, on page 1066
PEAP Protocol Flow, on page 1067

Configure RADIUS Settings

You can configure the RADIUS settings to detect the clients that fail to authenticate and to suppress the repeated reporting of successful authentications.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings**

Step 2 From the Settings navigation pane, click **Protocols**.

Step 3 Choose **RADIUS**.

Step 4 Enter the details as required to define the RADIUS settings.

Step 5 Click **Save** to save the settings.

RADIUS Settings

The following table describes the fields on the RADIUS Settings page. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Protocols** > **RADIUS**.

If you enable the **Suppress Repeated Failed Clients** option, clients with repeated authentication failures will be suppressed from the audit logs, and requests from these clients will be automatically rejected for the specified time period. You can also specify the number of authentication failures after which requests from these clients should be rejected. For example, if this value is configured as 5, when a client authentication fails five times, all requests received from that client will be rejected for the configured time period.

Note

- If the cause of endpoint authentication failure is the entry of a wrong password and user type is internal user, the endpoint is suppressed and enters rejection mode. However, if a wrong password is detected in the case of Active Directory users, the endpoint is suppressed but does not enter rejection mode.
- Client suppression in Cisco ISE works only if there is a MAC address associated with the calling station ID of the client.

An endpoint is released from the rejection mode at the end of the time specified in the **Reject RADIUS Requests from Clients with Repeated Failures** setting.

To release a rejected endpoint ahead of the **Reject RADIUS Requests from Clients with Repeated Failures** configuration:

- In the Cisco ISE administration portal, go to the **Context Visibility** > **Endpoints** page. Check the check boxes adjacent to the endpoints you want to release and click **Remove** at the top of the endpoints table.
- Use the ERS API PUT /ers/config/endpoint/{id}/releaserejectedendpoint to release the endpoint.

Note If you configure suppression of RADIUS failures, you may still receive the error "`5440 Endpoint Abandoned EAP Session and started a new one`" after you configure RADIUS log suppression. For more information, see the following ISE Community post:

https://community.cisco.com/t5/network-access-control/authentication-failed-quot-5440-endpoint-abandoned-eap-session/td-p/3191944

Table 151: RADIUS Settings

Field Name	Usage Guidelines
Suppress Repeated Failed Clients	

Field Name	Usage Guidelines
Suppress Repeated Failed Clients	Check this check box to suppress the clients for which the authentications fail repeatedly for the same reason. These clients are suppressed from the audit logs and the requests from these clients are rejected for the specified time period if **Reject RADIUS Requests from Clients with Repeated Failures** option is enabled. **Note** CTS related logs are not suppressed even if this option is enabled and are always included in the Live Logs.
Detect Two Failures Within	Enter the time interval in minutes. If a client fails authentication twice for the same reason within this time period, it will be suppressed from the audit logs, and the requests from this client will be rejected if **Reject RADIUS Requests from Clients with Repeated Failures** option is enabled.
Remember • If the **Suppress Repeated Failed Clients** check box is checked and two failures occur **within** the time specified in the **Detect Two Failures Within** field, the endpoint is considered misconfigured. A misconfigured endpoint requires the admin's intervention to ensure successful authentication. When an endpoint fails the first authentication, the relevant information is displayed in the admin's dashboard. Subsequent authentication failures with the same reasons do not contain any added information for the admin. Therefore, repeated authentication failures of an endpoint for a particular reason during the duration specified in the **Report Failures Once Every** field are not reported in the audit logs. After the duration specified in the **Report Failures Once Every** field,the **TotalFailedAttempts** and **TotalFailedTime** information about the misconfigured endpoint is reported to the monitoring node. • If the **Suppress Repeated Failed Clients** check box is checked and two failures occur **after** the time specified in the **Detect Two Failures Within** field, the failed authentication attempts of the endpoint will be reported in the audit logs as separate instances even if the reason for the authentication failure remains the same. • Cisco ISE allows the endpoint to conduct several consecutive failures with different failure reasons because endpoints can have various supplicant profiles. Therefore, if the endpoint fails to authenticate several times because of different failure reasons, Cisco ISE counts each failure reason separately.	
Report Failures Once Every	Enter the time interval in minutes for the failed authentications to be reported. For example, if this value is set as 15 minutes, clients that repeatedly fail authentication will be reported in the audit logs only once every 15 minutes, thereby preventing over-reporting.

Field Name	Usage Guidelines
Reject RADIUS Requests from Clients with Repeated Failures	Check this check box to automatically reject the RADIUS requests from the clients for which the authentications fail repeatedly. You can enable this option to avoid unnecessary processing by Cisco ISE and to protect against potential denial of service attacks.
Remember • If the **Reject RADIUS Requests from Clients with Repeated Failures** check box is checked and the endpoint experiences authentication failures equal to the number mentioned in the **Failures Prior to Automatic Rejection** field, the endpoint is considered misconfigured and is rejected. Cisco ISE will immediately reject the first RADIUS message with the authentication request from this endpoint, thus, not allowing the endpoint to complete the authentication. No audit logs will be generated for the endpoint. The endpoint stays rejected for the duration given in the **Continue Rejecting Requests for** field. The endpoint can send an authentication request after the duration specified in the **Continue Rejecting Requests for**, and if the authentication is successful, the endpoint will be configured. • You can view and release the rejected endpoints on the **Context Visibility** (**Context Visibility** > **Endpoints**) page. Select the rejected endpoints and click **Release Rejected** to release the rejected endpoints. The audit logs for the released endpoints will be sent to the monitoring node. • If there is no activity from the misconfigured endpoint for a period of six hours, it will no longer be considered as misconfigured.	
Failures Prior to Automatic Rejection	Enter the number of authentication failures after which requests from clients with repeated failures are automatically rejected. All the requests received from these clients are automatically rejected for the configured time period (specified in **Continue Rejecting Requests for** field). After the interval expires, the authentication requests from these clients are processed.
Continue Rejecting Requests for	Enter the time interval (in minutes) for which the requests from clients with repeated failures are to be rejected.
Ignore Repeated Accounting Updates Within	Repeated accounting updates that occur within this period will be ignored.
Suppress Successful Reports	
Suppress Repeated Successful Authentications	Check this check box to prevent repeated reporting of successful authentication requests in last 24 hours that have no change in identity context, network device, and authorization.
Authentications Details	

Field Name	Usage Guidelines
Highlight Steps Longer Than	Enter the time interval in milliseconds. If execution of a single step exceeds the specified threshold, it will be marked with a clock icon in the authentication details page.
Detect High Rate of RADIUS Requests	
Detect Steady High Rate of Radius Requests	Check this check box to raise an alarm for high RADIUS request load when the limit specified in the **Duration of RADIUS requests** and **Total number of RADIUS requests** fields is exceeded.
Duration of RADIUS Requests	Enter the period of time (in seconds) that will be used to calculate the RADIUS rate. The default is 60 seconds. The valid range is from 20 to 86400 seconds.
Total Number of RADIUS Requests	Enter the request limit that will be used to calculate the RADIUS rate. The default is 72000 requests. The valid range is from 24000 to 103680000 requests.
RADIUS UDP Ports	
Authentication Ports	Specify the ports to be used for RADIUS UDP authentication flows. You can specify a maximum of 4 port numbers (separated by a comma). By default, port 1812 and port 1645 are used. The valid range is from 1024 to 65535.
Accounting Ports	Specify the ports to be used for RADIUS UDP accounting flows. You can specify a maximum of 4 port numbers (separated by a comma). By default, port 1813 and port 1646 are used. The valid range is from 1024 to 65535. **Note** Ensure that these ports are not used by other services.
RADIUS DTLS	
Authentication and Accounting Port	Specify the port to be used for RADIUS DTLS authentication and accounting flows. By default, port 2083 is used. The valid range is from 1024 to 65535. **Note** Ensure that this port is not used by other services.
Idle Timeout	Enter the time (in seconds) that you want Cisco ISE to wait before it closes the TLS session if no packets are received from the network device. Default value is 120 seconds. The valid range is from 60 to 600 seconds.

Field Name	Usage Guidelines
Enable RADIUS/DTLS Client Identity Verification	Check this check box if you want Cisco ISE to verify the identity of the RADIUS/DTLS clients during the DTLS handshake. Cisco ISE fails the handshake if the client identity is not valid. Identity check is skipped for the default network device, if configured. Identity check is performed in the following sequence: **1.** If the client certificate contains the subject alternative name (SAN) attribute: • If SAN contains the DNS name, the DNS name specified in the certificate is compared with the DNS name that is configured for the network device in Cisco ISE. • If SAN contains the IP address (and does not contain the DNS name), the IP address specified in the certificate is compared with all the device IP addresses configured in Cisco ISE. **2.** If the certificate does not contain SAN, subject CN is compared with the DNS name that is configured for the network device in Cisco ISE. Cisco ISE fails the handshake in the case of mismatch.

Related Topics

Policy Set Protocol Settings, on page 1024
RADIUS Protocol Support in Cisco ISE, on page 1043
Configure RADIUS Settings, on page 1031

Configure Security Settings

Perform the following procedure to configure the security settings.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Security Settings**.

Step 2 In the **Security Settings** window, choose the required options:

- **Allow TLS 1.0**: Allows TLS 1.0 for communication with legacy peers for the following workflows:
  - Cisco ISE is configured as an EAP server
  - Cisco ISE downloads CRL from HTTPS or a secure LDAP server
  - Cisco ISE is configured as a secure TCP syslog client
  - Cisco ISE is configured as a secure LDAP client
  - Cisco ISE is configured as an ERS server

  Also allows TLS 1.0 for communication with the following Cisco ISE components:

  - All portals
  - Certificate Authority
  - MDM Client
  - pxGrid
  - PassiveID Agent

  Note We recommend that clients and servers negotiate to use a higher version of TLS for enhanced security.

- **Allow TLS 1.1**: Allows TLS 1.1 for communication with legacy peers for the following workflows:
  - Cisco ISE is configured as an EAP server
  - Cisco ISE downloads CRL from HTTPS or a secure LDAP server
  - Cisco ISE is configured as a secure TCP syslog client
  - Cisco ISE is configured as a secure LDAP client
  - Cisco ISE is configured as an ERS server

  Also allows TLS 1.1 for communication with the following Cisco ISE components:

  - All portals
  - Certificate Authority
  - External RESTful Services (ERS)
  - MDM Client
  - pxGrid

  Note We recommend that clients and servers negotiate to use a higher version of TLS for enhanced security.

- **Allow SHA-1 Ciphers**: Allows SHA-1 ciphers for communication with peers for the following workflows:
  - Cisco ISE is configured as an EAP server
  - Cisco ISE is configured as a RADIUS DTLS server
  - Cisco ISE is configured as a RADIUS DTLS client
  - Cisco ISE downloads CRL from HTTPS or a secure LDAP server
  - Cisco ISE is configured as a secure syslog client
  - Cisco ISE is configured as a secure LDAP client

  Also allows SHA-1 ciphers for communication with the following Cisco ISE components:

  - Admin Access UI
  - All portals
  - ERS

  - pxGrid
  - Admin Access: 443
  - Cisco ISE Portals: 9002, 8443, 8444, 8445, 8449
  - ERS: 9060, 9061, 9063
  - pxGrid: 8910

  Note This option is disabled by default.

  You must restart all the nodes in a deployment after enabling or disabling the **Allow SHA-1 Ciphers** option. If restart is not successful, the configuration changes are not applied. In such a scenario, you must restart all the nodes manually using the following commands:

  application stop ise and **application start ise**.

  You can select one of the following options while allowing SHA-1 ciphers for communication with legacy peers:

  - **Allow all SHA-1 Ciphers**: Allows all SHA-1 ciphers for communication with legacy peers.
  - **Allow only TLS_RSA_with_AES_128_CBC_SHA**: Allows only TLS_RSA_with_AES_128_CBC_SHA cipher for communication with legacy peers.

  Note We recommend that you use SHA-256 or SHA-384 ciphers for enhanced security.

- **Allow ECDHE-RSA Ciphers**: Allows ECDHE-RSA ciphers for communication with peers for the following workflows:
  - Cisco ISE is configured as an EAP server
  - Cisco ISE is configured as a RADIUS DTLS server
  - Cisco ISE is configured as a RADIUS DTLS client
  - Cisco ISE downloads CRL from HTTPS or a secure LDAP server
  - Cisco ISE is configured as a secure syslog client
  - Cisco ISE is configured as a secure LDAP client
- **Allow 3DES ciphers**: Allows 3DES ciphers for communication with peers for the following workflows:
  - Cisco ISE is configured as an EAP server
  - Cisco ISE is configured as a RADIUS DTLS server
  - Cisco ISE is configured as a RADIUS DTLS client
  - Cisco ISE downloads CRL from HTTPS or a secure LDAP server
  - Cisco ISE is configured as a secure syslog client
  - Cisco ISE is configured as a secure LDAP client
- **Accept Certificates without Validating Purpose**: When Cisco ISE acts as an EAP or RADIUS DTLS server, client certificates are accepted without checking whether:

    - The Key Usage extension contains the keyAgreement bit for ECDHE-ECDSA ciphers or the keyEncipherment bit for other ciphers
    - Extended Key Usage attribute value is ClientAuth

  When this option is disabled, Cisco ISE will validate the purpose of all the client certificates. A certificate will be considered valid only if one of the following conditions is met:

    - If there is no value for the Extended Key Usage attribute:
        - If the cipherGroup is ECDHE-ECDSA, then the Key Usage extension must contain the KeyAgreement value.
        - If the cipherGroup is not ECDHE-ECDSA, then the Key Usage extension must contain the keyEncipherment and digitalSignature values.
    - If the Extended Key Usage attribute value is ClientAuth:
        - If the cipherGroup is ECDHE-ECDSA, then the Key Usage extension must contain the KeyAgreement value.
        - If the cipherGroup is not ECDHE-ECDSA, then the Key Usage extension must contain the keyEncipherment and digitalSignature values.

  The certificate validation will fail if none of the above conditions are met.

- **Allow DSS ciphers for ISE as a client**: When Cisco ISE acts as a client, allows DSS ciphers for communication with a server for the following workflows:
    - Cisco ISE is configured as a RADIUS DTLS client
    - Cisco ISE downloads CRL from HTTPS or a secure LDAP server
    - Cisco ISE is configured as a secure syslog client
    - Cisco ISE is configured as a secure LDAP client
- **Allow Legacy Unsafe TLS Renegotiation for ISE as a Client**: Allows communication with legacy TLS servers that do not support safe TLS renegotiation for the following workflows:
    - Cisco ISE downloads CRL from HTTPS or a secure LDAP server
    - Cisco ISE is configured as a secure syslog client
    - Cisco ISE is configured as a secure LDAP client
- **Disclose invalid usernames**: By default, Cisco ISE displays the `invalid` message for authentication failures because of incorrect usernames. To aid in debugging, this option forces Cisco ISE to display usernames in reports, instead of the `invalid` message. Note that usernames are always displayed for failed authentications that are not because of incorrect usernames.

  This feature is supported for Active Directory, Internal Users, LDAP, and ODBC identity sources. It is not supported for other identity stores, such as RADIUS token, RSA, or SAML.

Step 3 Click **Save**.

Supported Cipher Suites

Cisco ISE supports TLS versions 1.0, 1.1, and 1.2.

Cisco ISE supports RSA and ECDSA server certificates. The following elliptic curves are supported:

- secp256r1
- secp384r1
- secp521r1

The following table lists the supported Cipher Suites:

Cipher Suite	**When Cisco ISE is configured as an EAP server** **When Cisco ISE is configured as a RADIUS DTLS server**	**When Cisco ISE downloads CRL from HTTPS or a secure LDAP server** **When Cisco ISE is configured as a secure syslog client or a secure LDAP client** **When Cisco ISE is configured as a RADIUS DTLS client for CoA**
TLS 1.0 support	When TLS 1.0 is allowed (DTLS server supports only DTLS 1.2) Allow TLS 1.0 option is disabled by default in Cisco ISE 2.3 and above. TLS 1.0 is not supported for TLS based EAP authentication methods (EAP-TLS, EAP-FAST/TLS) and 802.1X supplicants when this option is disabled. If you want to use the TLS based EAP authentication methods in TLS 1.0, check the Allow TLS 1.0 check box in the **Security Settings** window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Protocols** > **Security Settings**.	When TLS 1.0 is allowed (DTLS client supports only DTLS 1.2)
TLS 1.1 support	When TLS 1.1 is allowed	When TLS 1.1 is allowed
ECC DSA ciphers		
ECDHE-ECDSA-AES256-GCM-SHA384	Yes	Yes

ECDHE-ECDSA-AES128-GCM-SHA256	Yes	Yes
ECDHE-ECDSA-AES256-SHA384	Yes	Yes
ECDHE-ECDSA-AES128-SHA256	Yes	Yes
ECDHE-ECDSA-AES256-SHA	When SHA-1 is allowed	When SHA-1 is allowed
ECDHE-ECDSA-AES128-SHA	When SHA-1 is allowed	When SHA-1 is allowed
ECC RSA ciphers		
ECDHE-RSA-AES256-GCM-SHA384	When ECDHE-RSA is allowed	When ECDHE-RSA is allowed
ECDHE-RSA-AES128-GCM-SHA256	When ECDHE-RSA is allowed	When ECDHE-RSA is allowed
ECDHE-RSA-AES256-SHA384	When ECDHE-RSA is allowed	When ECDHE-RSA is allowed
ECDHE-RSA-AES128-SHA256	When ECDHE-RSA is allowed	When ECDHE-RSA is allowed
ECDHE-RSA-AES256-SHA	When ECDHE-RSA/SHA-1 is allowed	When ECDHE-RSA/SHA-1 is allowed
ECDHE-RSA-AES128-SHA	When ECDHE-RSA/SHA-1 is allowed	When ECDHE-RSA/SHA-1 is allowed
DHE RSA ciphers		
DHE-RSA-AES256-SHA256	No	Yes
DHE-RSA-AES128-SHA256	No	Yes
DHE-RSA-AES256-SHA	No	When SHA-1 is allowed
DHE-RSA-AES128-SHA	No	When SHA-1 is allowed
RSA ciphers		
AES256-SHA256	Yes	Yes
AES128-SHA256	Yes	Yes
AES256-SHA	When SHA-1 is allowed	When SHA-1 is allowed

AES128-SHA	When SHA-1 is allowed	When SHA-1 is allowed
3DES ciphers		
DES-CBC3-SHA	When 3DES/SHA-1 is allowed	When 3DES/DSS and SHA-1 are enabled
DSS ciphers		
DHE-DSS-AES256-SHA	No	When 3DES/DSS and SHA-1 are enabled
DHE-DSS-AES128-SHA	No	When 3DES/DSS and SHA-1 are enabled
EDH-DSS-DES-CBC3-SHA	No	When 3DES/DSS and SHA-1 are enabled
Weak RC4 ciphers		
RC4-SHA	When "Allow weak ciphers" option is enabled in the Allowed Protocols page and when SHA-1 is allowed	No
RC4-MD5	When "Allow weak ciphers" option is enabled in the Allowed Protocols page	No
EAP-FAST anonymous provisioning only: ADH-AES-128-SHA	Yes	No
Peer certificate restrictions		
Validate KeyUsage	Client certificate should have KeyUsage=Key Agreement and ExtendedKeyUsage=Client Authentication for the following ciphers: • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	

Validate ExtendedKeyUsage	Client certificate should have KeyUsage=Key Encipherment and ExtendedKeyUsage=Client Authentication for the following ciphers: • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA • DHE-RSA-AES128-SHA • DHE-RSA-AES256-SHA • DHE-RSA-AES128-SHA256 • DHE-RSA-AES256-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES256-SHA • ECDHE-RSA-AES128-SHA • EDH-RSA-DES-CBC3-SHA • DES-CBC3-SHA • RC4-SHA • RC4-MD5	Server certificate should have ExtendedKeyUsage=Server Authentication

RADIUS Protocol Support in Cisco ISE

RADIUS is a client/server protocol through which remote-access servers communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. You can use RADIUS to maintain user profiles in a central database that all remote servers can share. This protocol provides better security, and you can use it to set up a policy that is applied at a single administered network point.

RADIUS also functions as a RADIUS client in Cisco ISE to proxy requests to a remote RADIUS server, and it provides Change of Authorization (CoA) activities during an active session.

Cisco ISE supports RADIUS protocol flow according to RFC 2865 and generic support for all general RADIUS attributes as described in RFC 2865 and its extension. Cisco ISE supports parsing of vendor-specific attributes only for vendors that are defined in the Cisco ISE dictionary.

RADIUS interface supports the following attribute data types that are defined in RFC 2865:

- Text (Unicode Transformation Format [UTF])
- String (binary)
- Address (IP)
- Integer
- Time

ISE Community Resource

For information about the network access attributes supported by Cisco ISE, see ISE Network Access Attributes.

Allowed Protocols

The following table describes the fields in the **Allowed Protocols** window, which allows you to configure the protocols to be used during authentication. **Policy** > **Policy Elements** > **Results** > **Authentication** > **Allowed Protocols**.

Table 152: Allowed Protocols

Field Name	**Usage Guidelines**
Allowed Protocols > Authentication Bypass	
Process Host Lookup	Check this check box if you want Cisco ISE to process the Host Lookup request. The Host Lookup request is processed for PAP/CHAP protocol when the RADIUS Service-Type equals 10 (Call-Check) and the username is equal to Calling-Station-ID. The Host Lookup request is processed for EAP-MD5 protocol when the Service-Type equals 1 (Framed) and the username is equal to Calling-Station-ID. Uncheck this check box if you want Cisco ISE to ignore the Host Lookup request and use the original value of the system username attribute for authentication. When unchecked, message processing is done according to the protocol (for example, PAP). **Note** Disabling this option could result in the failure of existing MAB authentications.
Allowed Protocols > Authentication Protocols	
Allow PAP/ASCII	This option enables PAP/ASCII. PAP uses cleartext passwords (that is, unencrypted passwords) and is the least secure authentication protocol.
Allow CHAP	This option enables CHAP authentication. CHAP uses a challenge-response mechanism with password encryption. CHAP does not work with Microsoft Active Directory.
Allow MS-CHAPv1	Check this check box to enable MS-CHAPv1.
Allow MS-CHAPv2	Check this check box to enable MS-CHAPv2.
Allow EAP-MD5	Check this check box to enable EAP-based MD5 password hashed authentication.

Field Name	Usage Guidelines
Allow EAP-TLS	Check this check box to enable EAP-TLS Authentication protocol and configures EAP-TLS settings. You can specify how Cisco ISE will verify the user identity as presented in the EAP identity response from the end-user client. User identity is verified against information in the certificate that the end-user client presents. This comparison occurs after an EAP-TLS tunnel is established between Cisco ISE and the end-user client. **Note** EAP-TLS is a certificate-based authentication protocol. EAP-TLS authentication can occur only after you have completed the required steps to configure certificates. • **Allow authentication of expired certificates to allow certificate renewal in Authorization Policy**: Check this check box, if you want to allow users to renew certificates. If you check this check box, ensure that you configure appropriate authorization policy rules to check if the certificate has been renewed before processing the request any further. • **Enable Stateless Session Resume**: Check this check box to allow EAP-TLS session resumption without requiring the session state to be stored at the server. Cisco ISE supports session ticket extension as described in RFC 5077. Cisco ISE creates a ticket and sends it to an EAP-TLS client. The client presents the ticket to ISE to resume a session. • **Proactive Session Ticket update**: Enter the value as a percentage to indicate how much of the Time To Live (TTL) must elapse before the session ticket is updated. For example, if you enter the value 60, the session ticket is updated after 60 percent of the TTL has expired. • **Session ticket Time to Live**: Enter the time after which the session ticket expires. This value determines the duration that a session ticket remains active. You can enter the value in seconds, minutes, hours, days, or weeks.
Allow LEAP	Check this check box to enable Lightweight Extensible Authentication Protocol (LEAP) authentication.

Field Name	Usage Guidelines

Allow PEAP	Check this check box to enable PEAP authentication protocol and PEAP settings. The default inner method is MS-CHAPv2.
	When you check the Allow PEAP check box, you can configure the following PEAP inner methods:
	• **Allow EAP-MS-CHAPv2**: Check this check box to use EAP-MS-CHAPv2 as the inner method.
	  • **Allow Password Change**: Check this check box for Cisco ISE to support password changes.
	  • **Retry Attempts**: Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 0 to 3.
	• **Allow EAP-GTC**: Check this check box to use EAP-GTC as the inner method.
	  • **Allow Password Change**: Check this check box for Cisco ISE to support password changes.
	  • **Retry Attempts**: Specifies how many times Cisco ISE requests user credentials before returning login failure. The valid range is from 0 to 3.
	• **Allow EAP-TLS**: Check this check box to use EAP-TLS as the inner method.
	Check the **Allow authentication of expired certificates to allow certificate renewal in Authorization Policy** check box, if you want to allow users to renew certificates. If you check this check box, ensure that you configure appropriate authorization policy rules to check if the certificate has been renewed before processing the request any further.
	• **Require Cryptobinding TLV**: Check this check box if you want both the EAP peer and the EAP server to participate in the inner and outer EAP authentications of the PEAP authentication.
	• **Allow PEAPv0 Only for Legacy Clients**: Check this check box to allow PEAP supplicants to negotiate using PEAPv0. Some legacy clients do not conform to the PEAPv1 protocol standards. To ensure that such PEAP conversations are not dropped, check this check box.

Field Name	Usage Guidelines
Allow EAP-FAST	

Field Name	Usage Guidelines

	Check this check box to enable EAP-FAST authentication protocol and EAP-FAST settings. The EAP-FAST protocol can support multiple internal protocols on the same server. The default inner method is MS-CHAPv2.
	When you check the Allow EAP-FAST check box, you can configure EAP-FAST as the inner method:
	• **Allow EAP-MS-CHAPv2**
	  • **Allow Password Change**: Check this check box for Cisco ISE to support password changes.
	  • **Retry Attempts**: Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 0-3.
	• **Allow EAP-GTC**
	Allow Password Change: Check this check box for Cisco ISE to support password changes.
	Retry Attempts: Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 0-3.
	• **Use PACs**: Choose this option to configure Cisco ISE to provision authorization Protected Access Credentials (PAC) for EAP-FAST clients. Additional PAC options appear.
	• **Don't Use PACs**: Choose this option to configure Cisco ISE to use EAP-FAST without issuing or accepting any tunnel or machine PACs. All requests for PACs are ignored and Cisco ISE responds with a Success-TLV without a PAC.
	When you choose this option, you can configure Cisco ISE to perform machine authentication.
	• **Allow EAP-TLS**: Check this check box to use EAP-TLS as the inner method.
	Check the **Allow authentication of expired certificates to allow certificate renewal in Authorization Policy** check box, if you want to allow users to renew certificates. If you check this check box, ensure that you configure appropriate authorization policy rules to check if the certificate has been renewed before processing the request any further.
	• **Enable EAP Chaining**: Check this check box to enable EAP chaining.
	EAP chaining allows Cisco ISE to correlate the results of user and machine authentication and apply the appropriate authorization policy using the EAPChainingResult attribute.
	EAP chaining requires a supplicant that supports EAP

Field Name	Usage Guidelines
	chaining on the client device. Choose the User and Machine Authentication option in the supplicant. EAP chaining is available when you choose the EAP-FAST protocol (both in PAC based and PAC less mode). For PAC-based authentication, you can use user authorization PAC or machine authorization PAC, or both to skip the inner method. For certificate-based authentication, if you enable the Accept Client Certificate for Provisioning option for the EAP-FAST protocol (in the Allowed Protocol service), and if the endpoint (AnyConnect) is configured to send the user certificate inside the tunnel, then during tunnel establishment, ISE authenticates the user using the certificate (the inner method is skipped), and machine authentication is done through the inner method. If these options are not configured, EAP-TLS is used as the inner method for user authentication. After you enable EAP chaining, update your authorization policy and add a condition using the NetworkAccess:EapChainingResult attribute and assign appropriate permissions.

Field Name	Usage Guidelines

Allow EAP-TTLS	Check this check box to enable EAP-TTLS protocol.
	You can configure the following inner methods:
	• **Allow PAP/ASCII**: Check this check box to use PAP/ASCII as the inner method. You can use EAP-TTLS PAP for token and OTP-based authentications.
	• **Allow CHAP**: Check this check box to use CHAP as the inner method. CHAP uses a challenge-response mechanism with password encryption. CHAP does not work with Microsoft Active Directory.
	• **Allow MS-CHAPv1**: Check this check box to use MS-CHAPv1 as the inner method.
	• **Allow MS-CHAPv2**: Check this check box to use MS-CHAPv2 as the inner method.
	• **Allow EAP-MD5**: Check this check box to use EAP-MD5 as the inner method.
	• **Allow EAP-MS-CHAPv2**: Check this check box to use EAP-MS-CHAPv2 as the inner method.
	  • **Allow Password Change**: Check this check box for Cisco ISE to support password changes.
	  • **Retry Attempts**: Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 0 to 3.

Field Name	Usage Guidelines
Allow TEAP	

Field Name	Usage Guidelines

	Check this check box to enable the Tunnel Extensible Authentication Protocol (TEAP) and configure the TEAP settings. TEAP is a tunnel-based EAP method that enables secure communication between a peer and a server by using the Transport Layer Security (TLS) protocol to establish a tunnel. The type-length-value (TLV) objects are used within the TEAP tunnel to transport authentication-related data between the EAP peer and the EAP server.
	You can configure the following inner methods for TEAP:
	• **Allow EAP-MS-CHAPv2**: Check this check box to use EAP-MS-CHAPv2 as the inner method.
	  • **Allow Password Change**: Check this check box for Cisco ISE to support password changes.
	  • **Retries**: Enter the number of times that Cisco ISE will allow a user to enter the credentials before returning a login failure message. The valid range is from 0 to 3.
	• **Allow EAP-TLS**: Check this check box to use EAP-TLS as the inner method.
	  • **Allow Authentication of Expired Certificates to Allow Certificate Renewal in Authorization Policy**: Check this check box if you want to allow a user to renew certificates. If you enable this option, ensure that you configure the appropriate authorization policy rules to verify whether the certificates have been renewed, before processing the authorization request further.
	• **Allow Downgrade to MSK**: Check this check box if the inner method supports the Extended Master Session Key (EMSK), but the client device provides only the Master Session Key (MSK). Note that while EMSK is more secure than MSK, some client devices might not support EMSK.
	• **Accept Client Certificate during Tunnel Establishment**: Check this check box if you want Cisco ISE to request for a client certificate during TEAP tunnel establishment. If the certificate is not provided, Cisco ISE uses the configured inner methods for authentication.
	• **Enable EAP Chaining**: Check this check box to enable EAP chaining. EAP chaining allows Cisco ISE to run both the inner methods for user and machine authentication inside the same TEAP tunnel. This enables Cisco ISE to correlate the authentication results and apply the appropriate authorization policy, using the EAPChainingResult attribute.
	After you enable EAP chaining, update your authorization policy, add a condition using the

Field Name	Usage Guidelines
	NetworkAccess:EapChainingResult attribute, and assign the appropriate permissions. **Note** When EAP chaining is enabled, ensure that the user and machine certificates are copied in the supplicant if you want to do both user and machine authentication. **Note** • If EAP chaining is enabled in Cisco ISE, both the primary and secondary authentication method must be configured for the Microsoft supplicant. • If EAP chaining is disabled in Cisco ISE, only the primary authentication method must be configured for the Microsoft supplicant. • If both the primary and secondary authentication method are configured as None, EAP negotiation might fail with the following message: `Supplicant stopped responding to ISE`
Preferred EAP Protocol	Check this check box to choose your preferred EAP protocols from any of the following options: EAP-FAST, PEAP, LEAP, EAP-TLS, EAP-TTLS, and EAP-MD5. If you do not specify the preferred protocol, EAP-TLS is used by default.
EAP-TLS L-bit	Check this check box to support legacy EAP supplicants that expect length-included flag (L-bit flag) by default in TLS Change Cipher Spec message and Encrypted Handshake message from ISE. **Note** Enable this option only for supplicants that require this flag. Windows native supplicant does not support this flag with tunneled EAP protocols; such as PEAP, TEAP or EAP-FAST. If this option is enabled, and supplicant does not support it, and tunneled EAP protocol is being used, ISE will enable this flag in Application Data after establishing TLS tunnel, then supplicant will discard EAP session and will not complete EAP authentication for inner method of the tunnel which will result into a failed authentication with "Endpoint abandoned EAP session and started new" failure reason.

Field Name	Usage Guidelines
Allow Weak Ciphers for EAP	If this option is enabled, legacy clients are allowed to negotiate using weak ciphers (such as RSA_RC4_128_SHA, RSA_RC4_128_MD5). We recommend that you enable this option only if your legacy clients support only weak ciphers. This option is disabled by default. **Note** Cisco ISE does not support EDH_RSA_DES_64_CBC_SHA and EDH_DSS_DES_64_CBC_SHA.
Require Message Authenticator for all RADIUS Requests	If this option is enabled, Cisco ISE verifies whether the RADIUS Message Authenticator attribute is present in the RADIUS message. If the message authenticator attribute is not present, the RADIUS message is discarded. Enabling this option provides protection from spoofed Access-Request messages and RADIUS message tampering. The RADIUS Message Authenticator attribute is a Message Digest 5 (MD5) hash of the entire RADIUS message. **Note** EAP uses the Message Authenticator attribute by default and does not require that you enable it.
Allow 5G	Check this check box to enable Cisco Private 5G in Cisco ISE. **Note** You must already have Cisco Private 5G deployed in your network, prior to enabling 5G as a Service (5GaaS) in Cisco ISE

Related Topics

Allowed Protocols in FIPS and Non-FIPS Modes for TACACS+ Device Administration, on page 467

Define Allowed Protocols for Network Access, on page 1062

PAC Options

The following table describes the fields after you select Use PACs in the **Allowed Protocols Services List** window. To view this window, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Authentication** > **Allowed Protocols**.

Table 153: PAC Options

Field Name	Usage Guidelines
Use PAC	

Field Name	Usage Guidelines
	• Tunnel PAC Time To Live: The Time to Live (TTL) value restricts the lifetime of the PAC. Specify the lifetime value and units. The default is 90 days. The range is between 1 and 1825 days. • Proactive PAC Update When: <n%> of PAC TTL is Left: The Update value ensures that the client has a valid PAC. Cisco ISE initiates an update after the first successful authentication but before the expiration time that is set by the TTL. The update value is a percentage of the remaining time in the TTL. The default is 90%. • Allow Anonymous In-band PAC Provisioning: Check this check box for Cisco ISE to establish a secure anonymous TLS handshake with the client and provision it with a PAC by using phase zero of EAP-FAST with EAP-MSCHAPv2. To enable anonymous PAC provisioning, you must choose both of the inner methods, EAP-MSCHAPv2 and EAP-GTC. • Allow Authenticated In-band PAC Provisioning: Cisco ISE uses SSL server-side authentication to provision the client with a PAC during phase zero of EAP-FAST. This option is more secure than anonymous provisioning but requires that a server certificate and a trusted root CA be installed on Cisco ISE. When you check this option, you can configure Cisco ISE to return an Access-Accept message to the client after successful authenticated PAC provisioning. • Server Returns Access Accept After Authenticated Provisioning: Check this check box if you want Cisco ISE to return an access-accept package after authenticated PAC provisioning. • Allow Machine Authenticatio: Check this check box for Cisco ISE to provision an end-user client with a machine PAC and perform machine authentication (for end-user clients who do not have the machine credentials). The machine PAC can be provisioned to the client by request (in-band) or by the administrator (out-of-band). When Cisco ISE receives a valid machine PAC from the end-user client, the machine identity details are extracted from the PAC and verified in the Cisco ISE external identity source. Cisco ISE only supports Active Directory as an external identity source for machine authentication. After these details are correctly verified, no further authentication is performed. When you check this option, you can enter a value for the amount of time that a machine PAC is acceptable for use. When Cisco ISE receives an expired machine PAC, it automatically reprovisions the end-user client with a new

Field Name	Usage Guidelines
	machine PAC (without waiting for a new machine PAC request from the end-user client). • Enable Stateless Session Resume: Check this check box for Cisco ISE to provision authorization PACs for EAP-FAST clients and skip phase two of EAP-FAST (default = enabled). Uncheck this check box in the following cases: • If you do not want Cisco ISE to provision authorization PACs for EAP-FAST clients • To always perform phase two of EAP-FAST When you check this option, you can enter the authorization period of the user authorization PAC. After this period, the PAC expires. When Cisco ISE receives an expired authorization PAC, it performs phase two EAP-FAST authentication.

Related Topics

OOB TrustSec PAC, on page 1084

Generate the PAC for EAP-FAST, on page 1025

Cisco ISE Acting as a RADIUS Proxy Server

Cisco ISE can function both as a RADIUS server and as a RADIUS proxy server. When it acts as a proxy server, Cisco ISE receives authentication and accounting requests from the network access server (NAS) and forwards them to the external RADIUS server. Cisco ISE accepts the results of the requests and returns them to the NAS.

Cisco ISE can simultaneously act as a proxy server to multiple external RADIUS servers. You can use the external RADIUS servers that you configure here in RADIUS server sequences. The External RADIUS Server page lists all the external RADIUS servers that you have defined in Cisco ISE. You can use the filter option to search for specific RADIUS servers based on the name or description, or both. In both simple and rule-based authentication policies, you can use the RADIUS server sequences to proxy the requests to a RADIUS server.

The RADIUS server sequence strips the domain name from the RADIUS-Username attribute for RADIUS authentications. This domain stripping is not applicable for EAP authentications, which use the EAP-Identity attribute. The RADIUS proxy server obtains the username from the RADIUS-Username attribute and strips it from the character that you specify when you configure the RADIUS server sequence. For EAP authentications, the RADIUS proxy server obtains the username from the EAP-Identity attribute. EAP authentications that use the RADIUS server sequence will succeed only if the EAP-Identity and RADIUS-Username values are the same.

Configure External RADIUS Servers

You must configure the external RADIUS servers in the Cisco ISE to enable it to forward requests to the external RADIUS servers. You can define the timeout period and the number of connection attempts.

Before you begin

- You cannot use the external RADIUS servers that you create in this section by themselves. You must create a RADIUS server sequence and configure it to use the RADIUS server that you create in this section. You can then use the RADIUS server sequence in authentication policies.
- To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **External RADIUS Servers**.

The RADIUS Servers page appears with a list of external RADIUS servers that are defined in Cisco ISE.

Step 2 Click **Add** to add an external RADIUS server.

Step 3 Enter the values as required.

Step 4 Click **Submit** to save the external RADIUS server configuration.

Define RADIUS Server Sequences

RADIUS server sequences in Cisco ISE allow you to proxy requests from a NAD to an external RADIUS server that will process the request and return the result to Cisco ISE, which forwards the response to the NAD.

RADIUS Server Sequences page lists all the RADIUS server sequences that you have defined in Cisco ISE. You can create, edit, or duplicate RADIUS server sequences from this page.

Before you begin

- Before you begin this procedure, you should have a basic understanding of the Proxy Service and must have successfully completed the task in the first entry of the Related Links.
- To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **RADIUS Server Sequences**.

Step 2 Click **Add.**

Step 3 Enter the values as required.

Step 4 Click **Submit** to save the RADIUS server sequence to be used in policies.

Cisco ISE Acting as a TACACS+ Proxy Client

Cisco ISE can act as proxy client to external TACACS+ servers. When it acts as a proxy client, Cisco ISE receives authentication, authorization, and accounting requests from the Network Access Server (NAS) and forwards them to the external TACACS+ server. Cisco ISE accepts the results of the requests and returns them to the NAS.

The TACACS+ External Servers page lists all the external TACACS+ servers that you have defined in Cisco ISE. You can use the filter option to search for specific TACACS+ servers based on the name or description, or both.

Cisco ISE can simultaneously act as a proxy client to multiple external TACACS+ servers. In order to configure multiple external servers, you can use the TACACS+ server sequence page. Refer to the TACACS+ Server Sequence Settings page for more information.

Configure External TACACS+ Servers

You must configure the external TACACS servers in the Cisco ISE to enable it to forward requests to the external TACACS servers. You can define the timeout period and the number of connection attempts.

Before you begin

- You cannot use the external TACACS servers that you create in this section directly in the policy. You must create a TACACS server sequence and configure it to use the TACACS server that you create in this section. You can then use the TACACS server sequence in the policy sets.
- To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Network Resources** > **TACACS External Servers**.
The **TACACS External Servers** page appears with a list of external TACACS servers that are defined in Cisco ISE.

Step 2 Click **Add** to add an external TACACS server.

Step 3 Enter the values as required.

Step 4 Click **Submit** to save the external TACACS server configuration.

TACACS+ External Server Settings

The following table describes the fields in the TACACS External Servers page. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Network Resources** > **TACACS External Servers** page.

Table 154: TACACS+ External Server Settings

Fields	Usage Guidelines
Name	Enter the name of the TACACS+ external server.
Description	Enter a description for the TACACS+ external server setting.
Host IP	Enter the IP address (IPv4 or IPv6 address) of the remote TACACS+ external server.
Connection Port	Enter the port number of the remote TACACS+ external server. The port number is 49.

Fields	Usage Guidelines
Timeout	Specify the number of seconds that ISE should wait for a response from the external TACACS+ server. The default is 5 seconds. Valid values are from 1 to 120.
Shared Secret	A string of text that is used to secure a connection with the TACACS+ External Server. The connection will be rejected by the TACACS+ External server if this is not configured correctly.
Use Single Connect	The TACACS protocol supports two modes for associating sessions to connections: Single Connect and Non-Single Connect. Single connect mode reuses a single TCP connection for many TACACS+ sessions that a client may initiate. Non-Single Connect opens a new TCP connection for every TACACS+ session that a client initiates. The TCP connection is closed after each session. You can check the Use Single Connect check box for high-traffic environment and uncheck it for low-traffic environment.

Define TACACS+ Server Sequences

TACACS+ server sequences in Cisco ISE allow you to proxy requests from a NAD to an external TACACS+ server that will process the request and return the result to Cisco ISE, which forwards the response to the NAD. The TACACS+ Server Sequences page lists all the TACACS+ server sequences that you have defined in Cisco ISE. You can create, edit, or duplicate TACACS+ server sequences from this page.

Before you begin

- You should have a basic understanding of the Proxy Service, Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions.
- To perform the following task, you must be a Super Admin or System Admin.
- Ensure that the external TACACS+ servers that you intend to use in the TACACS+ server sequence are already defined.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Network Resources** > **TACACS External Server Sequence**.

Step 2 Click **Add**.

Step 3 Enter the required values.

Step 4 Click **Submit** to save the TACACS+ server sequence to be used in policies.

TACACS+ Server Sequence Settings

The following table describes the fields in the TACACS Server Sequence page. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Network Resources** > **TACACS Server Sequence** page.

Table 155: TACACS+ Server Sequence Settings

Fields	**Usage Guidelines**
Name	Enter the name of the TACACS proxy server sequence.
Description	Enter a description for the TACACS proxy server sequence.
Server List	Select the required TACACS proxy servers from the Available list. The available list contains the list of TACACS proxy servers configured in the TACACS External Services Page.
Logging Control	Check to enable logging control: • Local Accounting: Accounting messages are logged by the server that handles requests from devices. • Remote Accounting: Accounting messages are logged by the proxy server that handles requests from devices.
Username Stripping	Username Prefix/Suffix Stripping: • Prefix Strip: Check to strip the username from the prefix. For example, if the subject name is acme\smith and the separator is \, the username becomes smith. The default separator is \. • Suffix Strip: Check to strip the username from the suffix. For example, if the subject name is smith@acme.com and the separator is @, the username becomes smith. The default separator is @.

Network Access Service

A network access service contains the authentication policy conditions for requests. You can create separate network access services for different use cases, for example, Wired 802.1X, Wired MAB, and so on. To create a network access service, configure allowed protocols or server sequences. The network access service for network access policies is then configured from the Policy Sets page.

Define Allowed Protocols for Network Access

Allowed protocols define the set of protocols that Cisco ISE can use to communicate with the device that requests access to the network resources. An allowed protocols access service is an independent entity that you should create before you configure authentication policies. Allowed protocols access service is an object that contains your chosen protocols for a particular use case.

The Allowed Protocols Services page lists all the allowed protocols services that you create. There is a default network access service that is predefined in the Cisco ISE.

Before you begin

Before you begin this procedure, you should have a basic understanding of the protocol services that are used for authentication.

- Review the Cisco ISE Authentication Policies section in this chapter to understand authentication type and the protocols that are supported by various databases.
- Review the PAC Options to understand the functions and options for each protocol service, so you can make the selections that are appropriate for your network.
- Ensure that you have defined the global protocol settings.

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **Authentication** > **Allowed Protocols**.

If Cisco ISE is set to operate in FIPS mode, some protocols are disabled by default and cannot be configured.

Step 2 Click **Add**.

Step 3 Enter the required information.

Step 4 Select the appropriate authentication protocols and options for your network.

Step 5 If you choose to use PACs, make the appropriate selections.

To enable Anonymous PAC Provisioning, you must choose both the inner methods, EAP-MSCHAPv2 and Extensible Authentication Protocol-Generic Token Card (EAP-GTC). Also, be aware that Cisco ISE only supports Active Directory as an external identity source for machine authentication.

Step 6 Click **Submit** to save the allowed protocols service.

The allowed protocols service appears as an independent object in the simple and rule-based authentication policy pages. You can use this object in different rules.

You can now create a simple or rule-based authentication policy.

If you disable EAP-MSCHAP as inner method and enable EAP-GTC and EAP-TLS inner methods for PEAP or EAP-FAST, ISE starts EAP-GTC inner method during inner method negotiation. Before the first EAP-GTC message is sent to the client, ISE executes identity selection policy to obtain GTC password from the identity store. During the execution of this policy, EAP authentication is equal to EAP-GTC. If EAP-GTC inner method is rejected by the client and EAP-TLS is negotiated, identity store policy is not executed again. In case identity store policy is based on EAP authentication attribute, it might have unexpected results since the real EAP authentication is EAP-TLS but was set after identity policy evaluation.

Network Access for Users

For network access, a host connects to the network device and requests to use network resources. The network device identifies the newly connected host, and, using the RADIUS protocol as a transport mechanism, requests Cisco ISE to authenticate and authorize the user.

Cisco ISE supports network access flows depending on the protocol that is transported over the RADIUS protocol.

RADIUS-Based Protocols Without EAP

RADIUS-based protocols that do not include EAP include the following:

- Password Authentication Protocol (PAP)
- CHAP
- Microsoft Challenge Handshake Authentication Protocol version 1 (MS-CHAPv1)
- MS-CHAP version 2 (MS-CHAPv2)

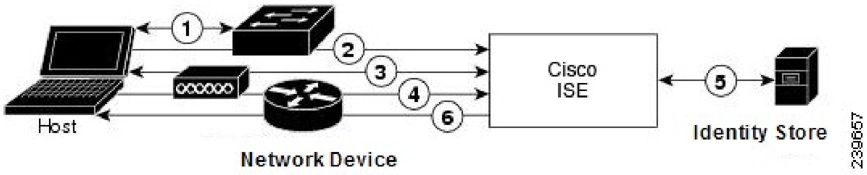
RADIUS-Based Non-EAP Authentication Flow

This section describes RADIUS-based flow without EAP authentication. RADIUS-based flow with PAP authentication occurs in the following process:

1. A host connects to a network device.
2. The network device sends a RADIUS request (Access-Request) to Cisco ISE that contains RADIUS attributes that are appropriate to the specific protocol that is being used (PAP, CHAP, MS-CHAPv1, or MS-CHAPv2).
3. Cisco ISE uses an identity store to validate user credentials.
4. A RADIUS response (Access-Accept or Access-Reject) is sent to the network device that will apply the decision.

The following figure shows a RADIUS-based authentication without EAP.

Figure 45: RADIUS-Based Authentication Without EAP



The non-EAP protocols supported by Cisco ISE are:

Password Authentication Protocol

PAP provides a simple method for users to establish their identity by using a two-way handshake. The PAP password is encrypted with a shared secret and is the least sophisticated authentication protocol. PAP is not a strong authentication method because it offers little protection from repeated trial-and-error attacks.

RADIUS-Based PAP Authentication in Cisco ISE

Cisco ISE checks the username and password pair against the identity stores, until it eventually acknowledges the authentication or terminates the connection.

You can use different levels of security concurrently with Cisco ISE for different requirements. PAP applies a two-way handshaking procedure. If authentication succeeds, Cisco ISE returns an acknowledgment; otherwise, Cisco ISE terminates the connection or gives the originator another chance.

The originator is in total control of the frequency and timing of the attempts. Therefore, any server that can use a stronger authentication method will offer to negotiate that method prior to PAP. RFC 1334 defines PAP.

Cisco ISE supports standard RADIUS PAP authentication that is based on the RADIUS UserPassword attribute. RADIUS PAP authentication is compatible with all identity stores.

The RADIUS-with-PAP-authentication flow includes logging of passed and failed attempts.

Challenge Handshake Authentication Protocol

CHAP uses a challenge-response mechanism with one-way encryption on the response. CHAP enables Cisco ISE to negotiate downward from the most-secure to the least-secure encryption mechanism, and it protects passwords that are transmitted in the process. CHAP passwords are reusable. If you are using the Cisco ISE internal database for authentication, you can use PAP or CHAP. CHAP does not work with the Microsoft user database. Compared to RADIUS PAP, CHAP allows a higher level of security for encrypting passwords when communicating from an end-user client to the AAA client.

Cisco ISE supports standard RADIUS CHAP authentication that is based on the RADIUS ChapPassword attribute. Cisco ISE supports RADIUS CHAP authentication only with internal identity stores.

Microsoft Challenge Handshake Authentication Protocol Version 1

Cisco ISE supports the RADIUS MS-CHAPv1 authentication and change-password features. RADIUS MS-CHAPv1 contains two versions of the change-password feature: Change-Password-V1 and Change-Password-V2.Cisco ISE does not support Change-Password-V1 based on the RADIUS MS-CHAP-CPW-1 attribute, and supports only Change-Password-V2 based on the MS-CHAP-CPW-2 attribute.The RADIUS MS-CHAPv1 authentication and change-password features are supported with the following identity sources:

- Internal identity stores
- Microsoft Active Directory identity store

Microsoft Challenge Handshake Authentication Protocol Version 2

The RADIUS MS-CHAPv2 authentication and change-password features are supported with the following identity sources:

- Internal identity stores
- Microsoft Active Directory identity store

RADIUS-Based EAP Protocols

EAP provides an extensible framework that supports various authentication types. This section describes the EAP methods supported by Cisco ISE and contains the following topics:

Simple EAP Methods

- EAP-Message Digest 5
- Lightweight EAP

EAP Methods That Use Cisco ISE Server Certificate for Authentication

- PEAP/EAP-MS-CHAPv2
- PEAP/EAP-GTC
- EAP-FAST/EAP-MS-CHAPv2
- EAP-FAST/EAP-GTC

Apart from the methods listed above, there are EAP methods that use certificates for both server and client authentication.

RADIUS-Based EAP Authentication Flow

Whenever EAP is involved in the authentication process, the process is preceded by an EAP negotiation phase to determine which specific EAP method (and inner method, if applicable) should be used. EAP-based authentication occurs in the following process:

1. A host connects to a network device.
2. The network device sends an EAP Request to the host.
3. The host replies with an EAP Response to the network device.
4. The network device encapsulates the EAP Response that it received from the host into a RADIUS Access-Request (using the EAP-Message RADIUS attribute) and sends the RADIUS Access-Request to Cisco ISE.
5. Cisco ISE extracts the EAP Response from the RADIUS packet and creates a new EAP Request, encapsulates it into a RADIUS Access-Challenge (again, using the EAP-Message RADIUS attribute), and sends it to the network device.
6. The network device extracts the EAP Request and sends it to the host.

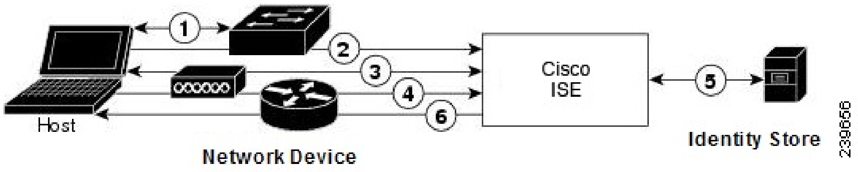
In this way, the host and Cisco ISE indirectly exchange EAP messages (transported over RADIUS and passed through the network device). The initial set of EAP messages that are exchanged in this manner negotiate the specific EAP method that will subsequently be used to perform the authentication.

The EAP messages that are subsequently exchanged are then used to carry the data that is needed to perform the actual authentication. If it is required by the specific EAP authentication method that is negotiated, Cisco ISE uses an identity store to validate user credentials.

After Cisco ISE determines whether the authentication should pass or fail, it sends either an EAP-Success or EAP-Failure message, encapsulated into a RADIUS Access-Accept or Access-Reject message to the network device (and ultimately also to the host).

The following figure shows a RADIUS-based authentication with EAP.

Figure 46: RADIUS-Based Authentication with EAP



Extensible Authentication Protocol-Message Digest 5

Extensible Authentication Protocol-Message Digest 5 (EAP-MD5) provides one-way client authentication. The server sends the client a random challenge. The client proves its identity in a response by encrypting the challenge and its password with MD5. Because a man in the middle could see the challenge and response, EAP-MD5 is vulnerable to dictionary attack when used over an open medium. Because no server authentication occurs, it is also vulnerable to spoofing. Cisco ISE supports EAP-MD5 authentication against the Cisco ISE internal identity store. Host Lookup is also supported when using the EAP-MD5 protocol.

Lightweight Extensible Authentication Protocol

Cisco ISE currently uses Lightweight Extensible Authentication Protocol (LEAP) only for Cisco Aironet wireless networking. If you do not enable this option, Cisco Aironet end-user clients who are configured to perform LEAP authentication cannot access the network. If all Cisco Aironet end-user clients use a different authentication protocol, such as Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), we recommend that you disable this option.

Note If users access your network by using a AAA client that is defined in the *Network Devices* section as a RADIUS (Cisco Aironet) device, then you must enable LEAP, EAP-TLS, or both; otherwise, Cisco Aironet users cannot authenticate.

Protected Extensible Authentication Protocol

Protected Extensible Authentication Protocol (PEAP) provides mutual authentication, ensures confidentiality and integrity to vulnerable user credentials, protects itself against passive (eavesdropping) and active (man-in-the-middle) attacks, and securely generates cryptographic keying material. PEAP is compatible with the IEEE 802.1X standard and RADIUS protocol. Cisco ISE supports PEAP version 0 (PEAPv0) and PEAP version 1 (PEAPv1) with Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol (EAP-MS-CHAP), Extensible Authentication Protocol-Generic Token Card (EAP-GTC), and EAP-TLS inner methods. The Cisco Secure Services Client (SSC) supplicant supports all of the PEAPv1 inner methods that Cisco ISE supports.

Advantages of Using PEAP

Using PEAP presents these advantages: PEAP is based on TLS, which is widely implemented and has undergone extensive security review. It establishes a key for methods that do not derive keys. It sends an identity within the tunnel. It protects inner method exchanges and the result message. It supports fragmentation.

Supported Supplicants for the PEAP Protocol

PEAP supports these supplicants:

- Microsoft Built-In Clients 802.1X XP

- Microsoft Built-In Clients 802.1X Vista
- Cisco Secure Services Client (SSC), Release 4.0
- Cisco SSC, Release 5.1
- Funk Odyssey Access Client, Release 4.72
- Intel, Release 12.4.0.0

PEAP Protocol Flow

A PEAP conversation can be divided into three parts:

1. Cisco ISE and the peer build a TLS tunnel. Cisco ISE presents its certificate, but the peer does not. The peer and Cisco ISE create a key to encrypt the data inside the tunnel.
2. The inner method determines the flow within the tunnel:
    - EAP-MS-CHAPv2 inner method—EAP-MS-CHAPv2 packets travel inside the tunnel without their headers. The first byte of the header contains the type field. EAP-MS-CHAPv2 inner methods support the change-password feature. You can configure the number of times that the user can attempt to change the password through the Admin portal. User authentication attempts are limited by this number.
    - EAP-GTC inner method—Both PEAPv0 and PEAPv1 support the EAP-GTC inner method. The supported supplicants do not support PEAPv0 with the EAP-GTC inner method. EAP-GTC supports the change-password feature. You can configure the number of times that the user can attempt to change the password through the Admin portal. User authentication attempts are limited by this number.
    - EAP-TLS inner method—The Windows built-in supplicant does not support fragmentation of messages after the tunnel is established, and this affects the EAP-TLS inner method. Cisco ISE does not support fragmentation of the outer PEAP message after the tunnel is established. During tunnel establishment, fragmentation works as specified in PEAP documentation. In PEAPv0, EAP-TLS packet headers are removed, and in PEAPv1, EAP-TLS packets are transmitted unchanged.
    - Extensible Authentication Protocol-type, length, value (EAP-TLV) extension—EAP-TLV packets are transmitted unchanged. EAP-TLV packets travel with their headers inside the tunnel.
3. There is protected acknowledgment of success and failure if the conversation has reached the inner method.

    The client EAP message is always carried in the RADIUS Access-Request message, and the server EAP message is always carried in the RADIUS Access-Challenge message. The EAP-Success message is always carried in the RADIUS Access-Accept message. The EAP-Failure message is always carried in the RADIUS Access-Reject message. Dropping the client PEAP message results in dropping the RADIUS client message.

Note Cisco ISE requires acknowledgment of the EAP-Success or EAP-Failure message during PEAPv1 communication. The peer must send back a PEAP packet with empty TLS data field to acknowledge the receipt of success or failure message.

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) is an authentication protocol that provides mutual authentication and uses a shared secret to establish a tunnel. The tunnel is used to protect weak authentication methods that are based on passwords. The shared secret, referred to as a Protected Access Credentials (PAC) key, is used to mutually authenticate the client and server while securing the tunnel.

Benefits of EAP-FAST

EAP-FAST provides the following benefits over other authentication protocols:

- Mutual authentication—The EAP server must be able to verify the identity and authenticity of the peer, and the peer must be able to verify the authenticity of the EAP server.
- Immunity to passive dictionary attacks—Many authentication protocols require a password to be explicitly provided, either as cleartext or hashed, by the peer to the EAP server.
- Immunity to man-in-the-middle attacks—In establishing a mutually authenticated protected tunnel, the protocol must prevent adversaries from successfully interjecting information into the conversation between the peer and the EAP server.
- Flexibility to enable support for many different password authentication interfaces such as MS-CHAPv2, Generic Token Card (GTC), and others—EAP-FAST is an extensible framework that allows support of multiple internal protocols by the same server.
- Efficiency—When using wireless media, peers are limited in computational and power resources. EAP-FAST enables the network access communication to be computationally lightweight.
- Minimization of the per-user authentication state requirements of the authentication server—With large deployments, it is typical to have many servers acting as the authentication servers for many peers. It is also highly desirable for a peer to use the same shared secret to secure a tunnel much the same way that it uses the username and password to gain access to the network. EAP-FAST facilitates the use of a single, strong, shared secret by the peer, while enabling servers to minimize the per-user and device state that it must cache and manage.

EAP-FAST Flow

The EAP-FAST protocol flow is always a combination of the following phases:

1. Provisioning phase—This is phase zero of EAP-FAST. During this phase, the peer is provisioned with a unique, strong secret that is referred to as the PAC that is shared between the Cisco ISE and the peer.
2. Tunnel establishment phase—The client and server authenticate each other by using the PAC to establish a fresh tunnel key. The tunnel key is then used to protect the rest of the conversation and provides message confidentiality and with authenticity.
3. Authentication phase—The authentication is processed inside the tunnel and includes the generation of session keys and protected termination.Cisco ISE supports EAP-FAST versions 1 and 1a.

Enable MAB from Non-Cisco Devices

Configure the following settings sequentially to configure MAB from non-Cisco devices.

Step 1 Ensure that the MAC address of the endpoints that are to be authenticated are available in the Endpoints database. You can add these endpoints or have them profiled automatically by the Profiler service.

Step 2 Create a Network Device Profile based on the type of MAC authentication used by the non-Cisco device (PAP, CHAP, or EAP-MD5).

a) Choose **Administration > Network Resources > Network Device Profiles**.

b) Click **Add**.

c) Enter a name and description for the network device profile.
d) Select the vendor name from the **Vendor** drop-down list.
e) Check the check boxes for the protocols that the device supports. If the device supports RADIUS, select the RADIUS dictionary to use with the network device.
f) Expand the **Authentication/Authorization** section to configure the device's default settings for flow types, attribute aliasing, and host lookup.
g) In the **Host Lookup (MAB)** section, do the following:

   - Process Host Lookup—Check this check box to define the protocols for host lookup used by the network device profile.

     Network devices from different vendors perform MAB authentication differently. Depending on the device type, check the **Check Password** check box and/or **Check Calling-Station-Id equals MAC Address** check box, for the protocol you are using.

   - Via PAP/ASCII—Check this check box to configure Cisco ISE to detect a PAP request from the network device profile as a Host Lookup request.

   - Via CHAP—Check this check box to configure Cisco ISE to detect this type of request from the network devices as a Host Lookup request.

   - Via EAP-MD5—Check this check box to enable EAP-based MD5 hashed authentication for the network device profile.

h) Enter the required details in the Permissions, Change of Authorization (CoA), and Redirect sections, and then click **Submit**.

   For information on how to create custom NAD profiles, see Network Access Device Profiles with Cisco Identity Services Engine.

Step 3 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration > Network Resources > Network Devices**.

Step 4 Select the device for which you want to enable MAB, and then click **Edit**.

Step 5 In the Network Device page, select the network device profile that you created in step 2 from the **Device Profile** drop-down list.

Step 6 Click **Save**.

Note For Cisco NADs, the Service-Type values used for MAB and web/user authentication are different. This allows ISE to differentiate MAB from web authentication when Cisco NADs are used. Some non-Cisco NADs use the same value for the Service-Type attribute for both MAB and web/user authentication; this may lead to security issues in your access policies. If you are using MAB with non-Cisco devices, we recommend that you configure additional authorization policy rules to ensure that your network security is not compromised. For example, if a printer is using MAB, you could configure an authorization policy rule to restrict it to printer protocol ports in the ACL.

Enable MAB from Cisco Devices

Configure the following settings sequentially to configure MAB from Cisco devices.

Step 1 Ensure that the MAC address of the endpoints that are to be authenticated are available in the Endpoints database. You can add these endpoints or have them profiled automatically by the Profiler service.

Step 2 Create a Network Device Profile based on the type of MAC authentication used by the Cisco device (PAP, CHAP, or EAP-MD5).

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Device Profiles**.
b) Click **Add**.
c) Enter a name and description for the network device profile.
d) Check the check boxes for the protocols that the device supports. If the device supports RADIUS, select the RADIUS dictionary to use with the network device.
e) Expand the **Authentication/Authorization** section to configure the device's default settings for flow types, attribute aliasing, and host lookup.
f) In the **Host Lookup (MAB)** section, do the following:

    - Process Host Lookup—Check this check box to define the protocols for host lookup used by the network device profile.

      Depending on the device type, check the **Check Password** check box and/or **Check Calling-Station-Id equals MAC Address** check box, for the protocol you are using.

    - Via PAP/ASCII—Check this check box to configure Cisco ISE to detect a PAP request from the network device profile as a Host Lookup request.

    - Via CHAP—Check this check box to configure Cisco ISE to detect this type of request from the network devices as a Host Lookup request.

    - Via EAP-MD5—Check this check box to enable EAP-based MD5 hashed authentication for the network device profile.

g) Enter the required details in the Permissions, Change of Authorization (CoA), and Redirect sections, and then click **Submit**.

   For information on how to create custom NAD profiles, see Network Access Device Profiles with Cisco Identity Services Engine.

Step 3 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Devices**.

Step 4 Select the device for which you want to enable MAB, and then click **Edit**.

Step 5 In the Network Device page, select the network device profile that you created in step 2 from the **Device Profile** drop-down list.

Step 6 Click **Save**.

ISE Community Resource

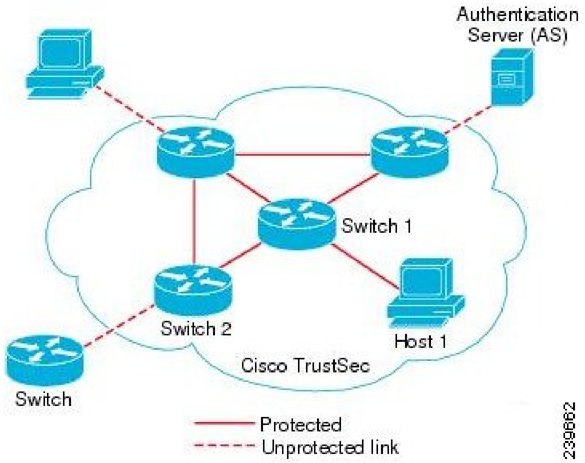
For information about IP phone authentication capabilities, see Phone Authentication Capabilities.

TrustSec Architecture

The Cisco TrustSec solution establishes clouds of trusted network devices to build secure networks. Each device in the Cisco TrustSec cloud is authenticated by its neighbors (peers). Communication between the devices in the TrustSec cloud is secured with a combination of encryption, message integrity checks, and data-path replay protection mechanisms. The TrustSec solution uses the device and user identity information that it obtains during authentication to classify, or color, the packets as they enter the network. This packet classification is maintained by tagging packets when they enter the TrustSec network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path. The tag, also called the security group tag (SGT), allows Cisco ISE to enforce access control policies by enabling the endpoint device to act upon the SGT to filter traffic.

The following figure shows an example of a TrustSec network cloud.

Figure 47: TrustSec Architecture



ISE Community Resource

For information on how to simplify network segmentation and improve security using Cisco TrustSec, see Simplify Network Segmentation with Cisco TrustSec and Policy-Based Software Defined Segmentation and Cisco TrustSec Improve Security White Paper.

For a complete list of Cisco TrustSec platform support matrices, see Cisco TrustSec Platform Support Matrix.

For a complete list of support documentation available for TrustSec, see Cisco TrustSec.

For a complete list of TrustSec community resources, see TrustSec Community.

TrustSec Components

The key TrustSec components include:

- Network Device Admission Control (NDAC)—In a trusted network, during authentication, each network device (for example Ethernet switch) in a TrustSec cloud is verified for its credential and trustworthiness by its peer device. NDAC uses the IEEE 802.1X port-based authentication and uses Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) as its Extensible Authentication Protocol (EAP) method. Successful authentication and authorization in the NDAC process results in Security Association Protocol negotiation for IEEE 802.1AE encryption. Cisco ISE has CTS Provisioning (EAP-FAST) TLSv1.2 support for switching platforms starting IOSXE 17.1, and for routing platforms starting IOSXE 17.6.

- Endpoint Admission Control (EAC)—An authentication process for an endpoint user or a device connecting to the TrustSec cloud. EAC typically happens at the access level switch. Successful authentication and authorization in EAC process results in SGT assignment to the user or device. EAC access methods for authentication and authorization includes:
  - 802.1X port-based authentication
  - MAC authentication bypass (MAB)
  - Web authentication (WebAuth)
- Security Group (SG)—A grouping of users, endpoint devices, and resources that share access control policies. SGs are defined by the administrator in Cisco ISE. As new users and devices are added to the TrustSec domain, Cisco ISE assigns these new entities to the appropriate security groups.
- Security Group Tag (SGT)—TrustSec service assigns to each security group a unique 16-bit security group number whose scope is global within a TrustSec domain. The number of security groups in the switch is limited to the number of authenticated network entities. You do not have to manually configure security group numbers. They are automatically generated, but you have the option to reserve a range of SGTs for IP-to-SGT mapping.
- Security Group Access Control List (SGACL)—SGACLs allow you to control the access and permissions based on the SGTs that are assigned. The grouping of permissions into a role simplifies the management of security policy. As you add devices, you simply assign one or more security groups, and they immediately receive the appropriate permissions. You can modify the security groups to introduce new privileges or restrict current permissions.
- Security Exchange Protocol (SXP)—SGT Exchange Protocol (SXP) is a protocol developed for TrustSec service to propagate the IP-SGT bindings across network devices that do not have SGT-capable hardware support to hardware that supports SGT/SGACL.
- Environment Data Download—The TrustSec device obtains its environment data from Cisco ISE when it first joins a trusted network. You can also manually configure some of the data on the device. The device must refresh the environment data before it expires. The TrustSec device obtains the following environment data from Cisco ISE:
  - Server lists—List of servers that the client can use for future RADIUS requests (for both authentication and authorization)
  - Device SG—Security group to which the device itself belongs
  - Expiry timeout—Interval that controls how often the TrustSec device should download or refresh its environment data
- Identity-to-Port Mapping—A method for a switch to define the identity on a port to which an endpoint is connected, and to use this identity to look up a particular SGT value in the Cisco ISE server.

TrustSec Terminology

The following table lists some of the common terms that are used in the TrustSec solution and their meaning in an TrustSec environment.

Table 156: TrustSec Terminology

Term	Meaning
Supplicant	A device that tries to join a trusted network.
Authentication	The process of verifying the identity of each device before allowing it to be part of the trusted network.
Authorization	The process of deciding the level of access to a device that requests access to a resource on a trusted network based on the authenticated identity of the device.
Access control	The process of applying access control on a per-packet basis based on the SGT that is assigned to each packet.
Secure communication	The process of encryption, integrity, and data-path replay protection for securing the packets that flow over each link in a trusted network.
TrustSec device	Any of the Cisco Catalyst 6000 Series or Cisco Nexus 7000 Series switches that support the TrustSec solution.
TrustSec-capable device	A TrustSec-capable device will have TrustSec-capable hardware and software. For example, the Nexus 7000 Series Switches with the Nexus operating system.
TrustSec seed device	The TrustSec device that authenticates directly against the Cisco ISE server. It acts as both the authenticator and supplicant.
Ingress	When packets first encounter a TrustSec-capable device that is part of a network where the Cisco TrustSec solution is enabled, they are tagged with an SGT. This point of entry into the trusted network is called the ingress.
Egress	When packets pass the last TrustSec-capable device that is part of a network where the Cisco TrustSec solution is enabled, they are untagged. This point of exit from the trusted network is called the egress.

Supported Switches and Required Components for TrustSec

To set up a Cisco ISE network that is enabled with the Cisco TrustSec solution, you need switches that support the TrustSec solution and other components. Apart from the switches, you also need other components for identity-based user access control using the IEEE 802.1X protocol. For a complete up-to-date list of the Trustsec-supported Cisco switch platforms and the required components, see Cisco TrustSec-Enabled Infrastructure.

Integration with Cisco Catalyst Center

Catalyst Center provides a mechanism to create a trusted communications link with Cisco ISE and to share data with Cisco ISE in a secure manner. After Cisco ISE is registered with Catalyst Center, any device that Catalyst Center discovers, along with relevant configuration and other data, is pushed to Cisco ISE. You can use Catalyst Center to discover devices and then apply both Catalyst Center and Cisco ISE functions to them because these devices will be displayed in both the applications. Catalyst Center and Cisco ISE devices are all uniquely identified by their device names.

Connecting Catalyst Center to Cisco ISE

For information about configuring Catalyst Center for Cisco ISE, see the *Cisco Catalyst Center Installation Guide*.

This section provides additional information about the Cisco ISE configuration for Catalyst Center.

- Passwords: Catalyst Center uses the Cisco ISE admin username and password when it connects to Cisco ISE. For information about system passwords, see Administrative Access to Cisco ISE, on page 25.

Note Catalyst Center versions earlier than 2.2.1.0 used Cisco ISE CLI to perform the initial integration steps. Hence, the Cisco ISE CLI and admin usernames and passwords had to be the same. From Catalyst Center Release 2.2.1.0 onwards, the use of Cisco ISE CLI has been dropped, and hence the Cisco ISE CLI and admin usernames and passwords need not be the same.

- APIs: External RESTful Services (ERS) API service must be enabled in Cisco ISE. Ensure that the **Use CSRF Check for Enhanced Security** option is disabled in Cisco ISE.
- pxGrid: Cisco ISE is a pxGrid controller, and Catalyst Center is a subscriber. Both Cisco ISE and Catalyst Center monitor the TrustSec (SD-Access) content, which contains SGT and SGACL information. Synchronize the system clocks between Cisco ISE and Catalyst Center. For more information about pxGrid in Cisco ISE, see Cisco pxGrid Node, on page 210.

Note Cisco ISE 2.4 and later supports pxGrid 2.0 and pxGrid 1.0. Although pxGrid 2.0 allows up to 4 pxGrid nodes in the Cisco ISE deployment, Catalyst Center does not currently support more than 2 pxGrid nodes.

- Cisco ISE IP Address: The connection between the Cisco ISE PAN and Catalyst Center must be direct. It cannot be through a proxy, a load balancer, or virtual IP address.

  Verify that Cisco ISE is not using a proxy. Otherwise, exclude the Catalyst Center IP from the proxy.

- SXP: Catalyst Center does not require SXP. You may want to enable SXP when you connect Cisco ISE to the Catalyst Center-managed network, so that Cisco ISE can communicate with network devices that don’t have hardware support for TrustSec (SD-Access).

Note When configuring your Cisco ISE deployment to support TrustSec, or when Cisco ISE is integrated with Catalyst Center, do not configure a Policy Service node as SXP-only. SXP is an interface between TrustSec and non-TrustSec devices. It does not communicate with the TrustSec-enabled network devices.

- Certificate for connections to Cisco ISE:
  - The Cisco ISE admin certificate must contain the Cisco ISE IP or FQDN in subject name or SAN.
  - ECDSA is not supported for SSH keys, ISE SSH access, or in certificates for the Catalyst Center and Cisco ISE connection.
  - Selfsigned certificates on Catalyst Center must have the Basic Constraint's extension with cA:TRUE (RFC5280 section-4.2.19).

Note In Catalyst Center releases earlier than 2.2.1.0, there was a requirement to enable SSH. From Catalyst Center Release 2.2.1.0 onwards, the use of SSH been dropped, and hence, there is no need to enable SSH.

TrustSec Dashboard

The TrustSec dashboard is a centralized monitoring tool for the TrustSec network.

The TrustSec dashboard contains the following dashlets:

- **Metrics**: The Metrics dashlet displays statistics about the behavior of the TrustSec network.
- **Active SGT Sessions**: The Active SGT Sessions dashlet displays the SGT sessions that are currently active in the network. The Alarms dashlet displays alarms that are related to the TrustSec sessions.
- **Alarms**
- **NAD / SGT/ACI Quick View**: The Quick View dashlet displays TrustSec-related information for NADs and SGTs.
- **TrustSec Sessions / NAD Activity/ACI endpoint Activity Live Log**: In the Live Log dashlet, click the TrustSec Sessions link to view the active TrustSec sessions. You can also view information about TrustSec protocol data requests and responses from NADs to Cisco ISE.

Metrics

This section displays statistics about the behavior of the TrustSec network. You can select the time frame (for example, past 2 hours, past 2 days, and so on) and the chart type (for example, bars, line, spline).

The latest bar values are displayed on the graphs. It also displays the percentage change from the previous bar. If there is an increase in the bar value, it will be displayed in green with a plus sign. If there is a decrease in the value, it will be displayed in red with a minus sign.

Place your cursor on a bar of a graph to view the time at which the value was calculated and its exact value in the following format: <Value:xxxx Date/Time: xxx>

You can view the following metrics:

SGT sessions	Displays the total number of SGT sessions created during the chosen time frame. **Note** SGT sessions are the user sessions that received an SGT as part of the authorization flow.
SGTs in use	Displays the total number of unique SGTs that were used during the chosen time frame. For example, in one hour, if there were 200 TrustSec sessions, but ISE responded with only 6 types of SGTs in the authorization responses, the graph will display a value 6 for this hour.
Alarms	Displays the total number of alarms and errors that occurred during the chosen time frame. Errors are displayed in red and alarms are displayed in yellow.
NADs in use	Displays the number of unique NADs, which took part in TrustSec authentications during the chosen time frame.

Current Network Status

The middle section of the dashboard displays information about the current status of the TrustSec network. The values displayed in the graphs are updated when the page is loaded and can be refreshed by using the Refresh Dashboard option.

Active SGT Sessions

This dashlet displays the SGT sessions that are currently active in the network. You can view the top 10 most used or least used SGTs. The X-axis shows the SGT usage and the Y-axis displays the names of the SGTs.

To view the TrustSec session details for an SGT, click on the bar corresponding to that SGT. The details of the TrustSec sessions related to that SGT are displayed in the Live Log dashlet.

Alarms

This dashlet displays the alarms related to the TrustSec sessions. You can view the following details:

- Alarm Severity—Displays an icon that represents the severity level of the alarm.
  - High—Includes the alarms that indicate failure in the TrustSec network (for example, device failed to refresh its PAC). Marked with red icon.

  - Medium—Includes warnings that indicate wrong configuration of the network device (for example, device failed to accept CoA message). Marked with yellow.
  - Low—Includes general information and update on network behavior (for example, configuration changes in TrustSec). Marked with blue.
- Alarm description
- Number of times the alarm occurred since this alarm counter was last reset.
- Alarm last occurrence time

Quick View

The Quick View dashlet displays TrustSec-related information for NADs. You can also view the TrustSec-related information for an SGT.

NAD Quick View

Enter the name of the TrustSec network device for which you want to view the details in the Search box and press **Enter**. The search box provides an autocomplete feature, which filters and shows the matched device names in a drop-down as the user types into the text box.

The following information is displayed in this dashlet:

- **NDGs**: Lists the Network Device Groups (NDGs) to which this network device belongs.
- **IP Address**: Displays the IP address of the network device Click on this link to view the NAD activity details in the Live Logs dashlet.
- **Active sessions**: Lists the number of active TrustSec sessions connected to this device.
- **PAC expiry**: Displays the PAC expiry date.
- **Last Policy Refresh**: Displays the policy last download date.
- **Last Authentication**: Displays the last authentication report timestamp for this device.
- **Active SGTs**: Lists the SGTs used in the active sessions that are related to this network device. The number displayed within the brackets denotes the number of sessions that are currently using this SGT. Click on an SGT link to view the TrustSec session details in the Live Log dashlet.

You can use the Show Latest Logs option to view the NAD activity live logs for the device.

SGT Quick View

Enter the name of the SGT for which you want to view the details in the Search box and press **Enter**.

The following information is displayed in this dashlet:

- **Value**: Displays the SGT value (both decimal and hexadecimal).
- **Icon**: Displays the icon that is assigned to this SGT.
- **Active sessions**: Lists the number of active sessions that are currently using this SGT.
- **Unique users**: Lists the number of unique usernames, which hold this SGT in their active sessions.

- **Updated NADs**: Lists the number of NADs which downloaded policies for this SGT.

ACI Quick View

The following information is displayed in this dashlet:

- **SDA SGTs**: Lists the number of SGTs sent by Cisco ISE to Cisco SD-Access.
- **ACI EPGs**: Lists the number of EPGs learnt by Cisco ISE from Cisco ACI.
- **SDA Bindings**: Lists the number of bindings sent by Cisco ISE to Cisco SD-Access.
- **ACI Bindings**: Lists the number of bindings learnt by Cisco ISE from Cisco ACI.
- **SDA VNs**: Lists the number of virtual networks learnt by Cisco ISE from Cisco SD-Access.
- **ACI VNs**: Lists the number of virtual networks learnt by Cisco ISE from Cisco ACI.
- **SDA Extended VNs**: Lists the number of extended virtual networks sent from the Cisco SD-Access domain to the Cisco ACI Domain.
- **SDA Tenant**: Displays the name of the tenant shared by Cisco SD-Access with Cisco ISE.
- **ACI Tenants**: Lists the number of tenants shared with Cisco SD-Access by Cisco ACI.
- **SDA Domain ID**: Displays the domain ID number of Cisco SD-Access.
- **ACI Domain ID**: Displays the domain ID number of Cisco ACI.
- **Peering State**: Displays the current state of the peering relation between the Cisco SD-Access domain and the Cisco ACI Domain.

To know more about Cisco Software-Defined Access (Cisco SD-Access) and Cisco Application Centric Infrastructure (Cisco ACI), see Connect Cisco Application Centric Infrastructure with Cisco ISE, on page 1124 and Cisco ACI and Cisco SD-Access Integration with Virtual Network Awareness, on page 1127.

Live Log

Click the **TrustSec Sessions** link to view the active TrustSec sessions (sessions that have SGT as part of their response).

Click the **NAD Activity** link to view information regarding TrustSec protocol data requests and responses from NADs to Cisco ISE.

Click the **ACI endpoint Activity** link to view the IP-SGT information learnt by Cisco ISE from Cisco ACI.

Configure TrustSec Global Settings

For Cisco ISE to function as an TrustSec server and provide TrustSec services, you must define some global TrustSec settings.

Before you begin

- Before you configure global TrustSec settings, ensure that you have defined global EAP-FAST settings (choose **Administration** > **System** > **Settings** > **Protocols** > **EAP-FAST** > **EAP-FAST Settings**).

You may change the Authority Identity Info Description to your Cisco ISE server name. This description is a user-friendly string that describes the Cisco ISE server that sends credentials to an endpoint client. The client in a Cisco TrustSec architecture can be either the endpoint running EAP-FAST as its EAP method for IEEE 802.1X authentication or the supplicant network device performing Network Device Access Control (NDAC). The client can discover this string in the protected access credentials (PAC) type-length-value (TLV) information. The default value is Identity Services Engine. You should change the value so that the Cisco ISE PAC information can be uniquely identified on network devices upon NDAC authentication.

- To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Settings** > **General TrustSec Settings**

Step 2 Enter the values in the fields. For information about the fields, see General TrustSec Settings, on page 1079

Step 3 Click **Save**.

What to do next

- Configure TrustSec Devices, on page 1084

General TrustSec Settings

Define the global TrustSec settings for Cisco ISE to function as a TrustSec server and provide TrustSec services. To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Settings** > **General TrustSec Settings**.

Verify Trustsec Deployment

This option helps you to verify that the latest TrustSec policies are deployed on all network devices. Alarms are displayed in the Alarms dashlet, under **Work Centers** > **TrustSec** > **Dashboard and Home** > **Summary**, if there are any discrepancies between the policies configured on Cisco ISE and on the network device. The following alarms are displayed in the TrustSec dashboard:

- An alarm displays with an **Info** icon whenever the verification process starts or completes.
- An alarm displays with an **Info** icon if the verification process was cancelled due to a new deployment request.
- An alarm displays with a **Warning** icon if the verification process fails with an error. For example, failure to open the SSH connection with the network device, or if the network device is unavailable, or if there is any discrepancy between the policies configured on Cisco ISE and on the network device.

The **Verify Deployment** option is also available from the below windows. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose:

- **Work Centers** > **TrustSec** > **Components** > **Security Groups**
- **Work Centers** > **TrustSec** > **Components** > **Security Group ACLs**
- **Work Centers** > **TrustSec** > **TrustSec Policy** > **Egress Policy** > **Matrix**

- **Work Centers > TrustSec > TrustSec Policy > Egress Policy > Source Tree**
- **Work Centers > TrustSec > TrustSec Policy > Egress Policy > Destination Tree**

Automatic Verification After Every Deploy: Check this check box if you want Cisco ISE to verify the updates on all the network devices after every deployment. When the deployment process is complete, the verification process starts after the time you specify in the **Time after Deploy Process** field.

Time After Deploy Process: Specify the time for which you want Cisco ISE to wait for after the deployment process is complete, before starting the verification process. The valid range is 10–60 minutes.

The current verification process is cancelled if a new deployment request is received during the waiting period or if another verification is in progress.

Verify Now: Click this option to start the verification process immediately.

Protected Access Credential (PAC)

- **Tunnel PAC Time to Live** :

  Specify the expiry time for the PAC. The tunnel PAC generates a tunnel for the EAP-FAST protocol. You can specify the time in seconds, minutes, hours, days, or weeks. The default value is 90 days. The following are the valid ranges:

  - 1–157680000 seconds
  - 1–2628000 minutes
  - 1–43800 hours
  - 1–1825 days
  - 1–260 weeks

- **Proactive PAC Update Will Occur After**: Cisco ISE proactively provides a new PAC to a client after successful authentication when a configured percentage of the Tunnel PAC TTL remains. The server starts the tunnel PAC update if the first successful authentication occurs before the PAC expires. This mechanism updates the client with a valid PAC. The default value is 10%.

Security Group Tag Numbering

- **System will Assign SGT Numbers**: Choose this option if you want Cisco ISE to automatically generate the SGT numbers.
- **Except Numbers in Range**: Choose this option to reserve a range of SGT numbers for manual configuration. Cisco ISE will not use the values in this range while generating the SGTs.
- **User Must Enter SGT Numbers Manually**: Choose this option to define the SGT numbers manually.

Security Group Tag Numbering for APIC EPGs

Security Group Tag Numbering for APIC EPGs : Check this check box and specify the range of numbers to be used for the SGTs created based on the EPGs learnt from APIC.

Automatic Security Group Creation

Auto Create Security Groups When Creating Authorization Rules: Check this check box to create the SGTs automatically while creating the authorization policy rules.

If you select this option, the following message displays at the top of the **Authorization Policy** window: `Auto Security Group Creation is On`

The autocreated SGTs are named based on the rule attributes.

Note The autocreated SGTs are not deleted if you delete the corresponding authorization policy rule.

By default, this option is disabled after a fresh install or upgrade.

- **Automatic Naming Options**: Use this option to define the naming convention for the autocreated SGTs.

  (Mandatory) **Name Will Include**: Choose one of the following options:

  - **Rule name**
  - **SGT number**
  - **Rule name and SGT number**

  By default, the **Rule name** option is selected.

  Optionally, you can add the following information to the SGT name:

  - **Policy Set Name** (this option is available only if **Policy Sets** are enabled)
  - **Prefix** (up to 8 characters)
  - **Suffix** (up to 8 characters)

  Cisco ISE displays a sample SGT name in the **Example Name** field, based on your selections.

  If an SGT exists with the same name, ISE appends *_x* to the SGT name, where *x* is the first value, starting with 1 (if 1 is not used in the current name). If the new name is longer than 32 characters, Cisco ISE truncate its to the first 32 characters.

IP SGT static mapping of hostnames

IP SGT Static Mapping of Hostnames: If you use FQDN and hostnames, Cisco ISE looks for the corresponding IP addresses in the PAN and PSN nodes while deploying the mappings and checking the deployment status. You can use this option to specify the number of mappings that are created for the IP addresses returned by the DNS query. You can select one of the following options:

- **Create mappings for all IP addresses returned by a DNS query**
- **Create mappings only for the first IPv4 address and the first IPv6 address that is returned by a DNS query**

TrustSec HTTP Service for Network Devices

- **Enable HTTP Service**: Use HTTP to transfer Trustsec data to network devices over port 9063.

- **Include entire response payload body in Audit**: Enable this option to display the entire TrustSec HTTP response payload body in the audit logs. This option may dramatically decrease performance. When this option is disabled, only HTTP headers, status, and authentication information are logged.

Related Topics

TrustSec Architecture, on page 1071
TrustSec Components, on page 1071
Configure TrustSec Global Settings, on page 1078

Configure TrustSec Matrix Settings

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Work Centers** > **TrustSec** > **Settings** > **TrustSec Matrix Settings**.

Step 2 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Settings** > **TrustSec Matrix Settings**.

Step 3 Enter the required details in the TrustSec Matrix Settings page.

Step 4 Click **Save**.

TrustSec Matrix Settings

The following table describes the fields on the TrustSec Matrix Settings window. To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Settings** > **TrustSec Matrix Settings**.

Table 157: Configuring TrustSec Matrix Settings

Field Name	Usage Guidelines
Allow Multiple SGACLs	Check this check box if you want to allow multiple SGACLs in a cell. If this option is not selected, Cisco ISE will allow only one SGACL per cell. By default, this option is disabled upon fresh install. After upgrade, Cisco ISE will scan the Egress cells and if it identifies at least one cell with multiple SGACLs assigned to it, it allows the admin to add multiple SGACLs in a cell. Otherwise, it allows only one SGACL per cell. **Note** Before disabling multiple SGACLs, you must edit the cells containing multiple SGACLs to include only one SGACL.

Field Name	Usage Guidelines
Allow Monitoring	Check this check box to enable monitoring for all cells in the matrix. If monitoring is disabled, Monitor All icon is greyed out and the Monitor option is disabled in the Edit Cell dialog. By default, monitoring is disabled upon fresh install. **Note** Before disabling monitoring at matrix level, you must disable monitoring for the cells that are currently being monitored.
Show SGT Numbers	Use this option to display or hide the SGT values (both decimal and hexadecimal) in the matrix cells. By default, the SGT values are displayed in the cells.
Appearance Settings	The following options are available: • **Custom settings**: The default theme (colors with no patterns) is displayed initially. You can set your own colors and patterns. • **Default settings**: Predefined list of colors with no patterns (not editable). • **Accessibility settings**: Predefined list of colors with patterns (not editable).
Color/Pattern	To make the matrix more readable, you can apply coloring and patterns to the matrix cells based on the cell contents. The following display types are available: • **Permit IP/Permit IP Log**: Configured inside the cell • **Deny IP/Deny IP Log**: Configured inside the cell • **SGACLs**: For SGACLs configured inside the cell • **Permit IP/Permit IP Log (Inherited)**: Taken from the default policy (for non-configured cells) • **Deny IP/Deny IP Log (Inherited)**: Taken from the default policy (for non-configured cells) • **SGACLs (Inherited)**: Taken from the default policy (for non-configured cells)

Related Topics

Egress Policy, on page 1096

Matrix View, on page 1097

Configure TrustSec Matrix Settings, on page 1082

Configure TrustSec Devices

For Cisco ISE to process requests from TrustSec-enabled devices, you must define these TrustSec-enabled devices in Cisco ISE.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Components** > **Network Devices**

Step 2 Click **Add**.

Step 3 Enter the required information in the **Network Devices** section.

Step 4 Check the **Advanced Trustsec Settings** check box to configure a Trustsec-enabled device.

Step 5 Click **Submit**.

OOB TrustSec PAC

All TrustSec network devices possess a TrustSec PAC as part of the EAP-FAST protocol. This is also utilized by the secure RADIUS protocol where the RADIUS shared secret is derived from parameters carried by the PAC. One of these parameters, Initiator-ID, holds the TrustSec network device identity, namely the Device ID.

If a device is identified using TrustSec PAC and there is no match between the Device ID, as configured for that device on Cisco ISE, and the Initiator-ID on the PAC, the authentication fails.

Some TrustSec devices (for example, Cisco firewall ASA) do not support the EAP-FAST protocol. Therefore, Cisco ISE cannot provision these devices with TrustSec PAC over EAP-FAST. Instead, the TrustSec PAC is generated on Cisco ISE and manually copied to the device; hence this is called as the Out of Band (OOB) TrustSec PAC generation.

When you generate a PAC from Cisco ISE, a PAC file encrypted with the Encryption Key is generated.

This section describes the following:

Generate a TrustSec PAC from the Settings Screen

You can generate a TrustSec PAC from the Settings screen.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings**

Step 2 From the Settings navigation pane on the left, click **Protocols**.

Step 3 Choose **EAP-FAST** > **Generate PAC**.

Step 4 Generate TrustSec PAC.

Generate a TrustSec PAC from the Network Devices Screen

You can generate a TrustSec PAC from the Network Devices screen.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Components** > **Network Devices**

Step 2 Click **Add**. You can also click **Add new device** from the action icon on the Network Devices navigation pane.

Step 3 If you are adding a new device, provide a device name.

Step 4 Check the **Advanced TrustSec Settings** check box to configure a TrustSec device.

Step 5 Under the **Out of Band (OOB) TrustSec PAC** sub section, click **Generate PAC**.

Step 6 Provide the following details:

- PAC Time to Live—Enter a value in days, weeks, months, or years. By default, the value is one year. The minimum value is one day and the maximum is ten years.
- Encryption Key—Enter an encryption key. The length of the key must be between 8 and 256 characters. The key can contain uppercase or lowercase letters, or numbers, or a combination of alphanumeric characters.

  The Encryption Key is used to encrypt the PAC in the file that is generated. This key is also used to decrypt the PAC file on the devices. Therefore, it is recommended that the administrator saves the Encryption Key for later use.

  The Identity field specifies the Device ID of a TrustSec network device and is given an initiator ID by the EAP-FAST protocol. If the Identity string entered here does not match that Device ID defined under TrustSec section in the Network Device creation page, authentication will fail.

  The expiration date is calculated based on the PAC Time to Live.

Step 7 Click **Generate PAC.**

Generate a TrustSec PAC from the Network Devices List Screen

You can generate a TrustSec PAC from the Network Devices list screen.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Components** > **Network Devices**

Step 2 Click **Network Devices**.

Step 3 Check the check box next to a device for which you want to generate the TrustSec PAC and click **Generate PAC.**

Step 4 Provide the details in the fields.

Step 5 Click **Generate PAC.**

Push Button

The Push option in the egress policy initiates a CoA notification that calls the Trustsec devices to immediately request for updates from Cisco ISE regarding the configuration changes in the egress policy.

Configure Cisco TrustSec AAA Servers

You can configure a list of Cisco TrustSec-enabled Cisco ISE servers in the AAA server list for Cisco TrustSec devices to authenticate against any of these servers. When you click Push, the new servers in this list download to the TrustSec devices. When a Cisco TrustSec device tries to authenticate, it chooses any Cisco ISE server from this list. If the first server is down or busy, the Cisco TrustSec device can authenticate itself against any of the other servers from this list. By default, the primary Cisco ISE server is a Cisco TrustSec AAA server. We recommend that you configure more Cisco ISE servers for a more reliable Cisco TrustSec environment.

Note If the Cisco ISE primary PAN is configured through an Amazon Machine Image (AMI) in Amazon Web Services (AWS), it is automatically added as a Cisco TrustSec AAA server with incorrect hostname and IP address values due to a known limitation. In the **TrustSec AAA Servers** window, add the Cisco ISE server by providing the correct hostname and IP address details. Then, delete the automatically added server from the **TrustSec AAA Servers** window by checking the check box next to the server and click **Delete**. For more information on Cisco ISE servers configured through AWS, see the Chapter "Install Cisco ISE with Amazon Web Services" in the *Cisco ISE Installation Guide, Release 3.1*.

This page lists the Cisco ISE servers in your deployment that you have configured as your Cisco TrustSec AAA servers.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Components** > **TrustSec AAA Servers**

Step 2 Click **Add**.

Step 3 Enter the values as described:

- **Name**: Name that you want to assign to the Cisco ISE server in this AAA Server list. This name can be different from the hostname of the Cisco ISE server.
- **Description**: An optional description.
- **IP**: IP address of the Cisco ISE server that you are adding to the AAA Server list.
- **Port**: Port over which communication between the Cisco TrustSec device and server should take place. The default is 1812.

Step 4 Click **Submit**.

Step 5 In the **AAA Servers** window that is then displayed, click **Push**.

What to do next

Configure Security Groups.

TrustSec HTTPS Servers

By default, Cisco ISE exchanges Trustsec environment data between Cisco ISE and Trustsec NADs using RADIUS. You can configure Cisco ISE to use HTTPS, which is faster and more reliable than RADIUS. Cisco ISE uses REST APIs to implement HTTP transfers.

HTTPS transfer requires:

- Port 9603 must be open between the HTTPS servers and the Trustsec network devices.
- The credentials of the HTTPS server on every network device that connects to a PSN must be unique.
- Cisco switches are running version 16.12.2, 17.1.1 or higher.

To configure HTTPS transfer:

1. On each network device, enable HTTP file transfer, and require credentials.
2. In Cisco ISE, enable **Trustsec REST API Service for Network Devices** in **General Trustsec Settings**.
3. In Cisco ISE, edit each PSN's network device definition to check **Enable HTTP REST API** and enter the credentials to the network device's HTTP server.
4. In Cisco ISE, add that network device as a Trustsec HTTPs Server under **Trustsec** > **Components**.

Note If you configure only one node for HTTPS, then the Trustsec servers that are not configured for HTTPS do not display in the Trustsec servers list. You must configure all the other Trustsec-enabled nodes in your deployment for HTTPS. If no PSNs are configured for HTTPS, then RADIUS is used, and all Cisco ISE lists all the PSN nodes in this Trustsec deployment.

After configuration is complete, Cisco ISE returns a list of configured servers in the TrustSec environment data under **Trustsec** > **Network Devices**.

Debug

Enable ERS in debug. This setting logs all ERS traffic. Don't leave this setting enabled for more than 30 mins to avoid overloading the log file.

You can enable additional audit information by checking **Include request payload body** under **Trustsec REST API Service for Network Devices** on **Trustsec** > **Settings** > **General Trustsec Settings**.General TrustSec Settings

Add an External Server to Cisco ISE TrustSec HTTPS Servers

You can achieve load balancing of the HTTPS TrustSec service by adding one or more external servers to the HTTPS servers list.

The external server can act as a load balancer in one of the following ways:

- **SSL Termination**

In this setup, the external server is the termination point for the SSL connection initiated by the TrustSec enabled network device. At the same time, the server establishes its own SSL sessions with the PSN nodes, and acts as a proxy to relay the information between the network device and a given PSN node. Hence, the external server must host a certificate containing its IP address, FQDN, or both. This certificate must be trusted by the network devices.

For the SSL session between the external server and the PSN nodes, the external server must trust the certificates from the PSN nodes. This establishment of trust is a device specific configuration aspect of the external server, depending on the product used for this purpose.

- **SSL Passthrough**

  In this setup, the external server acts as an IP address translation device and simply lets the communication between the network device and the PSN nodes pass through. As a result, there is no certificate present on the external server and the certificate trust needs to be established between the network device and the PSN nodes.

  The certificates used by the PSN nodes for this purpose must include the IP address of the external server, because the network devices establish the SSL session using the IP address of the external server. This can be achieved by using a wild card certificate or a universal certificate. You can add multiple FQDNs, IP addresses, or both, as SAN entries in a universal certificate.

Irrespective of the deployment option selected, whenever the external server directs communication from a network device to a specific PSN node, it must ensure persistence of that connection. This means that all parts of that communication must take place only between that network device and that specific PSN node.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers > TrustSec > Components > Trustsec Servers > HTTPS Servers**

Step 2 Click **Add External Server**.

Step 3 Enter the following details:

- **Name**: Name of the external server to be added to the Cisco ISE HTTPS servers list.
- **Hostname (FQDN)**: Hostname of the external server.

  Note You can choose to provide either the hostname or the IP address of the external server.

- **Description**: An optional description.
- **Port**: Port over which communication between the Cisco TrustSec device and the external server should take place.
- **IP Address**: IP address of the external server that you are adding to the Cisco ISE HTTPS servers list.

Step 4 Click **Add Certificate**.

SSL certificates are required to enable the external server for load balancing operations and secure communication. Add certificates in order of the chain of trust, starting with the root certificate.

Step 5 Enter a name in the **Certificate name** field.

Step 6 Add the SSL certificate in the **Certificate** field. You can do this by attaching a file or pasting the certificate from a clipboard.

Step 7 Click **Save**.

The notifications bar displays a dialog box with the following message:

```
There are TrustSec configuration changes that have not been notified to network devices. To notify
the relevant network devices about these changes, click the push button.
```

Step 8 Click **Push**.

The relevant network devices are now notified of these configuration changes.

You can now see the external server in the Cisco ISE HTTPS servers list.

Security Groups Configuration

A Security Group (SG) or Security Group Tag (SGT) is an element that is used in TrustSec policy configuration. SGTs are attached to packets when they move within a trusted network. These packets are tagged when they enter a trusted network (ingress) and untagged when they leave the trusted network (egress).

SGTs are generated in a sequential manner, but you have the option to reserve a range of SGTs for IP to SGT mapping. Cisco ISE skips the reserved numbers while generating SGTs.

TrustSec service uses these SGTs to enforce the TrustSec policy at egress.

You can configure security groups from the following pages in the Admin portal:

- In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Components** > **Security Groups**
- Directly from egress policy page at **Configure** > **Create New Security Group**.

You can click the **Push** button to initiate an environment CoA notification after updating multiple SGTs. This environment CoA notification goes to all TrustSec network devices forcing them to start a policy/data refresh request.

Note Frequent use of the **Push** or **Deploy** button is not advised. When there is a change in a matrix or SGACL, check the notification bar for any pending deployment requests before performing the next deployment operation.

Managing Security Groups in Cisco ISE

Prerequisites

To create, edit or delete Security Groups, you must be a Super Admin or System Admin.

Add a Security Group

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Components** > **Security Groups**.
2. Click **Add** to add a new security group.
3. Enter a name and description (optional) for the new security group.
4. Check the **Propagate to ACI** check box if you want to propagate this SGT to Cisco ACI. The SXP mappings that are related to this SGT will be propagated to Cisco ACI only if they belong to a VPN that is selected in the Cisco ACI Settings page.

   This option is disabled by default.
5. Enter a Tag Value. Tag value can be set to be entered manually or autogenerate. You can also reserve a range for the SGT. You can configure it from the General TrustSec Settings page (**Work Centers** > **TrustSec** > **Settings** > **General TrustSec Settings**).
6. Click **Save**.

Delete a Security Group

You can't delete security groups that are still in use by a source or destination. That includes the default groups, which are mapped to a function in Cisco ISE:

- BYOD
- Guest
- Trustsec Devices
- Unknown

Import Security Groups into Cisco ISE

You can import security groups in to a Cisco ISE node using a comma-separated value (CSV) file. You must first update the template before you can import security groups into Cisco ISE. You cannot run import of the same resource type at the same time. For example, you cannot concurrently import security groups from two different import files.

You can download the CSV template from the Admin portal, enter your security group details in the template, and save the template as a CSV file, which you can then import back into Cisco ISE.

While importing security groups, you can stop the import process when Cisco ISE encounters the first error.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Components** > **Security Groups**.

Step 2 Click **Import**.

Step 3 Click **Browse** to choose the CSV file from the system that is running the client browser.

Step 4 Check the **Stop Import on First Error** check box.

Step 5 Click **Import** .

Export Security Groups from Cisco ISE

You can export security groups configured in Cisco ISE in the form of a CSV file that you can use to import these security groups into another Cisco ISE node.

Step 1 Choose **Work Centers** > **TrustSec** > **Components** > **Security Groups**.

Step 2 Click **Export**.

Step 3 To export security groups, you can do one of the following:

- Check the check boxes next to the group that you want to export, and choose **Export** > **Export Selected**.
- Choose **Export** > **Export All** to export all the security groups that are defined.

Step 4 Save the export.csv file to your local hard disk.

Add IP SGT Static Mapping

You can use the IP-SGT static mappings to deploy the mappings on TrustSec devices and SXP domains in a unified manner. While creating a new IP-SGT static mapping, you can specify the SXP domains and the devices on which you want to deploy this mapping. You can also associate the IP-SGT mapping to a mapping group.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Components** > **IP SGT Static Mapping**.

Step 2 Click **Add**.

Step 3 In the **New** area displayed, choose **IP Address** or **Hostname** from the drop-down list, and enter the corresponding value in the field next to it.

In the **Map to SGT individually** option in the following step, you can specify a SXP domain to map to. However, the **Send to SXP Domain** field is not accessible if you choose **Hostname** in this step. To add an SXP domain in the next step, you must choose **IP Address** here.

Step 4 If you want to use an existing mapping group, click **Add to a Mapping Group** and select the required group from the **Mapping Group** drop-down list.

If you want to map this IP address/hostname to an SGT individually, click **Map to SGT Individually** and do the following:

- Select an SGT from the SGT drop-down list.
- Select the Virtual Network for the mapping from the drop-down list .
- Select the SXP VPN groups on which the mapping must be deployed.
- Specify the devices on which you want to deploy this mapping. You can deploy the mapping on all TrustSec devices, on selected network device groups, or on selected network devices.

Step 5 Click **Save**.

Deploy IP SGT Static Mappings

After adding the mappings, deploy the mappings on the target network devices using the **Deploy** option. You must do this explicitly even if you have saved the mappings earlier. Click **Check Status** to check the deployment status of the devices.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers > TrustSec > Components > IP SGT Static Mapping**

Step 2 Check the check boxes near the mappings that you want to deploy. Check the check box at the top if you want to deploy all the mappings.

Step 3 Click **Deploy**.

All the TrustSec devices are listed in the **Deploy IP SGT Static Mapping** window.

Step 4 Check the check boxes near the devices or the device groups to which the selected mappings must be deployed.

- Check the check box at the top if you want to select all the devices.
- Use the filter option to search for specific devices.
- If you do not select any device, the selected mappings are deployed on all the TrustSec devices.
- When you select devices to deploy new mapping, ISE selects **all** the devices that will be affected by the new mapping.

Step 5 Click **Deploy**. The deploy button updates the mapping on all the devices affected by the new maps.

The **Deployment Status** window shows the order in which the devices are updated and the devices that are not getting updated because of an error or because the device is unreachable. After the deployment is complete, the window displays the total number of devices that are successfully updated and the number of devices that are not updated.

Use the **Check Status** option in the **IP SGT Static Mapping** page to check if different SGTs are assigned to the same IP address for a specific device. You can use this option to locate the devices that have conflicting mappings, IP addresses that are mapped to multiple SGTs, and the SGTs that are assigned to the same IP address. The **Check Status** option can be used even if device groups, FQDN, hostname, or IPv6 addresses are used in the deployment. You must remove the conflicting mappings or modify the scope of deployment before deploying these mappings.

IPv6 addresses can be used in IP SGT static mappings. These mappings can be propagated using SSH or SXP to specific network devices or network device groups.

If FQDN and hostnames are used, Cisco ISE looks for the corresponding IP addresses in the PAN and PSN nodes while deploying the mappings and checking the deployment status.

Use the **IP SGT Static Mapping of Hostnames** option in the **General TrustSec Settings** window to specify the number of mappings created for the IP addresses returned by the DNS query. Select one of the following options:

- **Create mappings for all the IP addresses returned by a DNS query**.
- **Create mappings only for the first IPv4 address and the first IPv6 address returned by a DNS query**.

Import IP SGT Static Mappings into Cisco ISE

You can import IP SGT mappings using a CSV file.

You can also download the CSV template from the Admin portal, enter your mapping details, save the template as a CSV file, and then import it back into Cisco ISE.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Components** > **IP SGT Static Mapping**

Step 2 Click **Import**.

Step 3 Click **Browse** to select the CSV file from the system that is running the client browser.

Step 4 Click **Upload**.

Export IP SGT Static Mappings from Cisco ISE

You can export the IP SGT mappings in the form of a CSV file. You can use this file to import these mappings into another Cisco ISE node.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Components** > **IP SGT Static Mapping**.

Step 2 Do one of the following:

- Check the check boxes next to the mappings that you want to export, and choose **Export** > **Selected**.
- Choose **Export** > **All** to export all the mappings.

Step 3 Save the mappings.csv file to your local hard disk.

Add SGT Mapping Group

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Components** > **IP SGT Static Mapping** > **Manage Groups**.

Step 2 Click **Add**.

Step 3 Enter a name and description for the mapping group.

Step 4 Do the following:

- Select an SGT from the **SGT** drop-down list.
- Select the Virtual Network for the mapping from the drop-down list.

- Select the SXP VPN groups on which the mappings must be deployed.
- Specify the devices on which you want to deploy the mappings. You can deploy the mappings on all TrustSec devices, on selected network device groups, or on selected network devices.

Step 5 Click **Save**.

You can move an IP SGT mapping from one mapping group to another mapping group.

You can also update or delete the mappings and mapping groups. To update a mapping or mapping group, check the check box next to the mapping or mapping group that you want to update, and then click **Edit**. To delete a mapping or mapping group, check the check box next to the mapping or mapping group that you want to delete, and then click **Trash** > **Selected**. When a mapping group is deleted, the IP SGT mappings within that group are also deleted.

Add Security Group Access Control Lists

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Components** > **Security Group ACLs**.

Step 2 Click **Add** to create a new Security Group ACL.

Step 3 Enter the following information:

- Name—Name of the SGACL
- Description—An optional description of the SGACL
- IP Version—IP version that this SGACL supports:
  - IPv4—Supports IP version 4 (IPv4)
  - IPv6—Supports IP version 6 (IPv6)
  - Agnostic—Supports both IPv4 and IPv6
- Security Group ACL Content—Access control list (ACL) commands. For example:

  permit icmp

  deny ip

  The syntax of SGACL input is not checked within ISE. Make sure you are using the correct syntax so that switches, routers and access points can apply them without errors. The default policy can be configured as **permit IP**, **permit ip log**, **deny ip**, or **deny ip log**. A TrustSec network device attaches the default policy to the end of the specific cell policy.

  Here are two examples of SGACLs for guidance. Both include a final catch all rule. The first one denies as the final catch all rule, and the second one permits.

  Permit_Web_SGACL

```
permit tcp dst eq 80
permit tcp dst eq 443
deny ip
```

Deny_JumpHost_Protocols

```
deny tcp dst eq 23
deny tcp dst eq 23
deny tcp dst eq 3389
permit ip
```

The following table lists syntax for SGACL for IOS, IOS XE and NS-OS operating systems.

SGACL CLI and ACEs	Syntax common across IOS, IOS XE, and NX-OS
config acl	deny, exit, no, permit
deny permit	ahp, eigrp, gre, icmp, igmp, ip, nos, ospf, pcp, pim, tcp, udp
deny tcp deny tcp src deny tcp dst	dst, log, src
deny tcp dst eq deny tcp src eq	range 0 65535
deny udp deny udp src deny udp dest	Dst, log, src
deny tcp dst eq www deny tcp src eq www	range 0 65535

Note Hypens are not allowed by some Cisco switches. So `permit dst eq 32767-65535` is not valid. Use `permit dst eq range 32767 65535`. Some Cisco switches do not require `eq` in their command syntax. Thus, `permit dst eq 32767-65535` is not valid in these switches. Use `permit dst 32767-65535` or `permit dst range 32767 65535` instead.

Step 4 Click **Push**.

The Push option initiates a CoA notification that tells the Trustsec devices to immediately request updates from Cisco ISE about the configuration changes.

Note Cisco ISE has the following predefined SGACLs: Permit IP, Permit IP Log, Deny IP, and Deny IP Log. You can use these SGACLs to configure the TrustSec Matrix using the GUI or ERS API. Though these SGACLs are not listed in the Security Group ACLs listing page in the GUI, these SGACLs will be listed when you use the ERS API to list the available SGACLs (ERS getAll call).

Egress Policy

The egress table lists the source and destination SGTs, both reserved and unreserved. This page also allows you to filter the egress table to view specific policies and also to save these preset filters. When the source SGT tries to reach the destination SGT, the TrustSec-capable device enforces the SGACLs based on the TrustSec policy as defined in the Egress Policy. Cisco ISE creates and provisions the policy.

After you create the SGTs and SGACLs, which are the basic building blocks required to create a TrustSec policy, you can establish a relationship between them by assigning SGACLs to source and destination SGTs.

Each combination of a source SGT to a destination SGT is a cell in the Egress Policy.

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **TrustSec Policy** > **Egress Policy**

You can view the Egress policy in three different ways:

- Source Tree View
- Destination Tree View
- Matrix View

Source Tree View

The Source Tree view lists a compact and organized view of source SGTs in a collapsed state. You can expand any source SGT to see the internal table that lists all information related to that selected source SGT. This view displays only the source SGTs that are mapped to destination SGTs. If you expand a specific source SGT, it lists all destination SGTs that are mapped to this source SGT and and the corresponding policy (SGACLs) in a table.

You will see three dots (...) next to some fields. This signifies that there is more information contained in the cell. You can position the cursor over the three dots to view the rest of the information in a quick view popup. When you position the cursor over an SGT name or an SGACL name, a quick view popup opens to display the content of that particular SGT or SGACL.

Destination Tree View

The Destination Tree view lists a compact and organized view of destination SGTs in a collapsed state. You can expand any destination SGTs to see the internal table that lists all information related to that selected destination SGT. This view displays only the destination SGTs that are mapped to source SGTs. If you expand a specific destination SGT, it lists all source SGTs that are mapped to this destination SGT and and the corresponding policy (SGACLs) in a table.

You will see three dots (...) next to some fields. This signifies that there is more information contained in the cell. You can position the cursor over the three dots to view the rest of the information in a quick view popup. When you position the cursor over an SGT name or an SGACL name, a quick view popup opens to display the content of that particular SGT or SGACL.

Matrix View

The Matrix View of the Egress policy looks like a spreadsheet. It contains two axis:

- Source Axis—The vertical axis lists all the source SGTs.
- Destination Axis—The horizontal axis lists all the destination SGTs.

The mapping of a source SGT to a destination SGT is represented as a cell. If a cell contains data, then it represents that there is a mapping between the corresponding source SGT and the destination SGT. There are two types of cells in the matrix view:

- Mapped cells—When a source and destination pair of SGTs is related to a set of ordered SGACLs and has a specified status.
- Unmapped cells—When a source and destination pair of SGTs is not related to any SGACLs and has no specified status.

The Egress Policy cell displays the source SGT, the destination SGT, and the Final Catch All Rule as a single list under SGACLs, separated by commas. The Final Catch All Rule is not displayed if it is set to None. An empty cell in a matrix represents an unmapped cell.

In the Egress Policy matrix view, you can scroll across the matrix to view the required set of cells. The browser does not load the entire matrix data at once. The browser requests the server for the data that falls in the area you are scrolling in. This prevents memory overflow and performance issues.

You can use the following options in the **View** drop-down list to change the matrix view.

- Condensed with SGACL names—If you select this option, the empty cells are hidden and the SGACL names are displayed in the cells.
- Condensed without SGACL names—The empty cells are hidden and the SGACL names are not displayed in the cells. This view is useful when you want to see more matrix cells and differentiate between the content of the cells using colors, patterns, and icons (cell status).
- Full with SGACL names—If you select this option, the left and upper menus are hidden and the SGACL names are displayed in the cells.
- Full without SGACL names—When this option is selected, the matrix is displayed in full screen mode and the SGACL names are not displayed in the cells.

ISE allows you to create, name, and save the custom views. To create custom views, choose **Show > Create Custom View**. You can also update the view criteria or delete unused views.

The Matrix view has the same GUI elements as the Source and Destination views. However, it has these additional elements:

Matrix Dimensions

The **Dimension** drop-down list in the Matrix view enables you to set the dimensions of the matrix.

Create Custom View

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Matrix View page, select the **Create Custom View** option from the **Show** drop-down list.

Step 2 In the **Edit View** dialog box, enter the following details:

- View Name—Enter a name for the custom view.
- Source Security Groups—Move the SGTs that you want to include in the custom view to the Show transfer box.
- Show Relevant for Destination—Check this check box if you want to override your selection in the Source Security Group Show transfer box and copy all the entries in the Destination Security Group Hide transfer box. If there are more than 200 entries, the data will not be copied and a warning message will be displayed.
- Destination Security Groups—Move the SGTs that you want to include in the custom view to the Show transfer box.
- Show Relevant for Source—Check this check box if you want to override your selection in the Destination Security Group Show transfer box and copy all the entries in the Source Security Group Hide transfer box.
- Sort Matrix By—Select one of the following options:
  - Manual Order
  - Tag Number
  - SGT Name

Step 3 Click **Save**.

Matrix Operations

Navigating through the Matrix

You can navigate through the matrix either by dragging the matrix content area with the cursor or by using horizontal and vertical scroll bars. You can click and hold on a cell to drag it along with the entire matrix content in any direction. The source and destination bar moves along with the cells. The matrix view highlights the cell and the corresponding row (Source SGT) and column (Destination SGT) when a cell is selected. The coordinates (Source SGT and Destination SGT) of the selected cell are displayed below the matrix content area.

Selecting a Cell in the Matrix

To select a cell in the matrix view, click on it. The selected cell is displayed in different color, and the source and destination SGTs are highlighted. You can deselect a cell either by clicking it again or by selecting another cell. Multiple cell selection is not allowed in the matrix view. Double-click the cell to edit the cell configuration.

Configure SGACL from Egress Policy

You can create Security Group ACLs directly from the Egress Policy page.

Step 1 Choose **Work Centers** > **TrustSec** > **TrustSec Policy** > **Egress Policy**.

Step 2 From the Source or Destination Tree View page, choose **Configure** > **Create New Security Group ACL**.

Step 3 Enter the required details and click **Submit**.

Configure Work Process Settings

Before you begin

To perform the following task, you must be a Super Admin.

Step 1 Choose **Work Centers** > **TrustSec** > **Settings** > **Work Process Settings**.

Step 2 Select one of the following options:

- Single Matrix—Select this option if you want to create only one Policy matrix for all the devices in the TrustSec network.
- Multiple Matrices—Allows you to create multiple policy matrices for different scenarios. You can use these matrices to deploy different policies to different network devices.

  Note The matrices are independent and each network device can be assigned to only one matrix.

- Production and Staging Matrices with Approval Process—Select this option if you want to enable the Workflow mode. Select the users that are assigned to the editor and approver roles. You can select the users only from the Policy Admin and Super Admin groups. A user cannot be assigned to both editor and approver roles.

  Ensure that email addresses are configured for the users that are assigned to the editor and approver roles, otherwise email notifications regarding the workflow process will not be sent to these users.

  When the Workflow mode is enabled, a user that is assigned to the editor role can create a staging matrix, select the devices on which he wants to deploy the staging policy, and submit the staging policy to the approver for approval. The user that is assigned to the approver role can review the staging policy and approve or reject the request. The staging policy can be deployed on the selected network devices only after the staging policy is reviewed and approved by the approver.

Step 3 Check the **Use DEFCONS** check box if you want to create DEFCON matrices.

DEFCON matrices are standby policy matrices that can be easily deployed in the event of network security breaches.

You can create DEFCON matrices for the following severity levels: Critical, Severe, Substantial, and Moderate.

When a DEFCON matrix is activated, the corresponding DEFCON policy is immediately deployed on all the TrustSec network devices. You can use the Deactivate option to remove the DEFCON policy from the network devices.

Step 4 Click **Save**.

Matrices Listing Page

TrustSec policy matrices and DEFCON matrices are listed in the Matrices Listing page. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **TrustSec Policy** > **Egress Policy** > **Matrices List**. You can also view the number of devices that are assigned to each matrix.

Note Matrices Listing page is not displayed when Single Matrix mode is enabled with DEFCON matrix option disabled.

You can do the following from the Matrices Listing page:

- Add a new matrix
- Edit an existing matrix
- Delete a matrix
- Duplicate an existing matrix
- Assign NADs to a matrix

You can assign NADs to a matrix by using the Assign NADs option. To do this:

1. In the Assign Network Devices window, select the network devices that you want to assign to a matrix. You can also use the filter option to select the network devices.
2. Select the matrix from the Matrix drop-down list. All the existing matrices and the default matrix are listed in this drop-down list.

After assigning the devices to a matrix, click Push to notify the TrustSec configuration changes to the relevant network devices.

Note the following points while working on the Matrices Listing page:

- You cannot edit, delete, or rename the default matrix.
- While creating a new matrix you can start with a blank matrix or copy the policy from an existing matrix.
- If you delete a matrix, the NADs that are assigned to that matrix are automatically moved to the default matrix.
- When you copy an existing matrix, a copy of the matrix will be created but devices are not automatically assigned to the copied matrix.
- In the Multiple Matrices mode, all the devices are assigned to the default matrix at the initial stage.
- In the Multiple Matrices mode, some of the SGACLs might be shared among the matrices. In such cases, changing an SGACL content will affect all matrices that contain this SGACL in one of their cells.
- Multiple matrices cannot be enabled if staging is in progress.
- When you are moving from Multiple Matrices mode to Single Matrix mode, all the NADs are automatically assigned to the default matrix.
- You cannot delete a DEFCON matrix if it is currently activated.

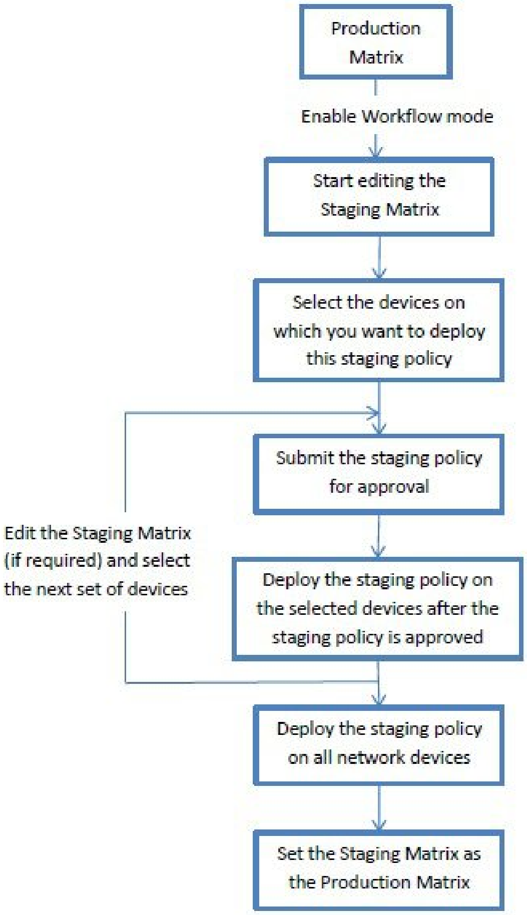
TrustSec Matrix Workflow Process

The Matrix Workflow feature helps you to test a new policy on a limited set of devices by using a draft version of the matrix (called staging matrix) before deploying the policy on all the network devices. You can submit the staging policy for approval and deploy the staging policy on the selected network devices after it is approved. This feature helps you to deploy the new policy on a limited set of devices, check whether it is working fine, and make any changes, if required. You can continue deploying the policy on next set of devices or on all the devices. When the staging policy is deployed on all the network devices, the staging matrix can be set as the new production matrix.

When the Workflow mode is enabled, a user that is assigned to the editor role can create a staging matrix and edit the matrix cells. The staging matrix is a copy of the production matrix that is currently deployed on the TrustSec network. The editor can select the devices on which he wants to deploy the staging policy and submit the staging policy to the approver for approval. The user that is assigned to the approver role can review the staging policy and approve or reject the request. The staging policy can be deployed on the selected network devices only after the staging policy is reviewed and approved by the approver.

The following figure describes the workflow process.

Figure 48: Matrix Workflow Process


Production Matrix
Enable Workflow mode
Start editing the Staging Matrix
Select the devices on which you want to deploy this staging policy
Submit the staging policy for approval
Edit the Staging Matrix (if required) and select the next set of devices
Deploy the staging policy on the selected devices after the staging policy is approved
Deploy the staging policy on all network devices
Set the Staging Matrix as the Production Matrix

Super Admin user can select the users that are assigned to the editor and approver roles in the **Workflow Process Settings** page. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Settings** > **Workflow Process**.

You cannot edit the SGTs and SGACLs after the staging policy is deployed on the selected devices, however, you can edit the matrix cells. You can use the Configuration Delta report to track the difference between the production matrix and the staging matrix. You can also click on the Delta icon on a cell to view the changes made to that cell during the staging process.

The following table describes the different stages of the workflow:

Stage	Description
Staging in Edit	The matrix is moved to Staging in Edit state, when an editor starts editing the staging matrix. After editing the staging matrix, the editor can select the devices on which he wants to deploy the new staging policy.
Staging Awaiting Approval	After editing the matrix, the editor submits the staging matrix to the approver for review and approval. While submitting the staging matrix for approval, the editor can add the comments that will be included in the email sent to the approver. The approver can review the staging policy and approve or reject the request. The approver can also view the selected network devices and the Configuration Delta report. While approving or rejecting a request, the approver can add the comments that will be included in the email sent to the editor. The editor can cancel the approval request as long as the staging policy is not deployed on any of the network devices.
Deploy Approved	When the approver approves the request, the staging matrix is moved to Deploy Approved state. If the request is rejected, the matrix is moved back to Staging in Edit state. The editor can deploy the staging policy on the selected network devices only after the staging policy is approved by the approver.
Partially Deployed	After the staging matrix is deployed on the selected devices, the matrix is moved to Partially Deployed state. The matrix remains in the Partially Deployed stage till the staging policy is deployed on all the network devices. You cannot edit the SGTs and SGACLs at this stage, however, you can edit the matrix cells. The devices that are not deployed with the latest policy (out-of-sync devices) are displayed in orange (with italic font) in the Network Device Deployment window. This status is also displayed on the deployment progress status bar. The editor can select these devices and request approval to synchronize the devices that were updated in different deployment cycles.

Stage	Description
Fully Deployed	The above process is repeated till the staging policy is deployed on all the network devices. When the staging matrix is deployed on all the network devices, the approver can set the staging matrix as the production matrix. We recommend that you take a copy of the production matrix before setting the staging matrix as the new production matrix, because after replacing the production matrix with the staging matrix, you cannot rollback to the previous version of the production matrix.

The options displayed in the Workflow drop-down list vary based on the workflow state and the user role (editor or approver). The following table lists the menu options displayed for an editor and approver:

Workflow state	Menu displayed for Editor	Menu displayed for Approver
Staging in Edit	• Select network devices The following options are available in the Network Device Deployment window: • Request approval for selected devices • Request approval for all/filtered Staging list • Request approval for all/filtered Production list • Request approval for all/filtered devices • Request approval for all devices • Discard staging • View deltas	• View network devices • View deltas

Workflow state	Menu displayed for Editor	Menu displayed for Approver

Staging Awaiting Approval	• Cancel approval request
	• View network devices
	The following option is available in the Network Device Deployment window:
	  • Cancel approval request
	• View deltas
		• Approve deploy
		• Reject deploy
		• View network devices
		The following options are available in the Network Device Deployment window:
		  • Approve deploy
		  • Reject deploy
		• View deltas

Approved - ready to deploy	• Deploy
	• Cancel approval request
	• View network devices
	The following options are available in the Network Device Deployment window:
	  • Deploy
	  • Cancel approval request
	• View deltas
		• Reject deploy
		• View network devices
		The following option is available in the Network Device Deployment window:
		  • Reject deploy
		• View deltas

Workflow state	Menu displayed for Editor	Menu displayed for Approver

Partially deployed	• Select network devices
	The following options are available in the Network Device Deployment window:
	  • Request approval for selected devices
	  • Request approval for all/filtered Staging list
	  • Request approval for all/filtered Production list
	  • Request approval for all/filtered devices
	• Request approval for all devices
	• View deltas
		• View network devices
		• View deltas

Workflow state	Menu displayed for Editor	Menu displayed for Approver

Fully deployed	• Select network devices
	The following options are available in the Network Device Deployment window:
	  • Request approval for selected devices
	  • Request approval for all/filtered Staging list
	  • Request approval for all/filtered Production list
	  • Request approval for all/filtered devices
	• Request approval for all devices
	• View deltas
		• Set as production
		• View network devices
		• View deltas

The workflow options are also available in the Source and Destination Tree view.

You can view the list of devices that downloaded the staging/production policy by using the TrustSec Policy Download report (Work Centers > TrustSec > Reports). The TrustSec Policy Download lists the requests sent by the network devices for policy (SGT/SGACL) download and the details sent by ISE. If the Workflow mode is enabled, the requests can be filtered for production or staging matrix.

Egress Policy Table Cells Configuration

Cisco ISE allows you to configure cells using various options that are available in the tool bar. Cisco ISE does not allow a cell configuration if the selected source and destination SGTs are identical to a mapped cell.

Add the Mapping of Egress Policy Cells

You can add the mapping cell for Egress Policy from the Policy page.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **TrustSec Policy** > **Egress Policy**.

Step 2 To select the matrix cells, do the following:

- In the matrix view, click a cell to select it.
- In the Source and Destination tree view, check the check box of a row in the internal table to select it.

Step 3 Click **Add** to add a new mapping cell.

Step 4 Select appropriate values for:

- Source Security Group
- Destination Security Group
- Status, Security Group ACLs
- Final Catch All Rule

Step 5 Click **Save**.

Export Egress Policy

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **TrustSec Policy** > **Egress Policy** > **Matrix** > **Export**.

Step 2 Check the **Include Empty Cells** check box if you want to include the empty cells (which do not have any SGACL configured) in the exported file.

When this option is enabled, the whole matrix is exported and the empty cells are marked with the "Empty" keyword in the SGACL column.

Note Ensure that the exported file does not contain more than 500000 lines, otherwise the export may fail.

Step 3 Select one of the following options:

- Local Disk—Select this option if you want to export the file to a local drive on your computer.
- Repository—Select this option if you want to export the file to a remote repository.

  You must configure the repositories before exporting the file. To configure the repositories, choose **Administration** > **Maintenance** > **Repository**. Ensure that read and write access privileges are provided for the repository that you have selected.

  You can encrypt the exported file by using an encryption key.

  You can modify the file name. File name should not include more than 50 characters. By default, the file name includes the current time, however, if the same file name exists on the remote repository, the file will be overwritten.

Step 4 Click **Export**.

Import Egress Policy

You can create the egress policy offline and then import it in to Cisco ISE. If you have a large number of security group tags, then creating the security group ACL mapping one by one might take some time. Instead, creating the egress policy offline and importing it in to Cisco ISE saves time for you. During import, Cisco ISE appends the entries from the CSV file to the egress policy matrix and does not overwrite the data.

Egress policy import fails if the:

- Source or destination SGTs do not exist
- SGACL does not exist
- Monitor status is different than what is currently configured in Cisco ISE for that cell

---

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **TrustSec Policy** > **Egress Policy** > **Matrix** > **Import**.

Step 2 Click **Generate a Template**.

Step 3 Download the template (CSV file) from the Egress Policy page and enter the following information in the CSV file:

- Source SGT
- Destination SGT
- SGACL
- Monitor status (enabled, disabled, or monitored)

Step 4 Check the **Overwrite Existing Data with New Data** check box if you want to overwrite the existing policy with the one that you are importing. If empty cells (cells that are marked with the "Empty" keyword in the SGACL column) are included in the imported file, the existing policy in the corresponding matrix cells will be deleted.

While exporting the egress policy, if you want to include the empty cells, check the **Include Empty Cells** check box. For more information, see Export Egress Policy, on page 1107.

Step 5 Click **Validate File** to validate the imported file. Cisco ISE validates the CSV structure, SGT names, SGACL, and file size before importing the file.

Step 6 Check the **Stop Import on First Error** check box for Cisco ISE to cancel the import if it encounters any errors.

Step 7 Click **Import**.

Configure SGT from Egress Policy

You can create Security Groups directly from the Egress Policy page.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **TrustSec Policy** > **Egress Policy**.

Step 2 From the Source or Destination Tree View page, choose **Configure** > **Create New Security Group**.

Step 3 Enter the required details and click **Submit**.

Monitor Mode

The Monitor All option in the egress policy allows you to change the entire egress policy configuration status to monitor mode with a single click. Check the **Monitor All** check box in the egress policy page to change the egress policy configuration status of all the cells to monitor mode. When you check the Monitor All check box, the following changes take place in the configuration status:

- The cells whose status is Enabled will act as monitored but appears as if they are enabled.
- The cells whose status is Disable will not be affected.
- The cells whose status is Monitor will remain Monitored.

Uncheck the **Monitor All** check box to restore the original configuration status. It does not change the actual status of the cell in the database. When you deselect **Monitor All**, each cell in the egress policy regains its original configuration status.

Features of Monitor Mode

The monitoring functionality of the monitor mode helps you to:

- Know how much traffic is filtered but monitored by the monitor mode
- Know that SGT-DGT pair is in monitor mode or enforce mode, and observe if there is any unusual packet drop is happening in the network
- Understand that SGACL drop is actually enforced by enforce mode or permitted by monitor mode
- Create custom reports based on the type of mode (monitor, enforce, or both)
- Identify which SGACL has been applied on NAD and display discrepancy, if any

The Unknown Security Group

The Unknown security group is a pre-configured security group that cannot be modified and represents the Trustsec with tag value 0.

The Cisco security group network devices request for cells that refer to the unknown SGT when they do not have an SGT of either source or destination. If only the source is unknown, the request applies to the <unknown, Destination SGT> cell. If only the destination is unknown, the request applies to the <source SGT, unknown> cell. If both the source and destination are unknown, the request applies to the <Unknown, Unknown> cell.

Default Policy

Default Policy refers to the <ANY,ANY> cell. Any source SGT is mapped to any destination SGT. Here, the ANY SGT cannot be modified and it is not listed in any source or destination SGTs. The ANY SGT can only be paired with ANY SGT. It cannot be paired with any other SGTs. A TrustSec network device attaches the default policy to the end of the specific cell policy.

- If a cell is empty, that means it contains the default policy alone.
- If a cell contains some policy, the resulting policy is a combination of the cell specific policy followed by the default policy.

According to Cisco ISE, the cell policy and the default policy are two separate sets of SGACLs that the devices get in response to two separate policy queries.

Configuration of the default policy is different from other cells:

- Status can take only two values, Enabled or Monitored.
- Security Group ACLs is an optional field for the default policy, so can be left empty.
- Final Catch All Rule can be any of the following: Permit IP, Deny IP, Permit IP log, or Deny IP log. Clearly the None option is not available here because there is no safety net beyond the default policy.

SGT Assignment

Cisco ISE allows you to assign an SGT to a TrustSec device if you know the device hostname or IP address. When a device with the specific hostname or IP address joins the network, Cisco ISE will assign the SGT before authenticating it.

The following SGTs are created by default:

- SGT_TrustSecDevices
- SGT_NetworkServices
- SGT_Employee
- SGT_Contractor
- SGT_Guest
- SGT_ProductionUser
- SGT_Developer
- SGT_Auditor
- SGT_PointofSale
- SGT_ProductionServers
- SGT_DevelopmentServers
- SGT_TestServers
- SGT_PCIServers
- SGT_BYOD
- SGT_Quarantine

Sometimes, devices need to be manually configured to map the security group tags to the endpoint. You can create this mapping from the Security Group Mappings page. Before you perform this action, ensure that you have reserved a range of SGTs.

ISE allows you to create up to 10,000 IP-to-SGT mappings. You can create IP-to-SGT mapping groups to logically group such large scale mappings. Each group of IP-to-SGT mappings contains a list of IP addresses, a single security group it would map to and a network device or network device group which is the deployment target for those mappings.

NDAC Authorization

You can configure the TrustSec policy by assigning SGTs to devices. You can assign security groups to devices based on TrustSec device ID attribute.

Configure NDAC Authorization

Before you begin

- Ensure that you create the security groups for use in the policy.
- To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **TrustSec Policy** > **Network Device Authorization**.

Step 2 Click the **Action** icon on the right-hand side of the Default Rule row, and click **Insert New Row Above**.

Step 3 Enter the name for this rule.

Step 4 Click the plus sign (+) next to **Conditions** to add a policy condition.

Step 5 You can click **Create New Condition (Advance Option)** and create a new condition.

Step 6 From the **Security Group** drop-down list, select the SGT that you want to assign if this condition evaluates to true.

Step 7 Click the **Action** icon from this row to add additional rules based on device attributes either above or below the current rule. You can repeat this process to create all the rules that you need for the TrustSec policy. You can drag and drop the rules to reorder them by clicking the ⠿ icon. You can also duplicate an existing condition, but ensure that you change the policy name.

The first rule that evaluates to true determines the result of the evaluation. If none of the rules match, the default rule will be applied; you can edit the default rule to specify the SGT that must be applied to the device if none of the rules match.

Step 8 Click **Save** to save your TrustSec policy.

If a TrustSec device tries to authenticate after you have configured the network device policy, the device will get its SGT and the SGT of its peers and will be able to download all the relevant details.

Note By default, the result of default **Network Device Authorization** policy is set to **TrustSec_Devices**.

Configure End User Authorization

Cisco ISE allows you to assign a security group as the result of an authorization policy evaluation. Using this option, you can assign a security group to users and end points.

Before you begin

- Read the information on authorization policies.

- To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Authorization Policy**.

Step 2 Create a new authorization policy.

Step 3 Select a security group, for Permissions.

If the conditions specified in this authorization policy is true for a user or endpoint, then this security group will be assigned to that user or endpoint and all data packets that are sent by this user or endpoint will be tagged with this particular SGT.

TrustSec Configuration and Policy Push

Cisco ISE supports Change of Authorization (CoA) which allows Cisco ISE to notify TrustSec devices about TrustSec configuration and policy changes, so that the devices can reply with requests to get the relevant data.

A CoA notification can trigger a TrustSec network device to send either an Environment CoA or a Policy CoA.

You can also push a configuration change to devices that do not intrinsically support the TrustSec CoA feature.

CoA Supported Network Devices

Cisco ISE sends CoA notifications to the following network devices:

- Network device with single IP address (subnets are not supported)
- Network device configured as a TrustSec device
- Network device set as CoA supported

When Cisco ISE is deployed in a distributed environment where there are several secondaries that interoperate with different sets of devices, CoA requests are sent from Cisco ISE primary node to all the network devices. Therefore, TrustSec network devices need to be configured with the Cisco ISE primary node as the CoA client.

The devices return CoA NAK or ACK back to the Cisco ISE primary node. However, the following TrustSec session coming from the network device would be sent to the Cisco ISE node to which the network devise sends all it's other AAA requests and not necessarily to the primary node.

Push Configuration Changes to Non-CoA Supporting Devices

Some platforms do not support Cisco ISE's "Push" feature for Change of Authorization (CoA), for example: some versions of the Nexus network device. For this case, ISE will connect to the network device and make it to trigger an updated configuration request towards ISE. To achieve this, ISE opens an SSHv2 tunnel to the network device, and the Cisco ISE sends a command that triggers a refresh of the TrustSec policy matrix. This method can also be carried out on network platforms that support CoA pushing.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Network Resources** > **Network Devices**.

Step 2 Check the checkbox next to the required network device and click **Edit**.

Verify that the network device's name, IP address, RADIUS and TrustSec settings are properly configured.

Step 3 Scroll down to **Advanced TrustSec Settings**, and in the **TrustSec Notifications and Updates** section, check the **Send configuration changes to device** checkbox, and click the **CLI (SSH)** radio button.

Step 4 (Optional) Provide an SSH key.

Step 5 Check the **Include this device when deploying Security Group Tag Mapping Updates** check box, for this SGA device to obtain the IP-SGT mappings using device interface credentials.

Step 6 Enter the username and password of the user having privileges to edit the device configuration in the Exec mode.

Step 7 (Optional) Enter the password to enable Exec mode password for the device that would allow you to edit its configuration. You can click **Show** to display the Exec mode password that is already configured for this device.

Step 8 Click **Submit** at the bottom of the page.

The network device is now configured to push Trustsec changes. After you change a Cisco ISE policy, click **Push** to have the new configuration reflected on the network device.

SSH Key Validation

You may want to harden security by using an SSH key. Cisco ISE supports this with its SSH key validation feature.

To use this feature, you open an SSHv2 tunnel from the Cisco ISE to the network device, then use the network device's own CLI to retrieve the SSH key. You then copy this key and paste it into Cisco ISE for validation. Cisco ISE terminates the connection if the SSH key is wrong.

Limitation: Currently, Cisco ISE can validate only one IP (not on ranges of IP, or subnets within an IP)

Before you begin

You will require:

- Login credentials
- CLI command to retrieve the SSH key

for the network device with which you want the Cisco ISE to communicate securely.

Step 1 On the network device:

a) Log on to the network device with which you want the Cisco ISE to communicate using SSH key validation.

b) Use the device's CLI to show the SSH key.

Example:

For Catalyst devices, the command is: `sho ip ssh`.

c) Copy the SSH key which is displayed.

Step 2 From the Cisco ISE user interface:

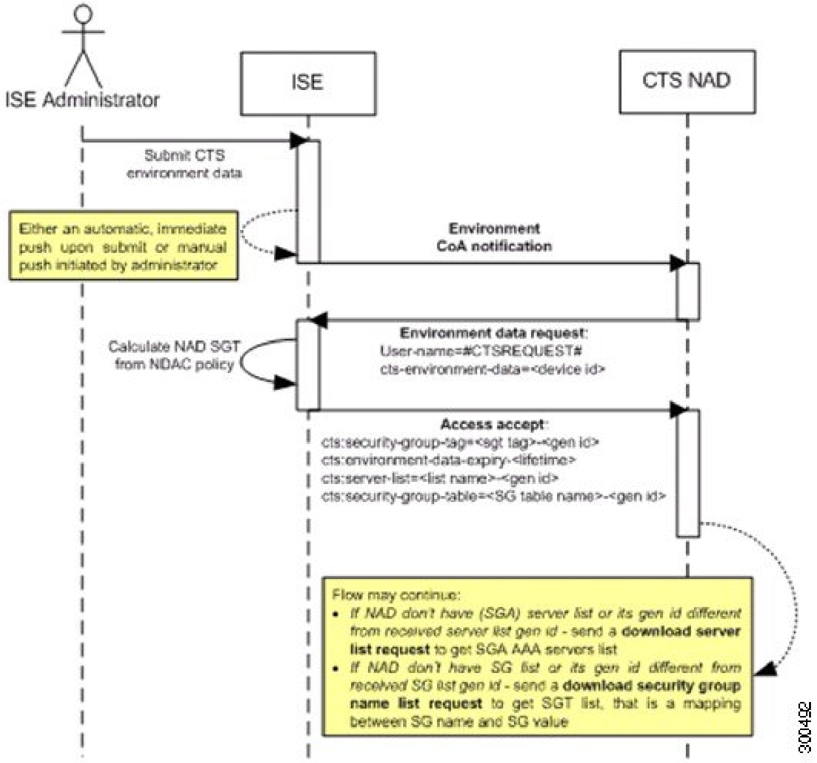
a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Network Resources** > **Network Devices**, and verify the required network device's name, IP address, RADIUS and TrustSec settings are properly configured.
b) Scroll down to **Advanced TrustSec Settings**, and in the **TrustSec Notifications and Updates** section, check the **Send configuration changes to device** checkbox, and click the **CLI (SSH)** radio button.
c) In the **SSH Key** field, paste the SSH key retrieved previously from the network device.
d) Click **Submit** at the bottom of the page.

The network device is now communicating with the Cisco ISE using SSH key validation.

Environment CoA Notification Flow

The following figure depicts the Environment CoA notification flow.

Figure 49: Environment CoA Notification Flow


ISE Administrator
ISE
CTS NAD
Submit CTS environment data
Either an automatic, immediate push upon submit or manual push initiated by administrator
Environment CoA notification
Environment data request:
User-name=#CTSREQUEST#
cts-environment-data=<device id>
Calculate NAD SGT from NDAC policy
Access accept:
cts:security-group-tag=<sgt tag>-<gen id>
cts:environment-data-expiry-<lifetime>
cts:server-list=<list name>-<gen id>
cts:security-group-table=<SG table name>-<gen id>
Flow may continue:
• If NAD don't have (SGA) server list or its gen id different from received server list gen id - send a download server list request to get SGA AAA servers list
• If NAD don't have SG list or its gen id different from received SG list gen id - send a download security group name list request to get SGT list, that is a mapping between SG name and SG value
300492

1. Cisco ISE sends an environment CoA notification to the TrustSec network device.

2. The device returns an environment data request.

3. In response to the environment data request, Cisco ISE returns:

   The environment data of the device that sent the request—This includes the TrustSec device's SGT (as inferred from the NDAC policy) and download environment TTL.

   The name and generation ID of the TrustSec AAA server list.

The names and generation IDs of (potentially multiple) SGT tables—These tables list SGT name versus SGT value, and together these tables hold the full list of SGTs.

4. If the device does not hold a TrustSec AAA server list, or the generation ID is different from the generation ID that is received, the device sends another request to get the AAA server list content.
5. If the device does not hold an SGT table listed in the response, or the generation ID is different from the generation ID that is received, the device sends another request to get the content of that SGT table.

Environment CoA Triggers

An Environment CoA can be triggered for:

- Network devices
- Security groups
- AAA servers

Trigger Environment CoA for Network Devices

To trigger an Environment CoA for the Network devices, complete the following steps:

Step 1 Choose In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Device Administration** > **Network Resources** > **Network Devices**.

Step 2 Add or edit a network device.

Step 3 Update TrustSec Notifications and Updates parameters under the Advanced TrustSec Settings section.

Changing the environment attribute is notified only to the specific TrustSec network device where the change took place.

Because only a single device is impacted, an environmental CoA notification is sent immediately upon submission. The result is a device update of its environment attribute.

Trigger Environment CoA for Security Groups

To trigger an Environment CoA for the security groups, complete the following steps.

Step 1 **Work Centers > TrustSec > Components > Security Groups**.

Step 2 In the Security Group page, change the name of an SGT, which will change the name of the mapping value of that SGT. This triggers an environmental change.

Step 3 Click the **Push** button to initiate an environment CoA notification after changing the names of multiple SGTs. This environment CoA notification goes to all TrustSec network devices and provides an update of all SGTs that were changed.

Trigger Environment CoA for TrustSec AAA Servers

To trigger an Environment CoA for the TrustSec AAA servers, complete the following steps.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Components** > **TrustSec AAA Servers**.

Step 2 In the TrustSec AAA Servers page create, delete or update the configuration of a TrustSec AAA server. This triggers an environment change.

Step 3 Click the **Push** button to initiate an environment CoA notification after you configure multiple TrustSec AAA servers. This environment CoA notification goes to all TrustSec network devices and provides an update of all TrustSec AAA servers that were changed.

Trigger Environment CoA for NDAC Policy

To trigger an Environment CoA for the NDAC Policies, complete the following steps.

Step 1 Choose **Work Centers** > **TrustSec** > **Policy** > **Network Device Authorization**.

In the NDAC policy page you can create, delete, or update rules of the NDAC policy. These environment changes are notified to all network devices.

Step 2 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **TrustSec Policy** > **Network Device Authorization**.

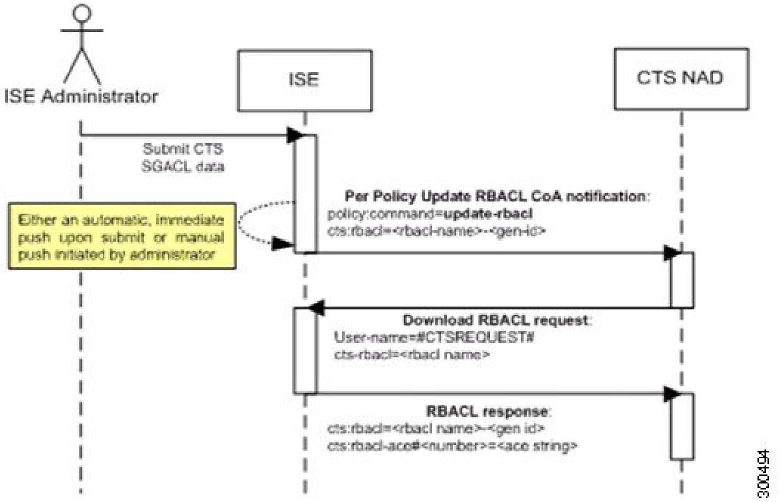
In the NDAC policy page you can create, delete, or update rules of the NDAC policy. These environment changes are notified to all network devices.

Step 3 You can initiate an environment CoA notification by clicking the **Push** button in the NDAC policy page. This environment CoA notification goes to all TrustSec network devices and provides an update of network device own SGT.

Update SGACL Content Flow

The following figure depicts the Update SGACL Content flow.

Figure 50: Update SGACL Content Flow


ISE Administrator
ISE
CTS NAD
Submit CTS SGACL data
Either an automatic, immediate push upon submit or manual push initiated by administrator
Per Policy Update RBACL CoA notification:
policy:command=update-rbacl
cts:rbacl=<rbacl-name>-<gen-id>
Download RBACL request:
User-name=#CTSREQUEST#
cts-rbacl=<rbacl name>
RBACL response:
cts:rbacl=<rbacl name>-<gen id>
cts:rbacl-ace#<number>=<ace string>
300494

1. Cisco ISE sends an update SGACL named list CoA notification to a TrustSec network device. The notification contains the SGACL name and the generation ID.
2. The device may replay with an SGACL data request if both of the following terms are fulfilled:

   If the SGACL is part of an egress cell that the device holds. The device holds a subset of the egress policy data, which are the cells related to the SGTs of its neighboring devices and endpoints (egress policy columns of selected destination SGTs).

   The generation ID in the CoA notification is different from the generation ID that the device holds for this SGACL.
3. In response to the SGACL data request, Cisco ISE returns the content of the SGACL (the ACE).

Initiate an Update SGACL Named List CoA

To trigger an Update SGACL Named List CoA, complete the following steps:

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Components** > **Security Group ACLs**.

Step 2 Change the content of the SGACL. After you submit a SGACL, it promotes the generation ID of the SGACL.

Step 3 Click the **Push** button to initiate an Update SGACL Named List CoA notification after you change the content of multiple SGACLs. This notification goes to all TrustSec network devices, and provides an update of that SGACL content on the relevant devices.

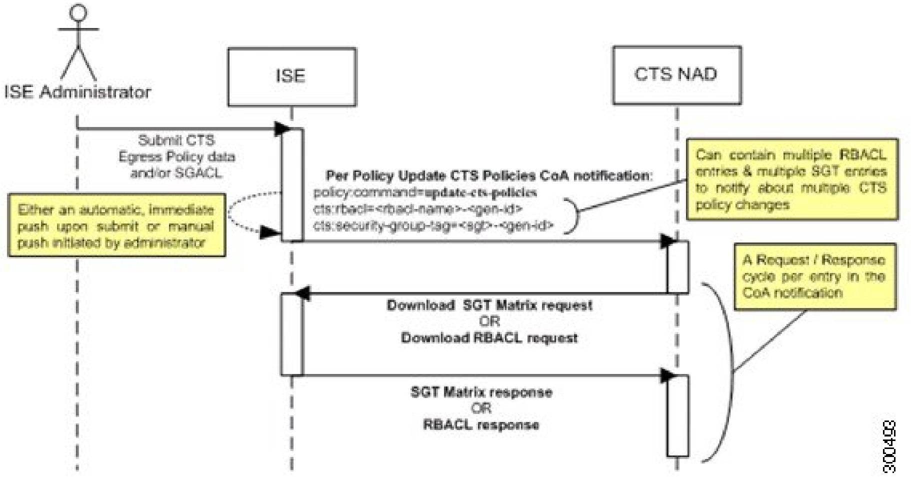
Changing the name or the IP version of an SGACL does not change its generation ID; hence it does not require sending an update SGACL named list CoA notification.

However, changing the name or IP version of an SGACL that is in use in the egress policy indicates a change in the cell that contains that SGACL, and this changes the generation ID of the destination SGT of that cell.

Policies Update CoA Notification Flow

The following figure depicts the Policies CoA Notification flow.

Figure 51: Policies CoA Notification flow

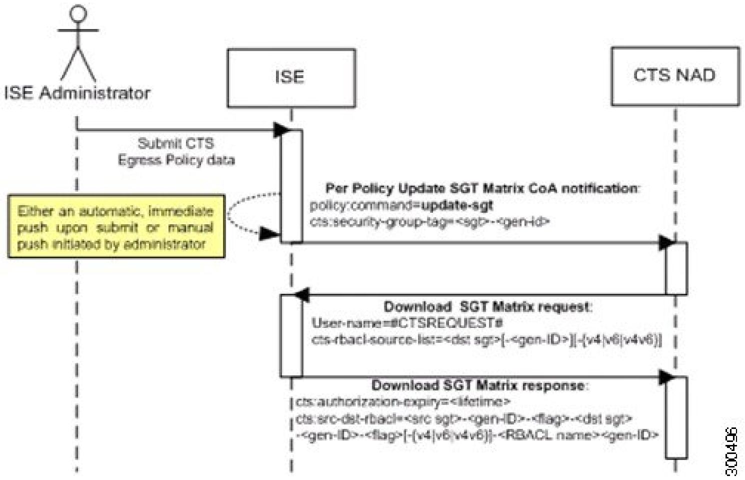

ISE Administrator
ISE
CTS NAD
Submit CTS Egress Policy data and/or SGACL
Either an automatic, immediate push upon submit or manual push initiated by administrator
Per Policy Update CTS Policies CoA notification:
policy:command=update-cts-policies
cts:rbacl=<rbacl-name>-<gen-id>
cts:security-group-tag=<sgt>-<gen-id>
Can contain multiple RBACL entries & multiple SGT entries to notify about multiple CTS policy changes
A Request / Response cycle per entry in the CoA notification
Download SGT Matrix request
OR
Download RBACL request
SGT Matrix response
OR
RBACL response
300493

1. Cisco ISE sends an update policies CoA notification to a TrustSec network device. The notification may contain multiple SGACL names and their generation IDs, and multiple SGT values and their generation IDs.
2. The device may replay with multiple SGACL data requests and/or multiple SGT data.
3. In response to each SGACL data request or SGT data request, Cisco ISE returns the relevant data.

Update SGT Matrix CoA Flow

The following figure depicts the Update SGT Matrix CoA flow.

Figure 52: Update SGT Matrix CoA flow


ISE Administrator
ISE
CTS NAD
Submit CTS Egress Policy data
Either an automatic, immediate push upon submit or manual push initiated by administrator
Per Policy Update SGT Matrix CoA notification:
policy:command=update-sgt
cts:security-group-tag=<sgt>-<gen-id>
Download SGT Matrix request:
User-name=#CTSREQUEST#
cts-rbacl-source-list:=<dst sgt>[-<gen-ID>][-(v4|v6|v4v6)]
Download SGT Matrix response:
cts:authorization-expiry=<lifetime>
cts:src-dst-rbacl=<src sgt>-<gen-ID>-<flag>-<dst sgt>-<gen-ID>-<flag>[-(v4|v6|v4v6)]-<RBACL name><gen-ID>
300496

1. Cisco ISE sends an updated SGT matrix CoA notification to a TrustSec network device. The notification contains the SGT value and the generation ID.
2. The device may replay with an SGT data request if both the following terms are fulfilled:

   If the SGT is the SGT of a neighboring device or endpoint, the device downloads and hold the cells related to SGTs of neighboring devices and endpoints (a destination SGT).

   The generation ID in the CoA notification is different from the generation ID that the device holds for this SGT.
3. In response to the SGT data request, Cisco ISE returns the data of all egress cells, such as the source and destination SGTs, the status of the cell, and an ordered list of the SGACL names configured in that cell.

Initiate Update SGT Matrix CoA from Egress Policy

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **TrustSec Policy** > **Egress Policy**.

Step 2 On the Egress Policy page, change the content of a cell (status, SGACLs).

Step 3 After you submit the changes, it promotes the generation ID of the destination SGT of that cell.

Step 4 Click the **Push** button to initiate the Update SGT matrix CoA notification after you change the content of multiple egress cells. This notification goes to all TrustSec network devices, and provides an update of cells content on the relevant devices.

TrustSec CoA Summary

The following table summarizes the various scenarios that may require initiating a TrustSec CoA, the type of CoA used in each scenario, and the related UI pages.

Table 158: TrustSec CoA Summary

UI Page	Operation that triggers CoA	How it is triggered	CoA type	Send to
Network Device	Changing the environment TTL in the TrustSec section of the page	Upon successful Submit of TrustSec network device	Environment	The specific network device
TrustSec AAA Server	Any change in the TrustSec AAA server (create, update, delete, reorder)	Accumulative changes can be pushed by clicking the Push button on the TrustSec AAA servers list page.	Environment	All TrustSec network devices

UI Page	Operation that triggers CoA	How it is triggered	CoA type	Send to
Security Group	Any change in the SGT (create, rename, delete)	Accumulative changes can be pushed by clicking the Push button on the SGT list page.	Environment	All TrustSec network devices
NDAC Policy	Any change in the NDAC policy (create, update, delete)	Accumulative changes can be pushed by clicking the Push button on the NDAC policy page.	Environment	All TrustSec network devices
SGACL	Changing SGACL ACE	Accumulative changes can be pushed by clicking the Push button on the SGACL list page.	Update RBACL named list	All TrustSec network devices
	Changing SGACL name or IP version	Accumulative changes can be pushed by clicking the Push button on the SGACL list page or the policy push button in the Egress table.	Update SGT matrix	All TrustSec network devices
Egress Policy	Any operation that changes the generation ID of an SGT	Accumulative changes can be pushed by clicking the Push button on the egress policy page.	Update SGT matrix	All TrustSec network devices

Security Group Tag Exchange Protocol

Security Group Tag (SGT) Exchange Protocol (SXP) is used to propagate the SGTs across network devices that do not have hardware support for TrustSec. SXP is used to transport an endpoint's SGT along with the IP address from one SGT-aware network device to another. The data that SXP transports is called as IP-SGT mapping. The SGT to which an endpoint belongs can be assigned statically or dynamically, and the SGT can be used as a classifier in network policies.

To enable SXP service on a node, check the Enable SXP Service check box in the General Node Settings page. You must also specify the interface to be used for SXP service.

SXP uses TCP as its transport protocol to set up SXP connection between two separate network devices. Each SXP connection has one peer designated as SXP speaker and the other peer as SXP listener. The peers can also be configured in a bi-directional mode where each of them act as both speaker and listener. Connections can be initiated by either peers, but mapping information is always propagated from a speaker to a listener.

Note Session bindings are always propagated on the default SXP domain.

The following table lists some of the common terms used in the SXP environment:

IP-SGT mapping	The IP Address to SGT mapping that is exchanged over SXP connection. To view all the mappings learned by the SXP devices (including static mappings and session mappings), choose **Work Centers** > **TrustSec** > **SXP** > **All SXP Mappings**.
SXP Speaker	The peer that sends the IP-SGT mappings over the SXP connection.
SXP Listener	The peer that receives the IP-SGT mappings over the SXP connection.

To view the SXP peer devices that are added to Cisco ISE, choose **Work centers** > **TrustSec** > **SXP** > **SXP Devices**.

Note We recommend that you run the SXP service on a standalone node.

Note the following points while using the SXP service:

- You must update the SXP device configuration with the connected PSN details in case of upgrade, node failure, or node configuration updates.
- When you deregister an SXP node and reregister it back to the existing deployment, the SXP devices that are connected to that node are removed from the deployment. These devices are not displayed in the **SXP Devices** window (**Work Centers** > **TrustSec** > **SXP** > **SXP Devices**). You must manually re-add these devices after reregistering the SXP node to the deployment. However, the SXP devices are not removed if the SXP service on an SXP node is disabled.
- Cisco ISE does not support multiple SXP session bindings with same IP address.
- If the RADIUS accounting updates are too frequent (for example, around 6 to 8 accounting updates in few seconds), sometimes the accounting update packet might be dropped and SXP might not receive the IP-SGT binding.
- After upgrading from a previous version of ISE, SXP does not start automatically. After the upgrade, you must change the SXP password and restart the SXP process.

Add an SXP Device

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Work Centers** > **TrustSec** > **SXP** > **SXP Devices**.

Step 2 Click **Add**.

Step 3 Enter the device details:

- Click **Upload from a CSV file** to add the SXP devices using a CSV file. Browse and select the CSV file, and then click **Upload**.

  You can also download the CSV template file, fill in the details of the devices that you want to add, and upload the CSV file.

- Click **Add Single Device** to add the device details manually for each SXP device.

  Enter the name, IP address, SXP role (listener, speaker, or both), password type, SXP version, and connected PSNs for the peer device. You must also specify the SXP domain to which the peer device is connected.

Step 4 (Optional) Click **Advanced Settings** and enter the following details:

- Minimum Acceptable Hold Timer—Specify the time, in seconds, a speaker will send keepalive messages for keeping the connection alive. The valid range is from 1 to 65534.
- Keep Alive Timer—Used by a speaker to trigger the dispatch of keepalive messages during intervals when no other information is exported via update messages. The valid range is from 0 to 64000.

Step 5 Click **Save**.

Add an SXP Domain Filter

You can view all the mappings learned by the SXP devices (including static mappings and session mappings). To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **SXP** > **All SXP Mappings**.

By default, session mappings learnt from the network devices are sent only to the default VPN group (called default). You can create SXP domain filters to send the mappings to different SXP domains (VPNs).

If the virtual network is not specified for a network device, Cisco ISE assigns that binding to the default virtual network (called DEFAULT_VN). The SXP filter has an internal rule routing “DEFAULT_VN” to “default” VPN.

When a new virtual network is created in Catalyst Center or when a virtual network creation ERS request is received, a new VPN is created in Cisco ISE. For example, when VN1 is created in Catalyst Center, a new VPN (SDA_VN1) is created in Cisco ISE. In addition, a new SXP filter rule (routing VN1 to SDA_VN1) is created internally in Cisco ISE. If you want the bindings from VN1 to be propagated to SDA_VN1, then SDA_VN1 must be assigned to those SXP devices.

You can assign a virtual network to an authorization profile. When an authentication request (Access-Request) is accepted, Cisco ISE adds the SGT, virtual network, and VLAN details in the response (Access-Accept). NADs must send the same SGT and virtual network in later requests like accounting-start or accounting-interim as Cisco AV pairs as shown below:

- cisco-av-pair=cts:security-group-tag
- cisco-av-pair=cts:vn

Note From Cisco ISE 3.0 onwards, a network device can be part of more than one SXP domain.

To add an SXP domain filter:

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **SXP** > **All SXP Mappings**.

Step 2 Click **Add SXP Domain Filter**.

Step 3 Do the following:

- Enter the subnet details. The session mappings of the network devices with IP addresses from this subnet are sent to the SXP domain (VPN) that is selected in the **SXP Domain** field.
- Select an SGT from the SGT drop-down list. The session mappings that are related to this SGT are sent to the SXP domain that is selected in the **SXP Domain** field.

  If you have specified both Subnet and SGT, the session mappings that match this filter are sent to the SXP domain that you have selected in the **SXP Domain** field.
- Specify the virtual network in the **VN** field. The session mappings that are related to this virtual network are sent to the SXP domain that is selected in the **SXP Domain** field.
- Select the SXP domain to which the mappings must be sent.

Step 4 Click **Save**.

You can also update or delete the SXP domain filters. To update a filter, click **Manage SXP Domain Filter**, check the check box next to the filter that you want to update, and then click **Edit**. To delete a filter, check the check box next to the filter that you want to delete, and then click **Trash** > **Selected**.

Configure SXP Settings

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Settings** > **SXP Settings**.

Step 2 Check the following check boxes:

- **Publish SXP Bindings on pxGrid**
- **Add Radius and PassiveID Mappings into SXP IP SGT Mapping Table**

If you uncheck the **Publish SXP Bindings on pxGrid** check box, the IP-SGT mappings will not be published through the pxGrid SXP topics.

Step 3 Enter the required details in the SXP Settings page.

Step 4 Click **Save**.

Note

- When the SXP settings are changed, the SXP service is restarted.
- You must update the SXP device configuration with the connected PSN details in case of upgrade, node failure, or node configuration updates.

Connect Cisco Application Centric Infrastructure with Cisco ISE

Cisco ISE can synchronize SGTs and SXP mappings with the Internal Endpoint Groups (IEPGs), External Endpoint Groups (EEPGs), and endpoint (EP) configuration of Cisco Application Centric Infrastructure (Cisco ACI).

Cisco ISE supports packets coming from the Cisco ACI domain to the TrustSec domain by synchronizing the IEPGs, and creating correlating read-only SGTs in ISE. These SGTs map the endpoints configured in Cisco ACI, and create correlating SXP mappings in ISE. The SGTs displayed on the Security Groups page (with the value "Cisco ACI" in the Learned From field). You can view the SXP mappings on the All SXP Mappings page. These mappings are sent to Cisco ACI only if the Policy Plane option is selected (in the Cisco ACI Settings page) and the SXP device belongs to an SXP domain, that you configured on the Cisco ACI Settings page.

Note You can’t use read-only SGTs in IP-SGT mappings, mapping groups, and SXP local mappings.

When you add a Security Group, you can specify whether the SGT is sent to Cisco ACI by enabling the **Propagate to ACI** option. When this option is enabled, the SXP mappings that are related to this SGT are sent to Cisco ACI. But, only if the Policy Plane option is selected (in the Cisco ACI Settings page) and the SXP device belongs to an SXP Domain, which you configure on the Cisco ACI Settings page.

Cisco ACI supports the packets that are sent from the TrustSec domain to the Cisco ACI domain by synchronizing the SGTs, and creating correlating EEPGs. Cisco ACI creates subnets under EEPG based on the SXP mappings from Cisco ISE. These subnets are not deleted from Cisco ACI, when the corresponding SXP mappings are deleted in Cisco ISE.

When an IEPG is updated in Cisco ACI, the corresponding SGT configuration is updated in Cisco ISE. A new EEPG is created in Cisco ACI, when an SGT is added in Cisco ISE. When an SGT is deleted, the corresponding EEPG is deleted in Cisco ACI. When an endpoint is updated in Cisco ACI, the corresponding SXP mapping is updated in Cisco ISE.

If the connection with the Cisco ACI server is lost, Cisco ISE re-synchronizes the data again when the connection is reestablished.

Note You must enable the SXP service to use the Cisco ACI integration feature.

You can view all the bindings sent to Cisco ACI from Cisco ISE and vice versa in the **All ACI Mappings** window. To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **ACI**. When the binding is learned from the Cisco ACI, the **Learned By** column displays **ACI** and the **PSNs involved** column is empty. Whereas when the binding is sent to Cisco ACI from Cisco ISE, the **Learned By** column displays the type of binding such as static, SXP or session and the **PSNs involved** column displays the FQDN of the PSNs involved. Tenant information is also displayed for the bindings that are sent to ACI in the **VN** column (in *tenant:VN* format).

To successfully integrate Cisco ISE and Cisco ACI, the signed certificate should have proper SAN fields. Cisco ISE will use values specified in the SAN extension property of the certificate presented by the APIC server.

Note Only IPv4-SXP bindings with Cisco ACI are currently supported by Cisco ISE. IPv6-SGT bindings from Cisco ACI are not supported.

Configure ACI Settings

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Trusted Certificates** > **Import**.

Step 2 Import the Cisco ACI certificate.

Step 3 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Settings** > **ACI Settings**.

Step 4 Check the **Enable ACI Integration** check box to learn endpoints from Cisco ACI and propagate them using SXP.

Step 5 Select one of the following options:

- **Data Plane / Hardware Integration**
- **Policy Plane / API Integration**

Note If you choose **Data Plane / Hardware Integration**, Cisco ISE must be integrated with Catalyst Center. If you choose **Policy Plane / API Integration**, SXP propagation is not possible without active SXP service. Activate SXP service in the **Deployment** window before selecting this option.

Step 6 Enter the following details if you select **Data Plane / Hardware Integration**:

- **IP address**: Enter the IP address or hostname of the Cisco ACI server. You can enter three IP addresses or host names separated by commas.
- **Username**: Enter the username of the Cisco ACI admin user.
- **Password**: Enter the password of the Cisco ACI admin user.
- **Tenant name**: Enter the name of the tenant that is configured on the Cisco ACI.
- **Test Connection to ACI**: Click this button to check the connectivity with the Cisco ACI server.
- **Renew Certificate**: Click this button to perform a domain manager refresh.

  A certificate is typically valid for 10 years. Successful peering should be available in the system before renewing the certificate. The Cisco ISE application has to be restarted from the CLI of all the nodes in the deployment after renewing the certificate. The approximate time to renew the certificate is five minutes.
- **New SGT Suffix**: This suffix will be added to the SGTs that are newly created based on the EPGs learnt from Cisco ACI.

  Note The EPG name will be truncated if it is greater than 32 characters. However, you can view the full name of the EPG, application profile name, and SGT suffix details in the Description field in the Security Groups listing page.
- **New EPG Suffix**: This suffix will be added to the EPGs that are newly created in Cisco ACI based on the SGTs learnt from Cisco ISE.
- **Enable Data Plane**: Check this check box to download the translation table for the border routers. If you enable the check box, you must select the default SGT name for the packets that cannot be matched to any other existing SGT.
  - **Default SGT name**: Choose the default name for the SGT from the drop-down list.
- **Enable Elements Limit**: This option is available only if you enable the data plane.
  - **Max number of IEPGs**: Specify the maximum number of IEPGs that will be converted to SGTs. IEPGs are converted in alphabetical order. Default value is 1000.
  - **Max number of SGTs**: Specify the maximum number of SGTs that will be converted to IEPGs. SGTs are converted in alphabetical order. Default value is 500.

Step 7 Enter the following details if you have selected the **Policy Plane / API Integration** option:

- **IP address / Hostname**: Enter the IP address or hostname of the Cisco ACI server. You can enter three IP addresses or host names separated by commas.
- **Admin name**: Enter the username of the Cisco ACI admin user.
- **Admin password**: Enter the password of the Cisco ACI admin user.
- **Tenant name**: Enter the name of the tenant that is configured on the Cisco ACI.

- **L3 Route network name**: Enter the name of the Layer 3 Route network that is configured on the Cisco ACI for synchronizing the policy elements.
- **Test Settings**: Click this button to check the connectivity with the Cisco ACI server.
- **New SGT Suffix**: This suffix will be added to the SGTs that are newly created based on the EPGs learnt from Cisco ACI.
- **New EPG Suffix**: This suffix will be added to the EPGs that are newly created in Cisco ACI based on the SGTs learnt from Cisco ISE.
- In the **SXP Propagation** area, you can select all the SXP domains or specify the SXP domains that will share the mappings with Cisco ACI.
- **Enable Data Plane**: Check this check box to download the translation table for the border routers. If you enable the check box, you must select the default SGT name for the packets that cannot be matched to any other existing SGT.
  - **EEPG name for untagged packets**: Cisco TrustSec packets that are not converted to an EEPG are tagged with this name in Cisco ACI.
  - **Default SGT name**: Choose the default name for the SGT from the drop-down list.
- **Enable Elements Limit**: This option is available only if you enable the data plane.

Step 8 Click **Save**.

Note You cannot change the EPG and SGT suffix when the ACI integration option is enabled. To change the EPG and SGT suffix, you must first disable the **Enable ACI Integration** option.

Cisco ACI and Cisco SD-Access Integration with Virtual Network Awareness

In Cisco ISE Release 2.7, there is a basic implementation of synchronizing SGT and SXP mappings with the Internal Endpoint Groups (IEPGs), External Endpoint Groups (EEPGs), and endpoint configuration of Cisco ACI.

Cisco ISE Release 3.0 supports an extra implementation that provides enhanced conversion of information exchange and cross-domain automation for a Cisco Software-Defined Access (SD-Access) fabric with Cisco ACI infrastructure. This implementation supports the following:

- Exchange and translation of EPG and SGT information
- Extension of Cisco SD-Access virtual networks into the Cisco ACI fabric
- Cisco SD-Access and Cisco ACI fabric dataplane automation
- Exchange of IP-SGT bindings
- Send the bindings to pxGrid and SXP domains

Cisco ISE learns the virtual network information from RADIUS bindings or Cisco ACI bindings, and provides a local static mapping for a specific virtual network. A virtual network can be used to enhance the SXP filter logic that is leveraged to coordinate the sharing of IP-SGT bindings with Cisco ACI. Note that the SXP domains and virtual networks are closely linked, in the sense that the virtual networks that are extended to Cisco ACI are the only constructs to share IP-SGT bindings with Cisco ACI. Therefore, specific SXP domains (denoted with the SD-Access- prefix) are mapped to the equivalent virtual network (SXP domain minus the SD-Access- prefix) in Cisco ISE.

In order to allow the Cisco SD-Access border node to know about the Cisco ACI bindings, the Cisco ACI bindings are replicated as if they were originated from all the extended virtual networks before they are sent through the SXP filter logic. For example, a binding from Cisco ACI with the original Cisco ACI virtual network is sent through the SXP filter four times, if Cisco SD-Access virtual network 1, virtual network 2 and virtual network 3 are extended to Cisco ACI. This exact same binding goes through the filter for all the four virtual networks. The filters can be modified and customized as per specific deployment requirements. However, the replication will always happen for all extended virtual networks.

Cisco ISE learns about the IP-SGT, EPG bindings from Cisco ACI whenever possible. However, Cisco ISE cannot force Cisco ACI to learn about any bindings. Cisco ACI has to explicitly request for the bindings from Cisco ISE.

The following table lists the source and destination combinations that are possible for IP-SGT or IP-EPG bindings in Cisco ISE.

Source Domain	Destination Domain	Source Grouping	Destination Grouping	Notes
Cisco ACI	SXP	Cisco ACI virtual network	SXP domain	Cisco ACI virtual network can be used as a key in the SXP filter to share the binding with one or more SXP domains.
Cisco ACI	PxGrid	Cisco ACI virtual network	VPN for SXP topic on PxGrid	Cisco ACI virtual network can be used as a key in the SXP filter to share the binding with one or more SXP VPNs on pxGrid.
Cisco ACI	Cisco SD-Access border node	Cisco SD-Access extended virtual network	SXP domain	The Cisco ACI bindings are shared with all the SXP domains that are auto-created for the border node virtual network information exchange (“SD-Access-“ prefixed domains).

Cisco ISE static mapping	SXP	Cisco SD-Access virtual network or existing SXP domain	SXP domain	The static bindings can be sent to the SXP domain either directly (specify SXP domain in static mapping) or through the SXP filter (along with the virtual network information). If no virtual network is specified, then the SXP filter uses the DEFAULT_VN for the virtual network.
Cisco ISE static mapping	pxGrid	Cisco SD-Access virtual network	SXP domain	The static bindings can be sent to the SXP domain either directly (specify SXP domain in static mapping) or through the SXP filter (along with the virtual network information). If no virtual network is specified, then the SXP filter uses the DEFAULT_VN for the virtual network.
Cisco ISE static mapping	Cisco ACI	Cisco SD-Access virtual network	Cisco SD-Access virtual network	The Cisco SD-Access virtual network must be extended into Cisco ACI (mdpExtendvirtual networkReq) and the binding uses the virtual network in the SXP filter to send the binding to Cisco ACI, with the SXP domain mapped to a virtual network.
SXP	pxGrid	SXP domain	SXP domain	The SXP domain shows up as a VPN in the SXP topic on pxGrid.

SXP	Cisco ACI	SXP domain	Cisco SD-Access virtual network	SXP domain sharing is selected under Cisco ACI settings. Only the SXP Domain which is auto-created by the Cisco SD-Access virtual network (virtual network equivalent SXP Domain), is shared. The Cisco SD-Access virtual network should be extended to Cisco ACI for the virtual network to have a chance of sharing the bindings. The bindings must be a part of the consumer service for which Cisco ACI requests endpoint data.
SXP	SXP	SXP Domain	SXP Domain	SXP bindings that make it through prioritization are shared.
RADIUS bindings	Cisco ACI	Cisco SD-Access virtual network	Cisco SD-Access virtual network	The RADIUS bindings are sent through SXP filter (along with the virtual network information). If no virtual network is specified for the binding, then the SXP filter uses DEFAULT_VN for the virtual network.
RADIUS bindings	pxGrid	Cisco SD-Access virtual network	Cisco SD-Access virtual network	The RADIUS bindings make it to the session directory topic on pxGrid with the virtual network field added to the topic.

RADIUS bindings	SXP	Cisco SD-Access virtual network	SXP domain	Cisco SD-Access virtual network can be used as a key in the SXP filter to select an SXP domain to share the binding with.

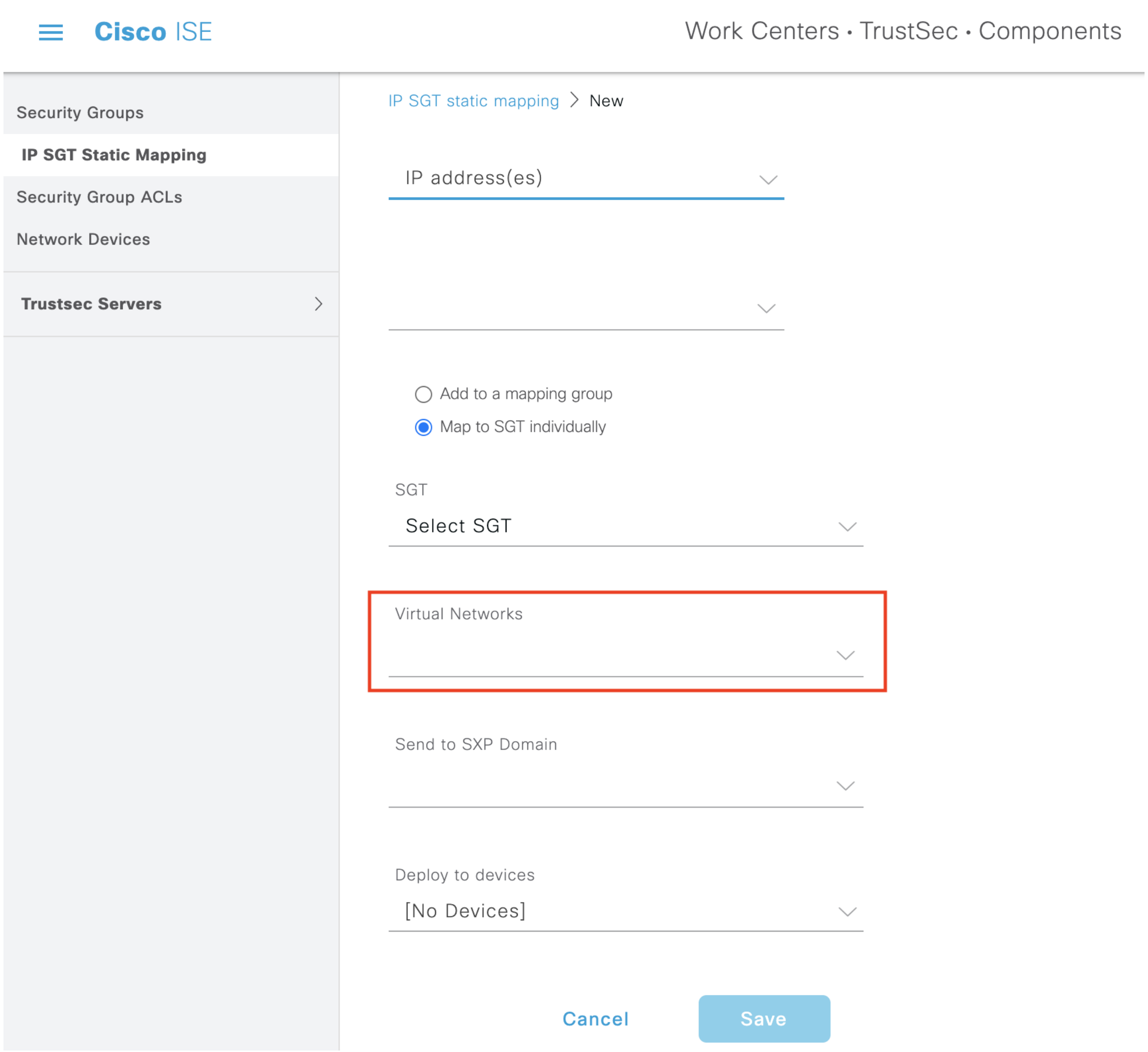
To promote cross-domain support, you must have the ability to exchange and filter the various network forwarding domains, for example, IP address, subnet mask, Security Group Tag, EPGs, virtual networks, Virtual Routing and Forwarding(VRF), from one policy domain, or a forwarding domain within a policy domain, to another and vice versa. This is especially important when a policy domain, for example Cisco SD-Access, Cisco ACI, SD-WAN, CPC, and Meraki, has multiple forwarding domains.

You can identify, capture, and store the policy domain's network-specific forwarding domain and the domain-specific attributes for all the sessions and bindings learned from other policy domains. These will be used by the policy administrator to filter the sessions and bindings into specific SXP domains. In addition, it enables the administrator to create policies that map or filter only certain bindings from one forwarding domain to another.

From Cisco ISE 3.0 onwards, with every virtual network learnt by the Cisco ISE from Catalyst Center, you will find an automatically created SXP filter and an SXP domain in the SXP Devices window. To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **SXP** > **SXP Devices**. These SXP domains will, in turn, be used to set the virtual networks in the bindings shared with Cisco ACI.

You can add and edit virtual networks to IP-SGT static mappings in the IP-SGT Static mapping window. To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **Components** > **IP SGT Static Mapping**. Click **Add** to add a new mapping, or click **Edit** to modify an existing mapping.

Figure 53: Add virtual network in IP SGT Static Mapping


Cisco ISE
Work Centers · TrustSec · Components
Security Groups
IP SGT Static Mapping
Security Group ACLs
Network Devices
Trustsec Servers
IP SGT static mapping > New
IP address(es)
Add to a mapping group
Virtual Networks
Send to SXP Domain
Cancel
Save

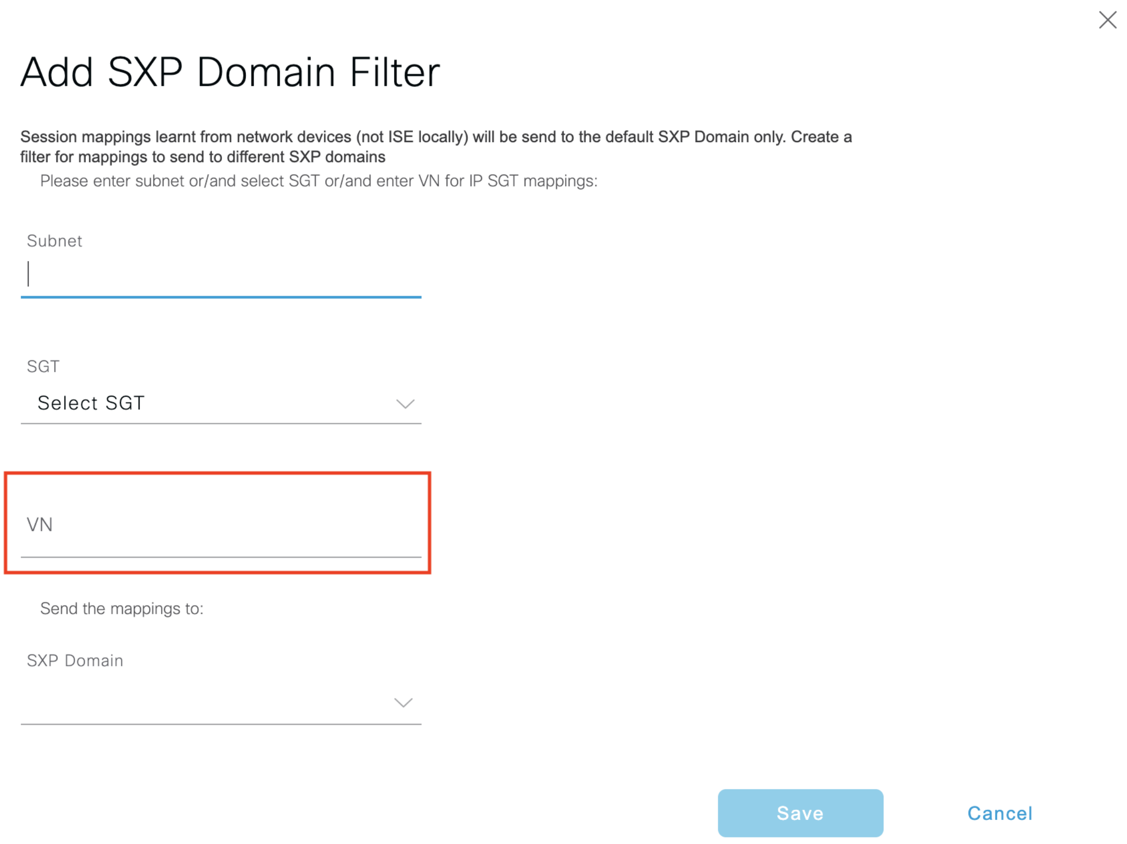
● Map to SGT individually

SGT: Select SGT

Deploy to devices: [No Devices]

You can also include virtual networks in the SXP domain filter to specify which SXP domain to send the mapping to when the mapping received by Cisco ISE is mapped to a particular virtual network. To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **TrustSec** > **SXP** > **SXP Devices** > **SXP mappings** and click **Add SXP Domain Filter**. The bindings learned by Cisco ACI have the original Cisco ACI virtual network, and these are sent to the SXP domain configured in the filter. This filter also influences how a binding is sent to the Cisco ACI.

Figure 54: Add virtual network information in SXP Device Filter



Add SXP Domain Filter

Session mappings learnt from network devices (not ISE locally) will be send to the default SXP Domain only. Create a filter for mappings to send to different SXP domains

Please enter subnet or/and select SGT or/and enter VN for IP SGT mappings:

Send the mappings to:

Configure Cisco ISE for Cisco ACI and Cisco SD-Access Integration

This task helps you to configure Cisco ISE to support Cisco ACI and Cisco SD-Access Integration.

Before you begin

Make sure Cisco ISE is integrated with the latest version of Catalyst Center, and the APIC version being used is 5.1 or later.

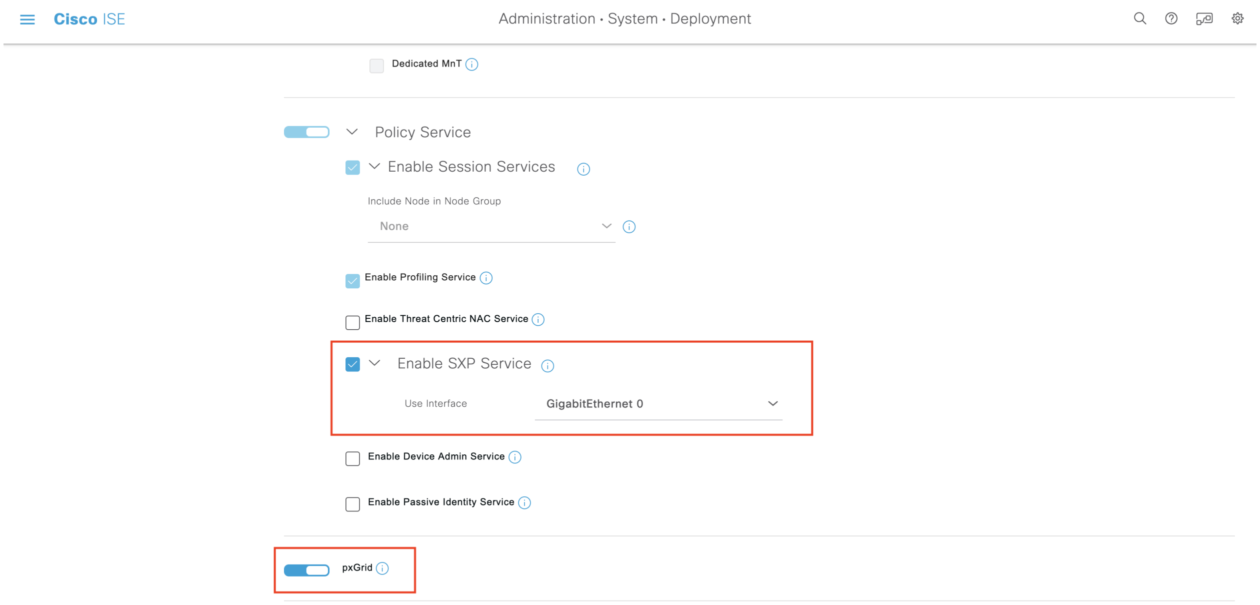
Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 2 From the nodes list, check the check box next to the node for which you want to enable the SXP and pxGrid services.

Step 3 Scroll down to the **Policy Service** section and enable the pxGrid and SXP services as shown in the following figure.

If you have more than one interface enabled on Cisco ISE, in the **Enable SXP Service** area, specify which interface will hold the SXP connection.

Figure 55: Enable SXP and pxGrid services


Cisco ISE
Administration · System · Deployment

☐ Dedicated MnT

Policy Service

☑ Enable Session Services

Include Node in Node Group: None

☑ Enable Profiling Service

☐ Enable Threat Centric NAC Service

☑ Enable SXP Service

Use Interface: GigabitEthernet 0

☐ Enable Device Admin Service

☐ Enable Passive Identity Service

pxGrid

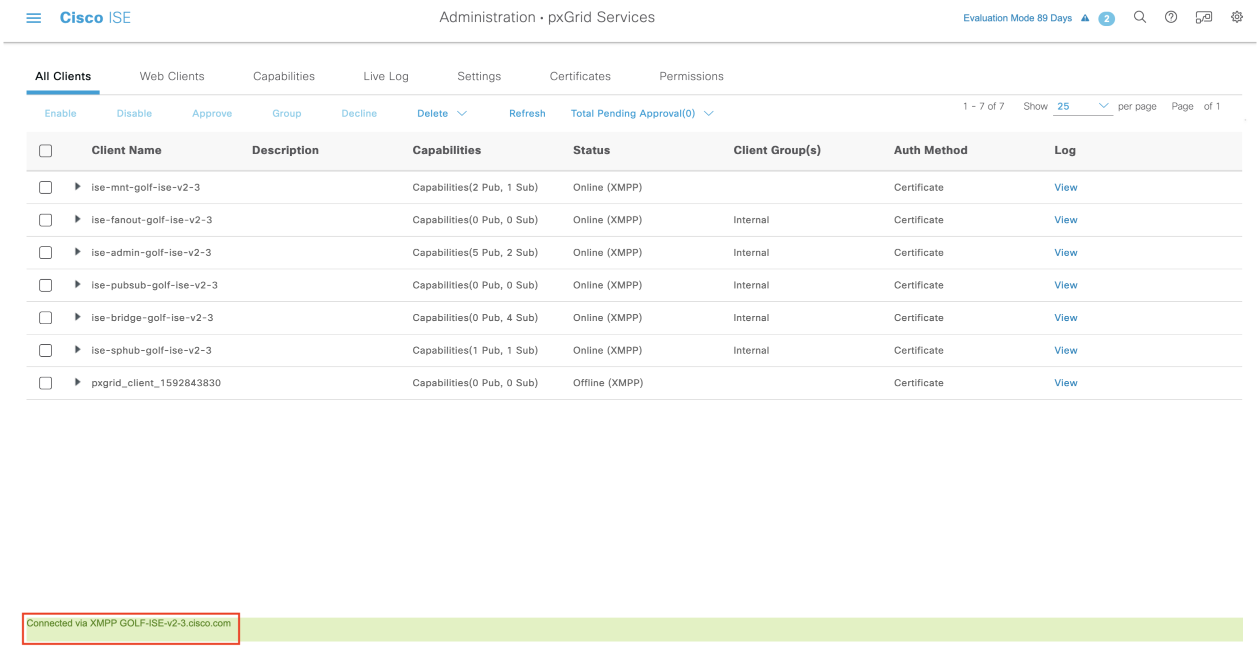
Step 4 Click **Save**.

Step 5 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **pxGrid Services** > **All Clients**.

Step 6 Verify whether the pxGrid service is up and running.

The notification for a successful connection shows up at the bottom-left corner of the window as shown in the following figure:

Figure 56: Verify Connectivity to pxGrid Service


Cisco ISE
Administration · pxGrid Services
Evaluation Mode 89 Days
2
All Clients
Web Clients
Capabilities
Live Log
Settings
Certificates
Permissions
Enable
Disable
Approve
Group
Decline
Delete
Refresh
Total Pending Approval(0)
1 - 7 of 7
Show 25 per page
Page of 1

☐	Client Name	Description	Capabilities	Status	Client Group(s)	Auth Method	Log
☐	ise-mnt-golf-ise-v2-3		Capabilities(2 Pub, 1 Sub)	Online (XMPP)		Certificate	View
☐	ise-fanout-golf-ise-v2-3		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
☐	ise-admin-golf-ise-v2-3		Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate	View
☐	ise-pubsub-golf-ise-v2-3		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
☐	ise-bridge-golf-ise-v2-3		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View
☐	ise-sphub-golf-ise-v2-3		Capabilities(1 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	View
☐	pxgrid_client_1592843830		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate	View

Connected via XMPP GOLF-ISE-v2-3.cisco.com

Step 7 Download the APIC certificates from the APIC controller browser. Click the lock icon in the address bar of the browser to view the certificate and download it as a PEM file.

Step 8 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Trusted Certificates**.

Step 9 Import the downloaded APIC certificate file in the **Trusted Certificates** window.

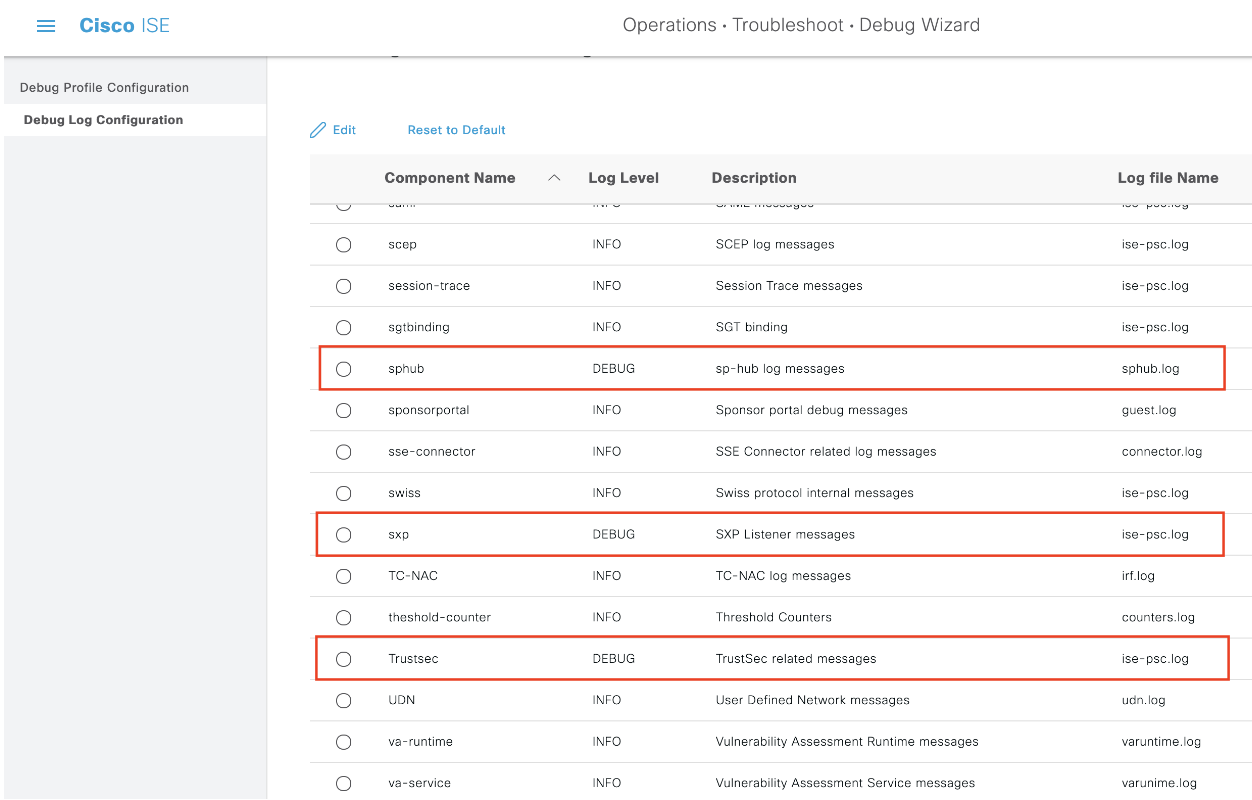
Step 10 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centres** > **TrustSec** > **Settings** > **ACI Settings**.

Step 11 Configure the ACI settings as required. For more information, see Configure ACI Settings, on page 1125.

Verify Cisco ACI and Cisco SD-Access Integration

To get detailed information between the Cisco ACI and Cisco SD-Access connectivity, choose **Operations** > **Troubleshoot** > **Debug Wizard** > **Debug Log Configuration**. Select the Cisco ISE node for which the SXP and pxGrid services are enabled and click Edit. Set the log level to DEBUG for the **spbhub**, **sxp** and **TrustSec** components as shown in the following figure.

Figure 57: Enable debug logs



Cisco ISE
Operations · Troubleshoot · Debug Wizard
Debug Profile Configuration
Debug Log Configuration
Edit
Reset to Default

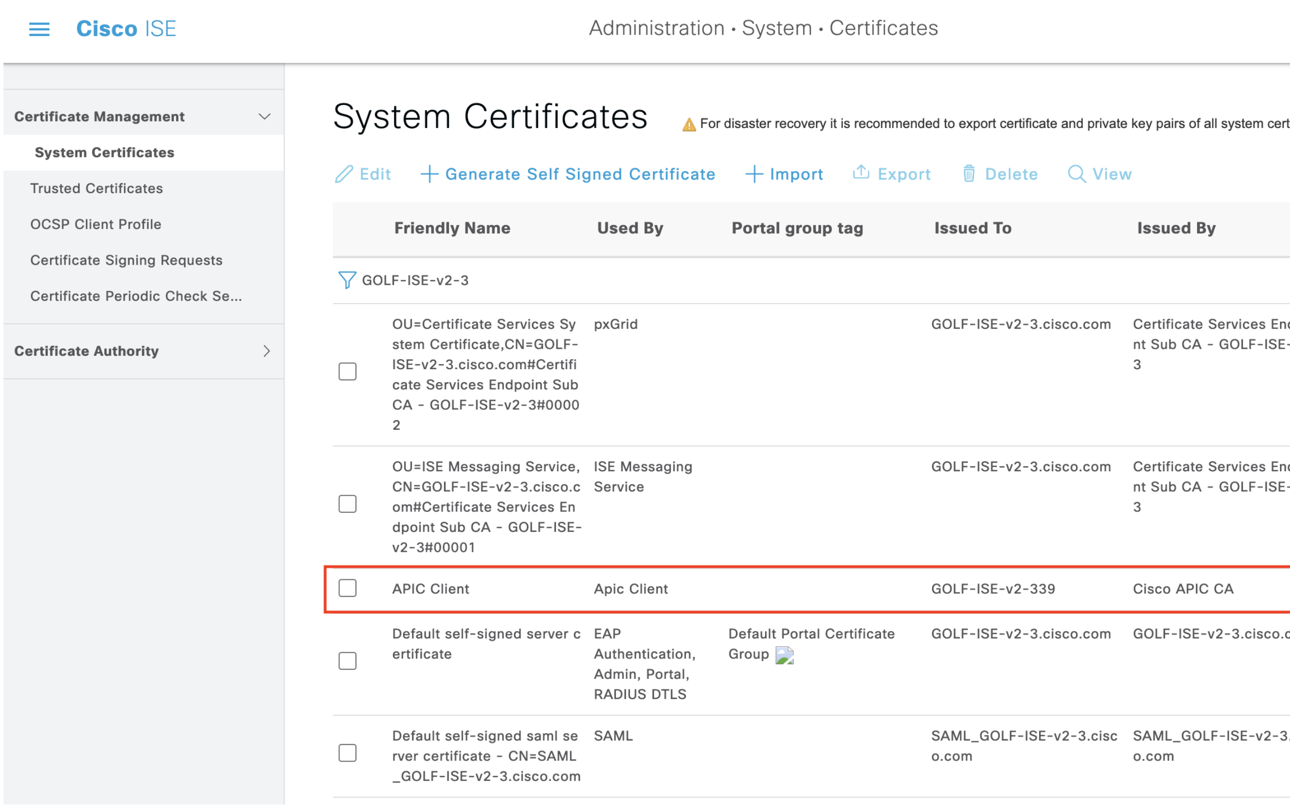
	Component Name	Log Level	Description	Log file Name
○	scep	INFO	SCEP log messages	ise-psc.log
○	session-trace	INFO	Session Trace messages	ise-psc.log
○	sgtbinding	INFO	SGT binding	ise-psc.log
○	sphub	DEBUG	sp-hub log messages	sphub.log
○	sponsorportal	INFO	Sponsor portal debug messages	guest.log
○	sse-connector	INFO	SSE Connector related log messages	connector.log
○	swiss	INFO	Swiss protocol internal messages	ise-psc.log
○	sxp	DEBUG	SXP Listener messages	ise-psc.log
○	TC-NAC	INFO	TC-NAC log messages	irf.log
○	theshold-counter	INFO	Threshold Counters	counters.log
○	Trustsec	DEBUG	TrustSec related messages	ise-psc.log
○	UDN	INFO	User Defined Network messages	udn.log
○	va-runtime	INFO	Vulnerability Assessment Runtime messages	varuntime.log
○	va-service	INFO	Vulnerability Assessment Service messages	varunime.log

The logs can be downloaded from the **Dowload Logs** window. (To view this window, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Dowload Logs**.) You can choose to download either a support bundle from the **Support Bundle** tab or download specific debug logs from the **Debug Logs** tab.

In addtion, the TrustSec Dashboard, on page 1075 is enhanced with the information learnt from the Cisco ACI integration, which is useful for troubleshooting Cisco ACI-related issues.

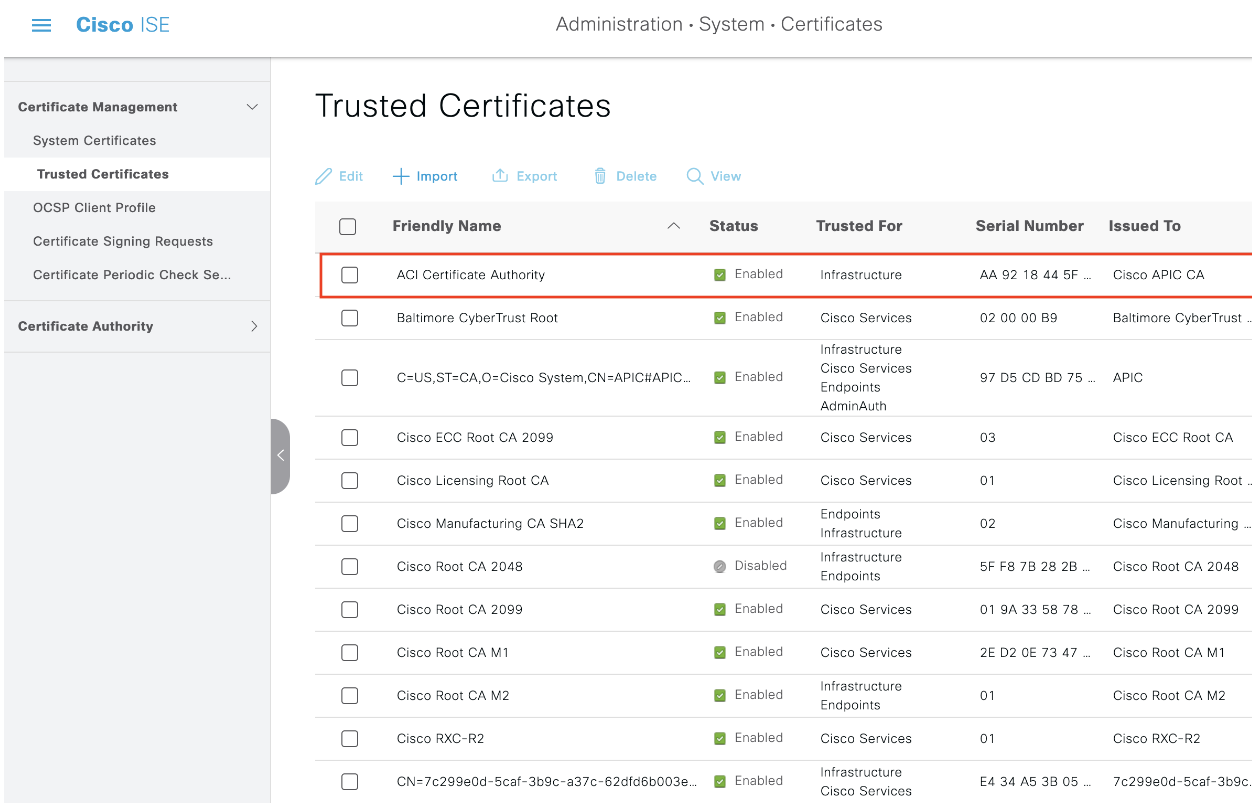
After the Catalyst Center sends out the domain advertisement, confirm whether the APIC certificates are obtained from the APIC domain manager or not, in the both the **Trusted Certificates** window and the **System Certificates** window of Cisco ISE.

Figure 58: Verify the Certificate in System Certificates window


Cisco ISE
Administration • System • Certificates
Certificate Management
System Certificates
Trusted Certificates
OCSP Client Profile
Certificate Signing Requests
Certificate Periodic Check Se...
Certificate Authority
System Certificates
For disaster recovery it is recommended to export certificate and private key pairs of all system cert
Edit
Generate Self Signed Certificate
Import
Export
Delete
View

	Friendly Name	Used By	Portal group tag	Issued To	Issued By
GOLF-ISE-v2-3					
☐	OU=Certificate Services System Certificate,CN=GOLF-ISE-v2-3.cisco.com#Certificate Services Endpoint Sub CA - GOLF-ISE-v2-3#00002	pxGrid		GOLF-ISE-v2-3.cisco.com	Certificate Services En nt Sub CA - GOLF-ISE- 3
☐	OU=ISE Messaging Service, CN=GOLF-ISE-v2-3.cisco.com#Certificate Services Endpoint Sub CA - GOLF-ISE-v2-3#00001	ISE Messaging Service		GOLF-ISE-v2-3.cisco.com	Certificate Services En nt Sub CA - GOLF-ISE- 3
☐	APIC Client	Apic Client		GOLF-ISE-v2-339	Cisco APIC CA
☐	Default self-signed server certificate	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group	GOLF-ISE-v2-3.cisco.com	GOLF-ISE-v2-3.cisco.c
☐	Default self-signed saml server certificate - CN=SAML_GOLF-ISE-v2-3.cisco.com	SAML		SAML_GOLF-ISE-v2-3.cisco.com	SAML_GOLF-ISE-v2-3. o.com

Figure 59: Verify the Certificate in Trusted Certificates window


Cisco ISE
Administration · System · Certificates
Certificate Management
System Certificates
Trusted Certificates
OCSP Client Profile
Certificate Signing Requests
Certificate Periodic Check Se...
Certificate Authority
Trusted Certificates
Edit
Import
Export
Delete
View

☐	Friendly Name	Status	Trusted For	Serial Number	Issued To
☐	ACI Certificate Authority	Enabled	Infrastructure	AA 92 18 44 5F ...	Cisco APIC CA
☐	Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust ...
☐	C=US,ST=CA,O=Cisco System,CN=APIC#APIC...	Enabled	Infrastructure Cisco Services Endpoints AdminAuth	97 D5 CD BD 75 ...	APIC
☐	Cisco ECC Root CA 2099	Enabled	Cisco Services	03	Cisco ECC Root CA
☐	Cisco Licensing Root CA	Enabled	Cisco Services	01	Cisco Licensing Root ...
☐	Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing ...
☐	Cisco Root CA 2048	Disabled	Infrastructure Endpoints	5F F8 7B 28 2B ...	Cisco Root CA 2048
☐	Cisco Root CA 2099	Enabled	Cisco Services	01 9A 33 58 78 ...	Cisco Root CA 2099
☐	Cisco Root CA M1	Enabled	Cisco Services	2E D2 0E 73 47 ...	Cisco Root CA M1
☐	Cisco Root CA M2	Enabled	Infrastructure Endpoints	01	Cisco Root CA M2
☐	Cisco RXC-R2	Enabled	Cisco Services	01	Cisco RXC-R2
☐	CN=7c299e0d-5caf-3b9c-a37c-62dfd6b003e...	Enabled	Infrastructure Cisco Services	E4 34 A5 3B 05 ...	7c299e0d-5caf-3b9c.

Run Top N RBACL Drops by User Report

You can run the Top N RBACL Drops by User report to see the policy violations (based on packet drops) by specific users.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **TrustSec**.

Step 2 Click **Top N RBACL Drops by User**.

Step 3 From the **Filters** drop-down menu, add the required monitor modes.

Step 4 Enter the values for the selected parameters accordingly. You can specify the mode from the Enforcement mode drop-down list as Enforce, Monitor, or Both.

Step 5 From the **Time Range** drop-down menu, choose a time period over which the report data will be collected.

Step 6 Click **Run** to run the report for a specific period, along with the selected parameters.

CHAPTER 13

Compliance

- Posture Types, on page 1140
- Agentless Posture, on page 1142
- Agentless Posture Troubleshooting, on page 1145
- Posture Administration Settings, on page 1145
- Posture General Settings, on page 1152
- Download Posture Updates to Cisco ISE, on page 1153
- Posture Acceptable Use Policy Configuration Settings, on page 1155
- Configure Acceptable Use Policies for Posture Assessment, on page 1156
- Posture Conditions, on page 1157
- Compliance Module, on page 1161
- Check Posture Compliance, on page 1162
- Create Patch Management Conditions, on page 1162
- Create Disk Encryption Conditions, on page 1163
- Posture Condition Settings, on page 1164
- Configure Posture Policies, on page 1186
- Configure AnyConnect Workflow, on page 1188
- Prerequisite for Certificate-Based Conditions, on page 1190
- Default Posture Policies, on page 1192
- Client Posture Assessment, on page 1193
- Posture Assessment Options, on page 1193
- Posture Remediation Options, on page 1195
- Custom Conditions for Posture, on page 1195
- Posture Endpoint Custom Attributes , on page 1196
- Create Posture Policy Using Endpoint Custom Attributes, on page 1196
- Custom Posture Remediation Actions, on page 1197
- Posture Assessment Requirements, on page 1203
- Posture Reassessment Configuration Settings, on page 1205
- Custom Permissions for Posture, on page 1207
- Configure Standard Authorization Policies, on page 1208
- Best Practices for Network Drive Mapping with Posture, on page 1208
- Configure AnyConnect Stealth Mode Workflow, on page 1208
- Enable AnyConnect Stealth Mode Notifications, on page 1212
- Configure Cisco Temporal Agent Workflow, on page 1213

- Posture Troubleshooting Tool, on page 1215
- Configure Endpoint Login Credentials, on page 1215
- Endpoint Scripts Settings, on page 1215
- Configure Client Provisioning in Cisco ISE, on page 1216
- Client Provisioning Resources, on page 1217
- Create Native Supplicant Profiles, on page 1220
- Client Provisioning Without URL Redirection for Different Networks, on page 1223
- AMP Enabler Profile Settings, on page 1224
- Cisco ISE Support for Onboarding Chromebook Devices, on page 1227
- Cisco AnyConnect Secure Mobility, on page 1238
- Posture State Synchronization, on page 1243
- Cisco Web Agent, on page 1245
- Configure Client Provisioning Resource Policies, on page 1245
- Client Provisioning Reports, on page 1248
- Client Provisioning Event Logs, on page 1248
- Portal Settings for Client Provisioning Portals, on page 1248
- HTML Support for Client Provisioning Portal Language Files, on page 1251
- Portal Settings for Client Provisioning Portals, on page 1252
- HTML Support for Client Provisioning Portal Language Files, on page 1254

Posture Types

The following posture agents monitor and enforce Cisco ISE posture policies:

- **AnyConnect**: Deploys the AnyConnect agent to monitor and enforce Cisco ISE posture policies that require interaction with the client. The AnyConnect agent stays on the client. For more information about using AnyConnect in Cisco ISE, see Cisco AnyConnect Secure Mobility, on page 1238.

- **AnyConnect Stealth**: Runs posture as a service, with no user interface. The agent stays on the client.

  When you choose the AnyConnect Stealth posture type in the posture requirement, some of the conditions, remediations, or attributes in a condition are disabled (grayed out). For example, when you enable AnyConnect Stealth requirement, the Manual Remediation Type is disabled (grayed out) because this action requires client-side interaction.

  When you map the posture profile to the AnyConnect configuration, and then map the AnyConnect configuration to the Client Provisioning window for AnyConnect Stealth mode deployment:

  - AnyConnect can read the posture profile and set it to the intended mode.
  - AnyConnect can send information related to the selected mode to Cisco ISE during the initial posture request.
  - Cisco ISE can match the right policy, based on the mode and other factors, such as identity group, OS, and compliance module.

Note AnyConnect Stealth mode requires AnyConnect version 4.4 and later.

For more information about configuring AnyConnect Stealth in Cisco ISE, see Configure AnyConnect Stealth Mode Workflow, on page 1208.

- **Temporal Agent**: When a client attempts to access the trusted network, Cisco ISE opens the Client Provisioning portal. The portal instructs the user to download and install the agent, and run the agent. The temporal agent checks the compliance status, and sends the status to Cisco ISE. Cisco ISE acts based on the results. The temporal agent removes itself from the client after compliance processing completes. The temporal agent does not support custom remediation. The default remediation supports only message text.

  The Temporal Agent does not support the following conditions:

  - Service Condition MAC—System Daemon check
  - Service Condition-MAC—Daemon or User Agent check
  - PM—Up To Date check
  - PM—Enabled check
  - DE—Encryption check

  - Configure posture policies using the **Posture Types Temporal Agent** and **Compliance Module 4.x or later**. Do not configure the compliance module as **3.x or earlier** or **Any Version**.
  - For the Temporal Agent, you can only view Patch Management conditions containing the **Installation** check type in the **Requirements** window.
  - Cisco ISE does not support VLAN-controlled posture with the Temporal Agent for macOS. When you change the network access from an existing VLAN to a new VLAN, the user's IP address is released before the VLAN change. The client gets a new IP address by DHCP when the user connects to the new VLAN. Recognizing the new IP address requires root privileges, but the Temporal Agent runs as a user process.
  - Cisco ISE supports ACL-controlled posture environment, which does not require the refreshing of endpoint IP addresses.
  - For more information about configuring the Temporal agent in Cisco ISE, see Configure Cisco Temporal Agent Workflow, on page 1213.

- **AMP Enabler**—The AMP Enabler pushes the AMP for Endpoints software to a subset of endpoints from a server hosted locally within the enterprise, and installs AMP services to its existing user base.
- **Agentless Posture**—Agentless posture provides posture information from clients, and completely removes itself when finished. No action is required from the end user. Unlike the Temporal agent, Agentless Posture connects to the client as an administrative user. For more information about using Agentless Posture in Cisco ISE, see Agentless Posture, on page 1142.

You can select the posture type in the **Client Provisioning** window (**Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**) and the **Posture Requirements** window (**Policy** > **Policy Elements** > **Results** > **Posture** > **Requirements**). The best practice is to provision the posture profile in the Client Provisioning window.

Related Topics

Configure AnyConnect Stealth Mode Workflow, on page 1208
Configure Cisco Temporal Agent Workflow, on page 1213

Agentless Posture

Agentless posture provides posture information from clients, and completely removes itself when finished, until invoked by Cisco ISE again. No action is required from the end user.

The agentless posture package is available as part of the default Cisco ISE client provisioning resources. You can select this package while creating an agent configuration to be used for the client provisioning policy.

Prerequisites:

- The client must be reachable through its IPv4 address, and that IP address must be available in RADIUS accounting. IPv6 is not supported.
- Windows and Mac clients are currently supported:
  - For Windows clients, port 5985 to access powershell on the client must be open. Powershell must be v5.1 or later. The client must have cURL v7.34 or later.
  - For MacOS clients, port 22 to access SSH must be open to access the client. The client must have cURL v7.34 or later.
- Client credentials for shell login must have local admin privileges.
- Run the posture feed update to get the latest clients, as described in the configuration steps.
- Ensure that the following entry is updated in the sudoers file to avoid certificate installation failure on the endpoints:

  ```
  <macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript
  ```

- For MacOS, the user account that is configured must be an administrator's account. Agentless posture for MacOS does not work with any other account type, even if you grant more privileges. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Endpoint Scripts** > **Login Configuration** > **MAC Local User**.
- In case of changes in port-related activities in Windows clients due to updates from Microsoft, you might have to reconfigure the agentless posture configuration workflow for Windows clients.

Supported Posture Conditions

- File conditions, except the conditions that use the USER_DESKTOP and USER_PROFILE file paths
- Service conditions, except System Daemon and Daemon or User Agent checks on macOS
- Application conditions
- External Data Source conditions
- Compound conditions
- Anti-malware conditions
- Patch management condition, except the **Enabled** and **Up To Date** condition checks
- Firewall conditions
- Disk encryption conditions, except the encryption location-based condition check
- Registry conditions, except the conditions that use HCSK as root key

Note If dual stack protocol is used for authentication in the agentless posture flow, the NADs must also use the same protocol.

Unsupported Posture Conditions

- Remediation
- Grace period
- Periodic Reassessment
- Acceptable Use-policy

Supported Client Operating Systems

- Microsoft Windows versions: 10, 11
- macOS versions: 10.13, 10.14, 10.15, 13.x, and 14

Agentless Posture Process Flow

1. The client connects to the network.
2. Cisco ISE detects if agentless posture is enabled in the authorization profile used by client.
3. If so, Cisco ISE sends an agentless posture job request to the Cisco ISE Messaging queue.
4. Cisco ISE gets the job from the messaging queue, and starts the agentless posture flow.
5. Cisco ISE connects to the client via power shell or SSH.
6. Cisco ISE pushes the certificate, if it’s not already in the client's trust certificate authority store.
7. Cisco ISE runs the client provisioning policy.
8. Cisco ISE pushes the agentless plug-in to the client and launches the plug-in.
9. Posture evaluation runs on the client, and sends the status to Cisco ISE.
10. Cisco ISE removes the agentless plug-in from the client. Logs of the posture flow remain on the client for 24 hours, or until the client deletes them.

Agentless Posture Configuration

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture** > **Requirements**, and create one or more Posture Requirements that use Agentless posture to identify the requirement.
2. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Posture** > **Posture Policy**, and create one or more supported Posture Policy rules that use Agentless posture for that Posture Requirement. You can duplicate the rules you plan to use, and change the Posture type to Agentless.
3. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Authoriation** > **Authorization Profiles** and create an Authorization Profile that evaluates the results from Agentless Posture.

- Enable Agentless posture in the authorization profile.
- Use this profile only for Agentless posture. Do not also use this for other posture types.
- CWA and Redirect ACL is not required for Agentless posture. You can use VLANs, DACLs, or ACLs as part of your segmentation rules.

4. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Client Provisioning** and add a Client Provisioning policy. For the Cisco Agent Configuration, choose the Agentless plug-in for the Operating System that you configured. For Windows, the plug-in is CiscoAgentlessWindows 4.9.01095. For MacOS, the plug-in is CiscoAgentlessOSX 4.9.01095. Select the posture condition this rule checks for. Note, if you're using Active Directory, you can use Active Directory groups in your policy.

Note Agentless posture configuration for MACOSX 10.14 and 10.15 versions aren't available until you update the posture feed. Before you can run the posture feed, update the posture feed URL. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Posture** > **Settings** > **Software Updates** > **Posture Updates**. In the **Posture Updates** window, enter the url (https://www.cisco.com/web/secure/spa/posture-update.xml) in the **Update Feed URL** field and click **Update Now**.

5. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Sets** and expand Authorization Policy. Enable and configure the following three Authorization policies:
   - **Unknown_Compliance_Redirect**: Configure conditions Network_Access_Authentication_Passed AND Compliance_Unknown_Devices with result Agentless Posture.
   - **NonCompliant_Devices_Redirect**: Configure conditions Network_Access_Authentication_Passed and Non_Compliant_Devices with result DenyAccess.
   - **Compliant_Devices_Access**: Configure conditions Network_Access_Authentication_Passed and Compliant_Devices with result PermitAccess.
6. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Settings** > **Endpoint Scripts** > **Endpoint Login Configuration** , and configure the client credentials to log onto clients. These same credentials are used by the Endpoint Scripts.
7. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Settings** > **Endpoint Scripts** > **Settings**, and configure **Max retry attempts for OS identification** and **Delay between retries for OS identification**. These settings determine how quickly connectivity issues can be confirmed. For example, an error that the PowerShell port is not open displays in logs only after all retries are not exhausted.
8. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **General Settings**, and configure the Agentless Posture settings.
9. As clients connect with Agentless posture, you can see them in the Live Logs.

Debugging and Troubleshooting

Enable debug log level for:

- Infrastructure
- Client Provisioning

- Posture

The debug log is in *ise-psc.log*

Agentless Posture Troubleshooting is available under:

- In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Live Logs**—The three dots under the Posture Status column opens Agentless Posture Troubleshooting.
- In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostics** > **General Tools**

Agentless Posture Troubleshooting

The Agentless Posture report is the main troubleshooting tool to use when agentless posture isn't working as expected. This report shows the stages of agentless flow, including events such as script upload completed, script upload failed, script execution completed, and so on, along with any known failure reasons, if any.

Note The agentless posture script cannot verify itself, but the script verifies the data received from Cisco ISE after it is executed.

You can access Agentless Posture Troubleshooting from two locations:

- In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Live Logs**, and click the vertical three dots in the **Posture Status** column adjacent to the client you want to troubleshoot.
- In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostics** > **General Tools** > **Agentless Posture Troubleshooting**.

The Agentless Posture Troubleshooting tool collects Agentless Posture activity for a specified client. **Agentless Posture Flow** initiates posture and displays all the interactions between a currently active client and Cisco ISE. **Only Download Client Logs** creates logs with up to 24 hours of posture flows from the client. The client can delete the logs at any time. After collection is completed, you can export a ZIP file of the logs.

Reports

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Reports** > **Endpoints and Users** > **Agentless Posture** to view all the endpoints that ran Agentless posture.

Posture Administration Settings

You can globally configure the Admin portal for posture services. You can download updates automatically to the Cisco ISE server through the web from Cisco. You can also update Cisco ISE manually offline later. In addition, having an agent like AnyConnect or the Web Agent installed on the clients provides posture assessment and remediation services to clients. The client agent periodically updates the compliance status of clients to Cisco ISE. After login and successful requirement assessment for posture, the client agent displays a dialog with a link that requires end users to comply with terms and conditions of network usage. You can use this link to define network usage information for your enterprise network that end users accept before they can gain access to your network.

Client Posture Requirements

To create a posture requirement:

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture** > **Requirements**.
2. From the **Edit** drop-down list at the end of any requirement row, choose **Insert New Requirement**.
3. Enter the required details and click **Done**.

The following table describes the fields in the **Client Posture Requirements** window.

Table 159: Posture Requirement

Field Name	Usage Guidelines
Name	Enter a name for the requirement.
Operating Systems	Choose an operating system. Click plus [+] to associate more than one operating system to the policy. Click minus [-] to remove the operating system from the policy.
Compliance Module	From the **Compliance Module** drop-down list, choose the required compliance module: • 4.x or Later: Supports antimalware, disk encryption, patch management, and USB conditions. • 3.x or Earlier: Supports antivirus, antispyware, disk encryption, and patch management conditions. • Any Version: Supports file, service, registry, application, and compound conditions. For more information about compliance module, see Compliance Module, on page 1161.
Posture Type	From the **Posture Type** drop-down list, choose the required posture type. • AnyConnect: Deploys the AnyConnect agent to monitor and enforce Cisco ISE policies that require client interaction. • AnyConnect Stealth: Deploys the AnyConnect agent to monitor and enforce Cisco ISE posture policies without any client interaction. • Temporal Agent: A temporary executable file that is run on the client to check the compliance status.

Field Name	Usage Guidelines
Conditions	Choose a Condition from the list. You can also create any user defined condition by clicking the Action Icon and associate it with the requirement. You cannot edit the associated parent operating system while creating user defined conditions. The pr_WSUSRule is a dummy compound condition, which is used in a posture requirement with an associated Windows Server Update Services (WSUS) remediation. The associated WSUS remediation action must be configured to validate Windows updates by using the severity level option. When this requirement fails, the agent on the Windows client enforces the WSUS remediation action based on the severity level that you define in the WSUS remediation. The pr_WSUSRule cannot be viewed in the Compound conditions list page. You can only select the pr_WSUSRule from the Conditions widget.
Remediation Actions	Choose a Remediation from the list. You can also create a remediation action and associate it with the requirement. You have a text box for all the remediation types that can be used to communicate to the agent users. In addition to remediation actions, you can communicate to agent users about the non-compliance of clients with messages. The **Message Text Only** option informs agent users about the noncompliance. It also provides optional instructions to the user to contact the Help desk for more information, or to remediate the client manually. In this scenario, the agent does not trigger any remediation action.

Related Topics

Configure Acceptable Use Policies for Posture Assessment, on page 1156

Create Client Posture Requirements, on page 1204

Timer Settings for Clients

You can set up timers for users to remediate, to transition from one state to another, and to control the login success screen.

We recommend configuring agent profiles with remediation timers and network transition delay timers and the timer used to control the login success screen on client machines so that these settings are policy based. You can configure all these timers for agents in client provisioning resources in the **AnyConnect Posture Profile** window (**Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources** > **Add** > **AnyConnect Posture Profile**).

However, when there are no agent profiles configured to match the client provisioning policies, you can use the settings in the **General Settings** configuration window (**Administration** > **System** > **Settings** > **Posture** > **General Settings**).

Set Remediation Timer for Clients to Remediate Within Specified Time

You can configure the timer for client remediation within a specified time. When clients fail to satisfy configured posture policies during an initial assessment, the agent waits for the clients to remediate within the time configured in the remediation timer. If the client fails to remediate within this specified time, then the client agent sends a report to the posture run-time services after which the clients are moved to the noncompliance state.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **General Settings**.

Step 2 In the **Remediation Timer** field, enter a time value in minutes.

The default value is 4 minutes. The valid range is 1–300 minutes.

Step 3 Click **Save**.

Set Network Transition Delay Timer for Clients to Transition

You can configure the timer for clients to transition from one state to the other state within a specified time using the network transition delay timer, which is required for Change of Authorization (CoA) to complete. It may require a longer delay time when clients need time to get a new VLAN IP address during success and failure of posture. When successfully postured, Cisco ISE allows clients to transition from unknown to compliant mode within the time specified in the network transition delay timer. Upon failure of posture, Cisco ISE allows clients to transition from unknown to noncompliant mode within the time specified in the timer.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **General Settings**.

Step 2 Enter a time value in seconds, in the **Network Transition Delay** field.

The default value is 3 seconds. The valid range is 2 to 30 seconds.

Step 3 Click **Save**.

Set Login Success Window to Close Automatically

After successful posture assessment, the client agent displays a temporary network access screen. The user needs to click the **OK** button in the login window to close it. You can set up a timer to close this login screen automatically after specified time.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **General Settings**.

Step 2 Check the **Automatically Close Login Success Screen After** check box.

Step 3 Enter a time value in seconds, in the field next to **Automatically Close Login Success Screen After** check box.

The valid range is 0 to 300 seconds. If the time is set to zero, then AnyConnect does not display the login success screen.

Step 4 Click **Save**.

Set Posture Status for Nonagent Devices

You can configure the posture status of endpoints that run on non-agent devices. When Android devices and Apple devices such as an iPod, iPhone, or iPad connect to a Cisco ISE enabled network, these devices assume the Default Posture Status settings.

These settings can also be applied to endpoints that run on Windows and MacOS operating systems when a matching client provisioning policy is not found during posture runtime while redirecting the endpoints to the client provisioning portal.

Before you begin

In order to enforce policy on an endpoint, you must configure a corresponding Client Provisioning policy (Agent installation package). Otherwise, the posture status of the endpoint automatically reflects the default setting.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **General Settings**.

Step 2 From the **Default Posture Status** drop-down list, choose the option as **Compliant** or **Noncompliant**.

Step 3 Click **Save**.

Posture Lease

You can configure Cisco ISE to perform posture assessment every time a user logs into your network or perform posture assessment in specified intervals. The valid range is from 1 to 365 days.

This configuration applies only for those who use AnyConnect agent for posture assessment.

When the posture lease is active, Cisco ISE will use the last known posture state and will not reach out to the endpoint to check for compliance. But when the posture lease expires, Cisco ISE does not automatically trigger a re-authentication or a posture reassessment for the endpoint. The endpoint will stay in the same compliance state since the same session is being used. When the endpoint re-authenticates, posture will be run and the posture lease time will be reset.

Example Use Case Scenario:

- The user logs on to the endpoint and gets it posture compliant with the posture lease set to one day.
- Four hours later the user logs off from the endpoint (the posture lease now has 20 hours left).
- One hour later the user logs on again. Now the posture lease has 19 hours left. The last know posture state was compliant. Hence the user is provided access without posture being run on the endpoint.
- Four hours later the user logs off (the posture lease now has 15 hours left).
- 14 hours later, the user logs on. The posture lease has one hour left. The last known posture state was compliant. The user is provided access without posture being run on the endpoint.
- One hour later, the posture lease expires. The user is still connected to the network as the same user session is being used.

- One hour later, user logs off (the session is tied to the user but not to the machine, so the machine can stay on the network).
- One hour later the user logs on. Since the posture lease has expired and a new user session is launched, the machine performs a posture assessment, the results are sent to the Cisco ISE and the posture lease timer is reset to one day in case of this use case.

Periodic Reassessments

Periodic reassessment (PRA) can be done only for clients that are already successfully postured for compliance. PRA cannot occur if clients are not compliant on your network.

A PRA is valid and applicable only if the endpoints are in a compliant state. The policy service node checks the relevant policies, and compiles the requirements depending on the client role that is defined in the configuration to enforce a PRA. If a PRA configuration match is found, the policy service node responds to the client agent with the PRA attributes that are defined in the PRA configuration for the client before issuing a CoA request. The client agent periodically sends the PRA requests based on the interval specified in the configuration. The client remains in the compliant state if the PRA succeeds, or the action configured in the PRA configuration is to continue. If the client fails to meet PRA, then the client is moved from the compliant state to the noncompliant state.

The PostureStatus attribute shows the current posture status as compliant in a PRA request instead of unknown even though it is a posture reassessment request. The PostureStatus is updated in the Monitoring reports as well.

When the posture lease has not expired, an endpoint becomes compliant based on the Access Control List (ACL), and PRA is initiated. If PRA fails, the endpoint is deemed noncompliant and the posture lease is reset.

Note PRA is not supported during PSN failover. After PSN failover, you must either enable rescan on the client or enable posture lease.

Configure Periodic Reassessments

You can configure periodic reassessments only for clients that are already successfully postured for compliance. You can configure each PRA to a user identity group that is defined in the system.

Before you begin

- Ensure that each Periodic reassessment (PRA) configuration has a unique group or a unique combination of user identity groups assigned to the configuration.
- You can assign a role_test_1 and a role_test_2, which are the two unique roles to a PRA configuration. You can combine these two roles with a logical operator and assign the PRA configuration as a unique combination of two roles. For example, role_test_1 OR role_test_2.
- Ensure that two PRA configurations do not have a user identity group in common.
- If a PRA configuration already exists with a user identity group *Any*, you cannot create other PRA configurations unless you perform one of the following:
    - Update the existing PRA configuration with the Any user identity group to reflect a user identity group other than *Any*.

- Delete the existing PRA configuration with a user identity group "*Any*".

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **Reassessments**.

Step 2 Click **Add**.

Step 3 Modify the values in the **New Reassessment Configuration** window to create a new PRA.

Step 4 Click **Submit** to create a PRA configuration.

Posture Troubleshooting Settings

The following table describes the fields on the Posture troubleshooting window, which you use to find and resolve posture problems on the network. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **Posture Troubleshooting**.

Table 160: Posture Troubleshooting Settings

Field Name	Usage Guidelines
Search and Select a Posture event for troubleshooting	
Username	Enter the username to filter on.
MAC Address	Enter the MAC address to filter on, using format: xx-xx-xx-xx-xx-xx
Posture Status	Select the authentication status to filter on:
Failure Reason	Enter the failure reason or click **Select** to choose a failure reason from a list. Click **Clear** to clear the failure reason.
Time Range	Select a time range. The RADIUS authentication records that are created during this time range are used.
Start Date-Time:	(Available only when you choose Custom Time Range) Enter the start date and time, or click the calendar icon to select the start date and time. The date should be in the *mm/dd/yyyy* format and time in the *hh:mm* format.
End Date-Time:	(Available only when you choose Custom Time Range) Enter the end date and time, or click the calendar icon to select the start date and time. The date should be in the *mm/dd/yyyy* format and time in the *hh:mm* format.
Fetch Number of Records	Select the number of records to display: 10, 20, 50, 100, 200, 500
Search Result	
Time	Time of the event
Status	Posture status

Field Name	Usage Guidelines
Username	User name associated with the event
MAC Address	MAC address of the system
Failure Reason	Failure reason for the event

Related Topics

Posture Troubleshooting Tool, on page 1215

Posture General Settings

The following table describes the fields on the Posture General Settings window, which you can use to configure general posture settings such as remediation time and posture status. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **General Settings**.

These settings are the default settings for posture, which can be overridden by a posture profile.

General Posture Settings

- **Remediation Timer**: Enter the time to wait before starting remediation. The default value is 4 minutes. The valid range is 1–300 minutes.
- **Network Transition Delay**: Enter a time value in seconds. The default value is 3 seconds. The valid range is from 2 to 30 seconds.
- **Default Posture Status**: Choose **Compliant** or **Noncompliant**. Non-agent devices assume this status while connecting to the network.
- **Automatically Close Login Success Screen After**: Check the check box to close the login success screen automatically after the specified time. You can configure the timer to close the login screen automatically. The valid range is from 0 to 300 seconds. If the time is set to zero, then the agents on the client do not display the login success screen.
- **Continuous Monitoring Interval**: Specify the time interval after which AnyConnect should start sending monitoring data. For application and hardware conditions, the default value is 5 minutes.
- **Agentless posture client timeout**: Specify how long to wait before a posture check is considered as failed.
- **Remove Agentless Plugin after each run**: Enabling this setting removes the agent from the client after running Agentless posture. We strongly recommend that you leave this disabled, so that the downloaded plugin can be reused, until newer versions are available. Leaving this disabled helps to reduce network traffic.
- **Acceptable Use Policy in Stealth Mode**: Choose **Block** in stealth mode to move a client to noncompliant posture status, if your company's network-usage terms and conditions are not met.

Posture Lease

- **Perform posture assessment every time a user connects to the network**: Select this option to initiate posture assessment every time the user connects to network

- **Perform posture assessment every n days**: Select this option to initiate posture assessment after the specified number of days, even if the client is already postured Compliant.
- **Cache Last Known Posture Compliant Status**: Check this check box for Cisco ISE to cache the result of posture assessment. By default, this field is disabled.
- **Last Known Posture Compliant Status**: This setting only applies if you have checked **Cache Last Known Posture Compliant Status**. Cisco ISE caches the result of posture assessment for the amount of time specified in this field. Valid values are from 1 to 30 days, or from 1 to 720 hours, or from 1 to 43200 minutes.

Related Topics

Posture Administration Settings, on page 1145
Posture Lease, on page 1149
Set Remediation Timer for Clients to Remediate Within Specified Time, on page 1147
Set Network Transition Delay Timer for Clients to Transition, on page 1148
Set Login Success Window to Close Automatically, on page 1148
Set Posture Status for Nonagent Devices, on page 1149

Download Posture Updates to Cisco ISE

Posture updates include a set of predefined checks, rules, and support charts for antivirus and antispyware for both Windows and MacOS operating systems, and operating systems information that are supported by Cisco. You can also update Cisco ISE offline from a file on your local system, which contains the latest archives of updates.

When you deploy Cisco ISE on your network for the first time, you can download posture updates from the web. This process usually takes approximately 20 minutes. After the initial download, you can configure Cisco ISE to verify and download incremental updates to occur automatically.

Cisco ISE creates default posture policies, requirements, and remediations only once during an initial posture updates. If you delete them, Cisco ISE does not create them again during subsequent manual or scheduled updates.

Before you begin

To ensure that you are able to access the appropriate remote location from which you can download posture resources to Cisco ISE, you may be required to verify that you have the correct proxy settings configured for your network as described in Specifying Proxy Settings in Cisco ISE.

You can use the Posture Update window to download updates dynamically from the web.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **Updates**.

Step 2 Choose the **Web** option to download updates dynamically.

Step 3 Click **Set to Default** to set the Cisco default value for the **Update Feed URL** field.

If your network restricts URL-redirection functions (via a proxy server, for example) and you are experiencing difficulty accessing the above URL, try also pointing your Cisco ISE to the alternative URL in the related topics.

Step 4 Modify the values in the **Posture Updates** window.

Step 5 Click **Update Now** to download updates from Cisco.

After being updated, the Posture Updates window displays the current Cisco updates version information as a verification of an update under Update Information section in the Posture Updates window.

Step 6 Click **Yes** to continue.

Cisco ISE Offline Updates

This offline update option allows you to download client provisioning and posture updates, when direct internet access to Cisco.com from a device using Cisco ISE is not available or is not permitted by a security policy.

To download offline client provisioning resources:

Step 1 Go to: https://software.cisco.com/download/home/283801620/type/283802505/release/3.0.0.

Step 2 Provide your login credentials.

Step 3 Navigate to the Cisco Identity Services Engine download window, and select the release.

The following Offline Installation Packages are available for download:

- **win_spw-<*version*>-isebundle.zip**—Offline SPW Installation Package for Windows
- **mac-spw-<*version*>.zip**—Offline SPW Installation Package for Mac OS X
- **compliancemodule-<*version*>-isebundle.zip**—Offline Compliance Module Installation Package
- **macagent-<*version*>-isebundle.zip**—Offline Mac Agent Installation Package
- **webagent-<*version*>-isebundle.zip**—Offline Web Agent Installation Package

Step 4 Click either **Download** or **Add to Cart**.

For more information on adding the downloaded installation packages to Cisco ISE, see the "Add Client Provisioning Resources from a Local Machine" section in the Cisco Identity Services Engine Administrator Guide.

You can update the checks, operating system information, and antivirus and antispyware support charts for Windows and Mac operating systems offline from an archive in your local system, using posture updates.

For offline updates, ensure that the versions of the archive files match the versions in the configuration file. Use offline posture updates after you configure Cisco ISE and want to enable dynamic updates for the posture policy service.

To download offline posture updates:

Step 1 Go to https://www.cisco.com/web/secure/spa/posture-offline.html.

Step 2 Save the **posture-offline.zip** file to your local system. This file is used to update the operating system information, checks, rules, and antivirus and antispyware support charts for Windows and Mac operating systems.

Step 3 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture**.

Step 4 Click the arrow to view the settings for posture.

Step 5 Click **Updates**.
The **Posture Updates** window is displayed.

Step 6 Click the **Offline** option.

Step 7 Click **Browse** to locate the archive file (posture-offline.zip) from the local folder in your system.

> **Note** The **File to Update** field is a mandatory field. You can select only one archive file (.zip) containing the appropriate files. Archive files other than .zip, such as .tar, and .gz are not supported.

Step 8 Click **Update Now**.

Download Posture Updates Automatically

After an initial update, you can configure Cisco ISE to check for the updates and download them automatically.

Before you begin

- You should have initially downloaded the posture updates to configure Cisco ISE to check for the updates and download them automatically.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **Updates**.

Step 2 In the **Posture Updates** window, check the **Automatically check for updates starting from initial delay** check box.

Step 3 Enter the initial delay time in hh:mm:ss format.

Cisco ISE starts checking for updates after the initial delay time is over.

Step 4 Enter the time interval in hours.

Cisco ISE downloads the updates to your deployment at specified intervals from the initial delay time.

Step 5 Click **Save**.

Posture Acceptable Use Policy Configuration Settings

The following table describes the fields in the Posture Acceptable Use Policy Configurations window, which you can use to configure an acceptable use policy for posture. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **Acceptable Use Policy**.

Table 161: Posture AUP Configurations Settings

Field Name	Usage Guidelines
Configuration Name	Enter the name of the AUP configuration that you want to create.

Field Name	Usage Guidelines
Configuration Description	Enter the description of the AUP configuration that you want to create.
Show AUP to Agent users (for Windows only)	When selected, the link to network usage terms and conditions for your network is displayed to users upon successful authentication and posture assessment.
Use URL for AUP message	When selected, you must enter the URL to the AUP message in the AUP URL field.
Use file for AUP message	When selected, you must browse to the location and upload a file in a zipped format. The file must contain the index.html at the top level. The .zip file can include other files and subdirectories in addition to the index.html file. These files can reference each other using HTML tags.
AUP URL	Enter the URL to the AUP, which users must access upon successful authentication and posture assessment.
AUP File	Browse to the file and upload it to the Cisco ISE server. It should be a zipped file and should contain the index.html file at the top level.
Select User Identity Groups	Choose a unique user identity group or a unique combination of user identity groups for your AUP configuration. Note the following while creating an AUP configuration: • Posture AUP is not applicable for a guest flow • No two configurations have any user identity group in common • If you want to create a AUP configuration with a user identity group “Any”, then delete all other AUP configurations first • If you create a AUP configuration with a user identity group “Any”, then you cannot create other AUP configurations with a unique user identity group or user identity groups. To create an AUP configuration with a user identity group other than Any, either delete an existing AUP configuration with a user identity group “Any” first, or update an existing AUP configuration with a user identity group “Any” with a unique user identity group or user identity groups.
Acceptable use policy configurations—Configurations list	Lists existing AUP configurations and end user identity groups associated with AUP configurations.

Related Topics

Configure Acceptable Use Policies for Posture Assessment, on page 1156

Configure Acceptable Use Policies for Posture Assessment

After login and successful posture assessment of clients, the client agent displays a temporary network access screen. This screen contains a link to an acceptable use policy (AUP). When the user clicks the link, they are redirected to a page that displays the network-usage terms and conditions, which they must read and accept.

Each Acceptable Use Policy configuration must have a unique user identity group, or a unique combination of user identity groups. Cisco ISE finds the AUP for the first matched user identity group, and then it communicates to the client agent that displays the AUP.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **Acceptable Use Policy**.

Step 2 Click **Add**.

Step 3 Modify the values in the **New Acceptable Use Policy Configuration** window.

Step 4 Click **Submit**.

Posture Conditions

A posture condition can be any one of the following simple conditions: a file, a registry, an application, a service, or a dictionary condition. One or more conditions from these simple conditions form a compound condition, which can be associated to a posture requirement.

When you deploy Cisco ISE on your network for the first time, you can download posture updates from the web. This process is called the initial posture update.

After an initial posture update, Cisco ISE also creates Cisco defined simple and compound conditions. Cisco defined simple conditions have pc_ as their prefixes and compound conditions have pr_ as their prefixes.

You can also configure Cisco ISE to download the Cisco-defined conditions periodically as a result of dynamic posture updates through the web. You cannot delete or edit Cisco defined posture conditions.

A user defined condition or a Cisco defined condition includes both simple conditions and compound conditions.

Simple Posture Conditions

You can use the **Posture Navigation** pane to manage the following simple conditions:

- File Conditions: A condition that checks the existence of a file, the date of a file, and the versions of a file on the client.
- Registry Conditions: A condition that checks for the existence of a registry key or the value of the registry key on the client.
- Application Conditions: A condition that checks if an application or process is running or not running on the client.

Note If a process is installed and running, user is compliant. However, the Application condition works in reverse logic; If an application is not installed and not running, the end user is complaint. If an application is installed and running, the end user is non-complaint.

- Service Conditions: A condition that checks if a service is running or not running on the client.

- Dictionary Conditions: A condition that checks a dictionary attribute with a value.
- USB Conditions: A condition that checks for the presence of USB mass storage device.

Create Simple Posture Conditions

You can create file, registry, application, service, and dictionary simple conditions that can be used in posture policies or in other compound conditions.

Before you begin

To perform the following task, you must be a Super Admin or Policy Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture**.

Step 2 Choose any one of the following: **File**, **Registry**, **Application**, **Service**, or **Dictionary Simple Condition**.

Step 3 Click **Add**.

Step 4 Enter the appropriate values in the fields.

Step 5 Click **Submit**.

Compound Posture Conditions

Compound conditions are made up of one or more simple conditions, or compound conditions. You can make use of the following compound conditions while defining a Posture policy.

- Compound Conditions: Contains one or more simple conditions, or compound conditions of the type File, Registry, Application, or Service condition
- Antivirus Compound Conditions: Contains one or more AV conditions, or AV compound conditions
- Antispyware Compound Conditions: Contains one or more AS conditions, or AS compound conditions
- Dictionary Compound Conditions: Contains one or more dictionary simple conditions or dictionary compound conditions
- Antimalware Conditions: Contains one or more AM conditions.

Create Compound Posture Conditions

You can create compound conditions that can be used in posture policies for posture assessment and validation.

Before you begin

To perform the following task, you must be a Super Admin or Policy Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Compound Conditions** > **Add**.

Step 2 Enter appropriate values for the fields.

Step 3 Click **Validate Expression** to validate the condition.

Step 4 Click **Submit**.

Dictionary Compound Condition Settings

Table 162: Dictionary Compound Condition Settings

Field Name	Usage Guidelines
Name	Enter the name of the dictionary compound condition that you want to create.
Description	Enter the description of the dictionary compound condition that you want to create.
Select Existing Condition from Library	Define an expression by selecting pre-defined conditions from the policy elements library or add ad-hoc attribute/value pairs to your expression in the subsequent steps.
Condition Name	Choose dictionary simple conditions that you have already created from the policy elements library.
Expression	The Expression is updated based on your selection from the Condition Name drop-down list.
AND or OR operator	Choose an AND, or an OR operator to logically combine dictionary simple conditions, which can be added from the library. Click the **Action** icon to do the following: • Add Attribute/Value • Add Condition from Library • Delete Cisco ISE will process each OR condition in a compound condition sequentially. For example, if a compound condition checks for A OR B, Cisco ISE first checks A and then B. If either condition A or B is passed, the overall result is marked as passed. If condition A fails and condition B succeeds, then the overall result is marked as passed. In this case, condition A is marked as failed and condition B as passed in the posture reports. If condition A succeeds, Cisco ISE skips condition B and marks the overall result as passed. In the posture reports, condition A is marked as passed, condition B as skipped, and the overall result as passed.
Create New Condition (Advance Option)	Select attributes from various system or user-defined dictionaries. You can also add predefined conditions from the policy elements library in the subsequent steps.
Condition Name	Choose a dictionary simple condition that you have already created.
Expression	From the Expression drop-down list, you can create a dictionary simple condition.

Field Name	Usage Guidelines
Operator	Choose an operator to associate a value to an attribute.
Value	Enter a value that you want to associate to the dictionary attribute, or choose a value from the drop-down list.

Related Topics

Compound Posture Conditions, on page 1158

Create Compound Posture Conditions, on page 1158

Predefined Condition for Enabling Automatic Updates in Windows Clients

The pr_AutoUpdateCheck_Rule is a Cisco predefined condition, which is downloaded to the Compound Conditions window. This condition allows you to check whether the automatic updates feature is enabled on Windows clients. If a Windows client fails to meet this requirement, then the Network Access Control (NAC) Agents enforce the Windows client to enable (remediate) the automatic updates feature. After this remediation is done, the Windows client becomes posture compliant. The Windows update remediation that you associate in the posture policy overrides the Windows administrator setting, if the automatic updates feature is not enabled on the Windows client.

Preconfigured Antivirus and Antispyware Conditions

Cisco ISE loads preconfigured antivirus and antispyware compound conditions in the AV and AS Compound Condition windows, which are defined in the antivirus and antispyware support charts for Windows and MacOS operating systems. These compound conditions can check if the specified antivirus and antispyware products exist on all the clients. You can also create new antivirus and antispyware compound conditions in Cisco ISE.

Antivirus and Antispyware Support Chart

Cisco ISE uses an antivirus and antispyware support chart, which provides the latest version and date in the definition files for each vendor product. Users must frequently poll antivirus and antispyware support charts for updates. The antivirus and antispyware vendors frequently update antivirus and antispyware definition files, look for the latest version and date in the definition files for each vendor product.

Each time the antivirus and antispyware support chart is updated to reflect support for new antivirus and antispyware vendors, products, and their releases, the agents receive a new antivirus and antispyware library. It helps the Agents to support newer additions. Once the agents retrieve this support information, they check the latest definition information from the periodically updated se-checks.xml file (which is published along with the se-rules.xml file in the se-templates.tar.gz archive), and determine whether clients are compliant with the posture policies. Depending upon what is supported by the antivirus and antispyware library for a particular antivirus, or antispyware product, the appropriate requirements will be sent to the agents for validating their existence, and the status of particular antivirus and antispyware products on the clients during posture validation.

For more information on the antivirus and anti-malware products supported by the ISE posture agent, see the Cisco AnyConnect ISE Posture Support Charts: Cisco ISE Compatibility Guide.

You can verify the minimum compliance module version while creating an anti-malware posture condition. After the posture feed is updated, choose **Work Centers** > **Posture** > **Policy Elements** > **Anti-Malware Condition** and then choose the **Operating System** and **Vendor** to view the support chart.

Note Some of the Anti-Malware endpoint security solutions (such as FireEye, Cisco AMP, Sophos, and so on) require network access to their respective centralized service for functioning. For such products, AnyConnect ISE posture module (or OESIS library) expects the endpoints to have internet connectivity. It is recommended that internet access is allowed for such endpoints during pre-posture for these online agents (if offline detection is not enabled). Signature Definition condition might not be applicable in such cases.

Compliance Module

The compliance module contains a list of fields, such as vendor name, product version, product name, and attributes provided by OPSWAT that supports Cisco ISE posture conditions.

Vendors frequently update the product version and date in the definition files, therefore, you must look for the latest version and date in the definition files for each vendor product by frequently polling the compliance module for updates. Each time the compliance module is updated to reflect the support for new vendors, products, and their releases, the AnyConnect agent receives a new library. It helps the AnyConnect agent to support newer additions. The AnyConnect agent retrieves this support information and checks the latest definition information from the periodically updated se-checks.xml file (which is published along with the se-rules.xml file in the se-templates.tar.gz archive), and determine whether clients are compliant with the posture policies. Depending upon what is supported by the library for a particular antivirus, antispyware, antimalware, disk encryption, or patch management product, the appropriate requirements will be sent to the AnyConnect agent for validating their existence, and the status of the particular products on the clients during posture validation.

The compliance module is available on Cisco.com.

Table given below lists the OPSWAT API versions that support and do not support the ISE posture policy. There are different policy rules for agents that support versions 3 and 4.

Table 163: OPSWAT API Versions

Posture Condition	Compliance Module Version
OPSWAT	
Antivirus	3.x or earlier
Antispyware	3.x or earlier
Antimalware	4.x or later
Disk Encryption	3.x or earlier and 4.x or later
Patch Management	3.x or earlier and 4.x or later
USB	4.x or later
Non-OPSWAT	
File	Any version
Application	Any version

Posture Condition	Compliance Module Version
Compound	Any version
Registry	Any version
Service	Any version

Note

- Be sure to create separate posture policies for version 3.x or earlier and version 4.x or later, in anticipation of clients that may have installed any one of the above versions.
- OESIS version 4 support is provided for compliance module 4.x and Cisco AnyConnect 4.3 and higher. However, AnyConnect 4.3 supports both OESIS version 3 and version 4 policies.
- Version 4 compliance module is supported by ISE 2.1 and higher.

Check Posture Compliance

Step 1 Log in to Cisco ISE and access the dashboard.

Step 2 In the **Posture Compliance** dashlet, hover your cursor over a stack bar or sparkline.

A tooltip provides detailed information.

Step 3 Expand the data categories for more information.

Step 4 Expand the **Posture Compliance** dashlet.

A detailed real-time report is displayed.

Note You can view the posture compliance report in the **Context Visibility** window. Navigate **Context Visibility** > **Endpoints** > **Compliance**. This window displays different charts based on **Compliance Status**, **Location**, **Endpoints**, and **Applications by Categories**.

You might see the posture status for endpoints that do not have any active sessions. For example, if the last known posture status for an endpoint is **Compliant**, the status remains **Compliant** in the **Context Visibility** window until the next update is received for the endpoint, even if the endpoint session is terminated. The posture status is retained in the **Context Visibility** window until that endpoint is deleted or purged.

Create Patch Management Conditions

You can create a policy to check the status of a selected vendor's patch management product.

For example, you can create a condition to check if Microsoft System Center Configuration Manager (SCCM), Client Version 4.x software product is installed at an endpoint.

Note Supported versions of Cisco ISE and AnyConnect:

- Cisco ISE version 1.4 and later
- AnyConnect version 4.1 and later

Before you begin

To perform the following task, you must be a Super Admin or Policy Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Patch Management Condition**.

Step 2 Click **Add**.

Step 3 Enter the condition name and description in the **Name** and **Description** fields.

Step 4 Choose the appropriate operating system from the **Operating System** drop-down field.

Step 5 Choose the **Compliance Module** from the drop-down list.

Step 6 Choose the **Vendor Name** from the drop-down list.

Step 7 Choose the **Check Type.**

Step 8 Choose the appropriate patch from the **Check patches installed** drop-down list.

Step 9 Click **Submit**.

Related Topics

Patch Management Condition Settings, on page 1182

Add a Patch Management Remediation, on page 1202

Create Disk Encryption Conditions

You can create a policy to check if an end point is compliant with the specified data encryption software.

For example, you can create a condition to check if the C: drive is encrypted in an end point. If the C: drive is not encrypted then the end point receives a non-compliance notification and ISE logs a message.

Before you begin

To perform the following task, you must be a Super Admin or Policy Admin. You can associate a Disk Encryption condition with a posture requirement only when you use the AnyConnect ISE posture agent.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Disk Encryption Condition**.

Step 2 Click **Add**.

Step 3 In the **Disk Encryption Condition** window, enter the appropriate values in the fields.

Step 4 Click **Submit**.

Posture Condition Settings

This section describes simple and compound conditions used for posture.

File Condition Settings

The following table describes the fields in the **File Conditions** window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **File Condition**.

Table 164: File Condition Settings

Field Name	Usage Guidelines for Windows OS	Usage Guidelines for macOS	Usage Guidelines for Linux OS
Name	Enter the name of the file condition.	Enter the name of the file condition.	Enter the name of the file condition.
Description	Enter a description for the file condition.	Enter a description for the file condition.	Enter a description for the file condition.
Operating System	Choose any Windows operating system to which the file condition should be applied.	Choose any macOS to which the file condition should be applied.	Choose any Linux OS (Ubuntu, Red Hat, or SUSE) to which the file condition should be applied. For OS support information, see the Compatibility Matrix for your Cisco ISE release.

Field Name	Usage Guidelines for Windows OS	Usage Guidelines for macOS	Usage Guidelines for Linux OS
File Type	Choose one of the following options: • **FileDate**: Checks whether a file with a particular file-created or file-modified date exists in the system. • **FileExistence**: Checks whether a file exists in the system. • **FileVersion**: Checks whether a particular version of a file exists in the system. • **CRC32**: Checks the data integrity of a file using the checksum function. • **SHA-256**: Checks the data integrity of a file using the hash function.	Choose one of the following options: • **FileDate**: Checks whether a file with a particular file-created or file-modified date exists in the system. • **FileExistence**: Checks whether a file exists in the system. • **CRC32**: Checks the data integrity of a file using the checksum function. • **SHA-256**: Checks the data integrity of a file using the hash function. • **PropertyList**: Checks the property value in a plist file, such as loginwindow.plist.	Choose one of the following options: • **FileDate**: Checks whether a file with a particular file-created or file-modified date exists in the system. • **FileExistence**: Checks whether a file exists in the system. • **CRC32**: Checks the data integrity of a file using the checksum function. • **SHA-256**: Checks the data integrity of a file using the hash function.

Field Name	Usage Guidelines for Windows OS	Usage Guidelines for macOS	Usage Guidelines for Linux OS
Data Type and Operator	NA	(Available only if you select **PropertyList** as the File Type) Choose the data type or value of the key to be searched in the plist files. Each data type contains a set of operators. • **Unspecified**: Checks the existence of the specified key. Enter an Operator (Exists, DoesNotExist). • **Number**: Checks for the specified key of number data type. Enter an Operator (equals, does not equal, greater than, less than, greater than or equal to, less than or equal to) and a Value. • **String**: Checks for the specified key of string data type. Enter an Operator (equals, does not equal, equals (ignore case), starts with, does not start with, contains, does not contain, ends with, does not end with) and a Value. • **Version**: Checks for the value of the specified key as a version string. Enter an Operator (earlier than, later than, same as) and a Value.	NA

Field Name	Usage Guidelines for Windows OS	Usage Guidelines for macOS	Usage Guidelines for Linux OS
Property Name	NA	(Available only if you select **PropertyList** as the File Type) Enter the name of the key, for example, BuildVersionStampAsNumber	NA

Field Name	Usage Guidelines for Windows OS	Usage Guidelines for macOS	Usage Guidelines for Linux OS
File Path	Choose one of the following options: • **ABSOLUTE_PATH**: Checks the file in the fully qualified path of the file. For example, C:\<directory>\file name. For other settings, enter only the file name. • **SYSTEM_32**: Checks the file in the C:\WINDOWS\system32 directory. Enter the file name. • **SYSTEM_DRIVE**: Checks the file in the C:\ drive. Enter the file name. • **SYSTEM_PROGRAMS**: Checks the file in the C:\Program Files. Enter the file name. • **SYSTEM_ROOT**: Checks the file in the root path for Windows system. Enter the file name. • **USER_DESKTOP**: Checks if the specified file is present on the Windows user's desktop. Enter the file name. • **USER_PROFILE**: Checks if the file is present in the Windows user's local profile directory. Enter the file path.	Choose one of the following options: • **Root**: Checks the file in the root (/) directory. Enter the file path. • **Home**: Checks the file in the home (~) directory. Enter the file path.	Choose one of the following options: • **Root**: Checks the file in the root (/) directory. Enter the file path. • **Home**: Checks the file in the home (~) directory. Enter the file path.

Field Name	Usage Guidelines for Windows OS	Usage Guidelines for macOS	Usage Guidelines for Linux OS
File Date Type	(Available only if you select **FileDate** as the File Type) Choose **Creation Date** or **Modification Date**.	(Available only if you select **FileDate** as the File Type) Choose **Creation Date** or **Modification Date**.	(Available only if you select **FileDate** as the File Type) Choose **Creation Date** or **Modification Date**.
File Operator	The **File Operator** options change according to the settings you select in the **File Type**. Choose the settings appropriately: **FileDate** • **EarlierThan** • **LaterThan** • **EqualTo** • **Within**: The last *n* number of days. Valid range is from 1 to 300. **FileExistence** • **Exists** • **DoesNotExist** **FileVersion** • **EarlierThan** • **LaterThan** • **EqualTo**	The **File Operator** options change according to the settings you select in the **File Type**. Choose the settings appropriately: **FileDate** • **EarlierThan** • **LaterThan** • **EqualTo** • **Within**: The last *n* number of days. Valid range is from 1 to 300. **FileExistence** • **Exists** • **DoesNotExist**	The **File Operator** options change according to the settings you select in the **File Type**. Choose the settings appropriately: **FileDate** • **EarlierThan** • **LaterThan** • **EqualTo** • **Within**: The last *n* number of days. Valid range is from 1 to 300. **FileExistence** • **Exists** • **DoesNotExist**
File CRC Data	(Available only if you select **CRC32** as the **File Type**) You can enter a checksum value, for example, 0x3c37fec3 to check file integrity. The checksum value should start with 0x, a hexadecimal integer.	(Available only if you select **CRC32** as the **File Type**) You can enter a checksum value, for example, 0x3c37fec3 to check file integrity. The checksum value should start with 0x, a hexadecimal integer.	(Available only if you select **CRC32** as the **File Type**) You can enter a checksum value, for example, 0x3c37fec3 to check file integrity. The checksum value should start with 0x, a hexadecimal integer.

Field Name	Usage Guidelines for Windows OS	Usage Guidelines for macOS	Usage Guidelines for Linux OS
File SHA-256 Data	(Available only if you select **SHA-256** as the **File Type**) You can enter a 64-byte hexadecimal hash value to check file integrity.	(Available only if you select **SHA-256** as the **File Type**) You can enter a 64-byte hexadecimal hash value to check file integrity.	(Available only if you select **SHA-256** as the **File Type**) You can enter a 64-byte hexadecimal hash value to check file integrity.
Date and Time	(Available only if you select **FileDate** as the **File Type**) Enter the date and time of the client system in mm/dd/yyyy and hh:mm:ss format.	(Available only if you select **FileDate** as the **File Type**) Enter the date and time of the client system in mm/dd/yyyy and hh:mm:ss format.	(Available only if you select **FileDate** as the **File Type**) Enter the date and time of the client system in mm/dd/yyyy and hh:mm:ss format.

Related Topics

Simple Posture Conditions, on page 1157
Compound Posture Conditions, on page 1158
Create a Posture Condition, on page 1211

Firewall Condition Settings

The Firewall condition checks if a specific Firewall product is running on an endpoint. The list of supported Firewall products is based on the OPSWAT support charts. You can enforce policies during initial posture and Periodic Reassessment (PRA).

Cisco ISE provides default Firewall conditions for Windows and macOS. These conditions are disabled by default.

Field Name	Usage Guidelines
Name	Enter the name of the Firewall condition.
Description	Enter a description for the Firewall condition.
Compliance Module	Choose the required compliance module. • 4.x or later • 3.x or later • Any Version
Operating System	Checks If the required Firewall product is installed on an endpoint. You can select the Windows OS or macOS.
Vendor	Choose a vendor name from the drop-down list. The Firewall products of a vendor and their check type are retrieved and displayed in the **Products for Selected Vendor** table. The list in the table changes according to the selected operating system.

Field Name	Usage Guidelines
Check Type	Enabled: To check if a specific Firewall is running on an endpoint. Verify if the vendor's product supports the chosen check type by referring to the **Products for Selected Vendor** list.

Registry Condition Settings

The following table describes the fields in the Registry Conditions window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Registry Condition**.

Table 165: Registry Condition Settings

Field Name	Usage Guidelines
Name	Enter the name of the registry condition.
Description	Enter a description for the registry condition.
Registry Type	Choose one of the predefined settings as the registry type.
Registry Root Key	Choose one of the predefined settings as the registry root key.
Sub Key	Enter the sub key without the backslash (“\”) to check the registry key in the path specified in the Registry Root Key. For example, SOFTWARE\Symantec\Norton AntiVirus\version will check the key in the following path: HKLM\SOFTWARE\Symantec\NortonAntiVirus\version
Value Name	(Available only if you select **RegistryValue** or **RegistryValueDefault** as the Registry Type) Enter the name of the registry key value to be checked for **RegistryValue**. This is the default field for **RegistryValueDefault**.
Value Data Type	(Available only if you select **RegistryValue** or **RegistryValueDefault** as the Registry Type) Choose one of the following settings: • **Unspecified**: Checks whether the registry key value exists or not. This option is available only for **RegistryValue**. • **Number**: Checks the specified number in the registry key value • **String**: Checks the string in the registry key value • **Version**: Checks the version in the registry key value
Value Operator	Choose the settings appropriately.
Value Data	(Available only if you select **RegistryValue** or **RegistryValueDefault** as the Registry Type) Enter the value of the registry key according to the data type you have selected in **Value Data Type**.
Operating System	Select the operating system to which the registry condition should be applied.

Related Topics

- Simple Posture Conditions, on page 1157
- Compound Posture Conditions, on page 1158

Continuous Endpoint Attribute Monitoring

You can use the AnyConnect agent to continuously monitor different endpoint attributes to improve the overall visibility of an endpoint. The AnyConnect agent monitors applications that are installed and running on an endpoint. You can turn on and off the feature and configure how often the data should be monitored. By default, data is collected every 5 minutes and is stored in the database. During initial posture, AnyConnect reports a complete list of running and installed applications. After initial posture, the AnyConnect agent scans the applications every X minutes and sends the differences from the last scan to the server. The server displays the complete list of running and installed applications.

Application Condition Settings

The application condition queries for applications that are installed on an endpoint. This helps you to get an aggregate visibility of the software distributed on your endpoints.

The following table describes the fields in the **Application Conditions** window. To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Posture** > **Policy Elements** > **Application Condition** > **Add**.

Field Name	Usage Guidelines
Name	Enter the name of the application condition.
Description	Enter the description for the application condition.
Operating System	Select the operating system to which the application condition should be applied. The options are available: • **Windows** • **Mac OSX** • **Linux**
Compliance Module	Choose one of the following options: • **4.x or later** • **3.x or earlier** • **Any Version**
Check By	Choose one of the following options: • **Process**: Choose this option to check if a process is running on an endpoint. • **Application**: Choose this option to check if an application is running on an enc **Note** Only the **Process** option is displayed for Linux OS.

Field Name	Usage Guidelines
Process Name	(Available only when you select **Process** as the **Check By** option) Enter the requ name.
Application Operator	(Available only when you select **Process** as the **Check By** option) Choose one of options: • **Running**: Choose this option to check if an application is running on an en • **Not Running**: Choose this option to check whether an application is not ru endpoint.
Application State	(Available only when you select **Application** as the **Check By** option) Choose o following options: • **Installed**: Choose this option to check whether the clients have malicious a installed. If a malicious application is found, the remediation action is trigg • **Running**: Choose this option to check if an application is running on an en
Provision By	(Available only when you select **Application** as the **Check By** option) Choose o following options: • **Everything**: You can select all listed categories such as Browser, Patch Ma so on. • **Name**: You should select at least one category. For example, if you choose category, it displays the corresponding vendors in the **Vendor** drop-down li • **Category**: You can check one or more categories such as Anti-Malware, Bac or Data Storage. **Note** Categories are dynamically updated from the OPSWAT library.

You can view the number of installed and running applications for each endpoint in the **Context Visibility** > **Endpoints** > **Compliance** window.

The **Home** > **Summary** > **Compliance** window displays the percentage of endpoints that are subject to posture assessment and are compliant.

Service Condition Settings

The following table describes the fields in the **Service Conditions** window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Service Condition**.

Table 166: Service Conditions Settings

Field Name	Usage Guidelines
Name	Enter a name for the service condition.
Description	Enter a description of the service condition.

Field Name	Usage Guidelines
Operating Systems	Select the operating system to which the service condition should be applied. You can select different versions of the Windows OS or macOS.
Service Name	Enter the name of the Daemon or User Agent service, for example, com.apple.geod, running as root. The AnyConnect agent uses the command **sudo launchctl list** to validate the service condition.
Service Type	Choose the type of service that AnyConnect should check for to ensure client compliance: • **Daemon**: Checks if a specified service, such as scanning a client device for malware, is present in the specified list of Daemon services in the client. • **User Agent**: Checks if a specified service, such as a service that runs when malware is detected, is present in the specified list of User services in the client. • **Daemon or User Agent**: Checks if the specified services are present either in the Daemon or User Agent services list.
Service Operator	Choose the service status that you want to check in the client: • **Windows OS**: To check if a service is **Running** or **Not Running**. • **Mac OSX**: To check if a service is **Loaded**, **Not Loaded**, **Loaded and Running**, **Loaded with Exit Code**, and **Loaded and running or with Exit code**.

Related Topics

Simple Posture Conditions, on page 1157

Compound Posture Conditions, on page 1158

Posture Compound Condition Settings

The following table describes the fields in the **Compound Conditions** window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Compound Condition**.

Table 167: Posture Compound Condition Settings

Field Name	Usage Guidelines
Name	Enter the name of the compound condition that you want to create.
Description	Enter the description of the compound condition that you want to create.
Operating System	Select one or more Windows operating systems. This allows you to associate Windows operating systems to which the condition is applied.
Parentheses ( )	Click the parentheses to combine two simple conditions from the following simple condition types: file, registry, application, and service conditions.

Field Name	Usage Guidelines
(&): AND operator (use "&" for an AND operator, without the quotes)	You can use the AND operator (ampersand [&]) in a compound condition. For example, enter **Condition1 & Condition2**.
(|): OR operator (use "|" for an OR operator, without the quotes)	You can use the OR operator (horizontal bar [|]) in a compound condition. For example, enter **Condition1 & Condition2**.
(!): NOT operator (use "!" for a NOT operator, without the quotes)	You can use the NOT operator (exclamation point [!]) in a compound conditions. For example, enter **Condition1 & Condition2**.
Simple Conditions	Choose from a list of simple conditions of the following types: file, registry, application, and service conditions. You can also create simple conditions of file, registry, application, and service conditions from the object selector. Click the quick picker (down arrow) on the **Action** button to create simple conditions of file, registry, application, and service conditions.

Related Topics

Posture Conditions, on page 1157

Create Compound Posture Conditions, on page 1158

AntiVirus Condition Settings

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Anti-Virus Condition**.

Field Name	Usage Guidelines
Name	Enter the name of the antivirus condition that you want to create.
Description	Enter the description of the antivirus condition that you want to create.
Operating System	Select an operating system to check the installation of an antivirus program on your client, or check the latest antivirus definition file updates to which the condition is applied.
Vendor	Choose a vendor from the drop-down list. The selection of Vendor retrieves their antivirus products and versions, which are displayed in the Products for Selected Vendor table.
Check Type	Choose whether to check an installation or check the latest definition file update on the client.
Installation	Choose to check only the installation of an antivirus program on the client.

Field Name	Usage Guidelines
Definition	Choose to check only the latest definition file update of an antivirus product on the client.

Products for Selected Vendor

Choose an antivirus product from the table. Based on the vendor that you select in the New Anti-virus Condition page, the table retrieves information on their antivirus products and their version, remediation support that they provide, latest definition file date and its version.

The selection of a product from the table allows you to check for the installation of an antivirus program, or check for the latest antivirus definition file date, and its latest version.

Note Only one condition can be configured for each antivirus product from either **Baseline Condition** or **Advance Condition**.

Baseline Condition

Field Name	Guideline
Minimum Version	(Available only when you update the Operating System and Vendor) Choose minimum version of the antivirus from the drop down list. The check will enforce the network policy on all the endpoints on your network to comply with the mimimum version of antivirus.
Maximum Version	The maximum version for antivirus is revised automatically when you update the posture feed.
Minimum Compliance Module Version	The minimum compliance module version is updated from the AnyConnect.

Advance Condition

Field Name	Guidelines
Check against latest AV definition file version, if available	(Available only when you choose Definition check type) Choose to check the antivirus definition file version on the client against the latest antivirus definition file version, if available as a result of posture updates in Cisco ISE. Otherwise, this option allows you to check the definition file date on the client against the latest definition file date in Cisco ISE.

Field Name	Guidelines
Allow virus definition file to be (Enabled)	(Available only when you choose Definition check type) Choose to check the antivirus definition file version and the latest antivirus definition file date on the client. The latest definition file date cannot be older than that you define in the next field (days older than field) from the latest antivirus definition file date of the product or the current system date. If unchecked, Cisco ISE allows you to check only the version of the antivirus definition file using the Check against latest AV definition file version, if available option.
Days Older than	Define the number of days that the latest antivirus definition file date on the client can be older from the latest antivirus definition file date of the product or the current system date. The default value is zero (0).
Latest File Date	Choose to check the antivirus definition file date on the client, which can be older by the number of days that you define in the days older than field. If you set the number of days to the default value (0), then the antivirus definition file date on the client should not be older than the latest antivirus definition file date of the product.
Current System Date	Choose to check the antivirus definition file date on the client, which can be older by the number of days that you define in the days older than field. If you set the number of days to the default value (0), then the antivirus definition file date on the client should not be older than the current system date.

Related Topics

Compound Posture Conditions, on page 1158

Preconfigured Antivirus and Antispyware Conditions, on page 1160

Antivirus and Antispyware Support Chart, on page 1160

Antispyware Compound Condition Settings

The following table describes the fields in the **AS Compound Conditions** window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **AS Compound Condition**.

Table 168: Antispyware Compound Condition Settings

Field Name	Usage Guidelines
Name	Enter the name of the antispyware compound condition that you want to create.

Field Name	Usage Guidelines
Description	Enter the description of the antispyware compound condition that you want to create.
Operating System	Selecting an operating system allows you to check the installation of an antispyware program on your client, or check the latest antispyware definition file updates to which the condition is applied.
Vendor	Choose a vendor from the drop-down list. The selection of Vendor retrieves their antispyware products and versions, which are displayed in the Products for Selected Vendor table.
Check Type	Choose if you want to choose a type whether to check an installation, or check the latest definition file update on the client.
Installation	Choose if you want to check only the installation of an antispyware program on the client.
Definition	Choose if you want to check only the latest definition file update of an antispyware product on the client.
Allow Virus Definition File to be (Enabled)	Check this check box when you are creating antispyware definition check types, and disabled when creating antispyware installation check types. If checked, the selection allows you to check antispyware definition file version and the latest antispyware definition file date on the client. The latest definition file date cannot be older than that you define in the days older than field from the current system date. If unchecked, the selection allows you to check only the version of the antispyware definition file as the Allow virus definition file to be check box is not checked.
Days Older than	Define the number of days that the latest antispyware definition file date on the client can be older from the current system date. The default value is zero (0).
Current System Date	Choose to check the antispyware definition file date on the client, which can be older by the number of days that you define in the days older than field. If you set the number of days to the default value (0), then the antispyware definition file date on the client should not be older than the current system date.
Products for Selected Vendor	Choose an antispyware product from the table. Based on the vendor that you select in the New Anti-spyware Compound Condition page, the table retrieves information on their antispyware products and their version, remediation support that they provide, latest definition file date and its version. The selection of a product from the table allows you to check for the installation of an antispyware program, or check for the latest antispyware definition file date, and its latest version.

Related Topics

Compound Posture Conditions, on page 1158

Preconfigured Antivirus and Antispyware Conditions, on page 1160

Antivirus and Antispyware Support Chart, on page 1160

Antimalware Condition Settings

The antimalware condition is a combination of the antispyware and antivirus conditions and is supported by OESIS version 4.x or later compliance module.

To view this window, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Antimalware Condition**.

Note It is recommended that you manually update the installed Antimalware products to have the latest definitions at least once. Otherwise, the posture checks using AnyConnect for Antimalware definitions might fail.

Field Name	Usage Guidelines
Name	Enter a name for the antimalware condition.
Description	Enter a description for the antimalware condition.
Operating System	Choose an operating system to check the installation of antimalware programs on your client, or check the latest antimalware definition file updates to which the condition is applied. It supports Windows, macOS, and Linux operating systems.
Vendor	Choose a vendor from the drop-down list. The selected vendor's antimalware products, versions, latest definition dates, latest definition versions, and minimum compliance module versions are displayed in the **Products for Selected Vendor** table.
Check Type	Choose one of the following options: • **Installation**: Choose this option to check only the installation of an antimalware program on the client. • **Definition**: Choose this option to check only the latest definition file update of an antimalware product on the client.
Check Against Latest AV Definition File Version, if Available	(Available only when you choose **Definition** check type) Choose this option to check the antimalware definition file version on the client against the latest antimalware definition file version, if available as a result of posture updates in Cisco ISE. Otherwise, this option allows you to check the definition file date on the client against the latest definition file date in Cisco ISE. This check will only work if there is a value listed in Cisco ISE for the **Latest Definition Date** or **Latest Definition Version** field for the selected product. Otherwise, the **Current System Date** field must be used.
Allow Virus Definition File to be	(Available only when you choose **Definition** check type) Choose this option to check the antimalware definition file version and the latest antimalware definition file date on the client. The latest definition file date cannot be older than that you define in the **Days Older Than** field. If unchecked, Cisco ISE allows you to check only the version of the antimalware definition file using the **Check against latest AV definition file version** option.

Field Name	Usage Guidelines
Days Older Than	Define the number of days that the latest antimalware definition file date on the client can be older than the latest antimalware definition file date of the product or the current system date. The default value is zero.
Latest File Date	Choose this option to define the number of days that the latest antimalware definition file date on the client can be older than the latest antimalware definition file date of the product. If you set the number of days to the default value, then the antimalware definition file date on the client should not be older than the latest antimalware definition file date of the product. This check works only if there is a value listed in Cisco ISE for the **Latest Definition Date** field for the selected product. Otherwise, the **Current System Date** field must be used.
Current System Date	Choose this option to define the number of days that the latest antimalware definition file date on the client can be older than the current system date. If you set the number of days to the default value, then the antimalware definition file date on the client should not be older than the current system date.

For an antimalware condition for Carbon Black Cloud 3.x on Mac OS to be successful, the condition must meet the following requirements:

- The compliance module must be greater than 4.3.2741.
- The condition must be associated with the vendor VMware, Inc.

When you upgrade from one Cisco ISE release to another with a preconfigured Carbon Black Cloud 3.x condition, after a posture feed update, two Carbon Black Cloud 3.x conditions are listed in the **Advanced Conditions** area of the **Anti-Malware Condition** windows.

You must delete the Carbon Black Cloud 3.x condition associated with the vendor Carbon Black, Inc. You must reconfigure any existing antimalware conditions that use the Carbon Black Cloud 3.x from Carbon Black, Inc. to use the condition from the vendor VMware, Inc.

Related Topics

Compound Posture Conditions, on page 1158

Dictionary Simple Condition Settings

The following table describes the fields in the **Dictionary Simple Conditions** window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Dictionary Simple Condition**.

Table 169: Dictionary Simple Condition Settings

Field Name	Usage Guidelines
Name	Enter the name of the dictionary simple condition that you want to create.
Description	Enter the description of the dictionary simple condition that you want to create.

Field Name	Usage Guidelines
Attribute	Choose an attribute from the dictionary.
Operator	Choose an operator to associate a value to the attribute that you have selected.
Value	Enter a value that you want to associate to the dictionary attribute, or choose a predefined value from the drop-down list.

Related Topics

Simple Posture Conditions, on page 1157

Create Simple Posture Conditions, on page 1158

Dictionary Compound Condition Settings

Table 170: Dictionary Compound Condition Settings

Field Name	Usage Guidelines
Name	Enter the name of the dictionary compound condition that you want to create.
Description	Enter the description of the dictionary compound condition that you want to create.
Select Existing Condition from Library	Define an expression by selecting pre-defined conditions from the policy elements library or add ad-hoc attribute/value pairs to your expression in the subsequent steps.
Condition Name	Choose dictionary simple conditions that you have already created from the policy elements library.
Expression	The Expression is updated based on your selection from the Condition Name drop-down list.

Field Name	Usage Guidelines
AND or OR operator	Choose an AND, or an OR operator to logically combine dictionary simple conditions, which can be added from the library. Click the **Action** icon to do the following: - Add Attribute/Value - Add Condition from Library - Delete Cisco ISE will process each OR condition in a compound condition sequentially. For example, if a compound condition checks for A OR B, Cisco ISE first checks A and then B. If either condition A or B is passed, the overall result is marked as passed. If condition A fails and condition B succeeds, then the overall result is marked as passed. In this case, condition A is marked as failed and condition B as passed in the posture reports. If condition A succeeds, Cisco ISE skips condition B and marks the overall result as passed. In the posture reports, condition A is marked as passed, condition B as skipped, and the overall result as passed.
Create New Condition (Advance Option)	Select attributes from various system or user-defined dictionaries. You can also add predefined conditions from the policy elements library in the subsequent steps.
Condition Name	Choose a dictionary simple condition that you have already created.
Expression	From the Expression drop-down list, you can create a dictionary simple condition.
Operator	Choose an operator to associate a value to an attribute.
Value	Enter a value that you want to associate to the dictionary attribute, or choose a value from the drop-down list.

Related Topics

Compound Posture Conditions, on page 1158

Create Compound Posture Conditions, on page 1158

Patch Management Condition Settings

The following table describes the fields in the **Patch Management Conditions** window. To view this window, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Patch Management Condition**.

Table 171: Patch Management Condition

Field Name	Usage Guidelines
Name	Enter the name of the patch management condition.

Field Name	Usage Guidelines
Description	Enter a description for the patch management condition.
Operating System	Choose an operating system to check the installation of a patch management software on the endpoint, or check the latest patch management definition file updates to which the condition is applied. You can select Windows, macOS, or Linux OS. You can also select more than one version of an operating system to create the patch management condition.
Vendor Name	Choose a vendor from the **Vendor Name** drop-down list. Based on your selection, the patch management products and their supported versions, check type, and minimum compliant module support details are displayed in the **Products for Selected Vendor** table. The list in the table changes according to the selected operating system.
Check Type	Choose one of the following options: • **Installation**: To check if the selected product is installed on the endpoint. This check type is supported by all vendors. **Note** For the Cisco Temporal Agent, you can only view the Patch Management conditions containing the **Installation** check type in the **Requirements** window. • **Enabled**: To check if the selected product is enabled on the endpoint. Verify if the vendor's product supports the chosen check type by referring to the **Products for Selected Vendor** list. • **Up to Date**: To check if the selected product does not have missing patches. Verify if the vendor's product supports the chosen check type by referring to the **Products for Selected Vendor** list. Click the **Products for Selected Vendor** drop-down list to view the list of products that the vendor you have specified in the **Vendor Name** field supports. For example, if you have selected Vendor A that has two products, namely Product 1 and Product 2. Product 1 may support the **Enabled** option, whereas Product 2 might not. Or, if Product 1 does not support any of the check types, it is grayed out. **Note** (Applicable for Cisco ISE 2.3 and above, and AnyConnect 4.5 and above) If you select the **Up to Date** Check Type in the Patch Management condition with SCCM, then Cisco ISE: **1.** Uses the Microsoft API to check the current security patch for the specified severity level. **2.** Triggers the Patch Management remediation for that missing security patch.

Field Name	Usage Guidelines
Check Patches Installed	(Available only when you select the **Up To Date** check type) You can configure severity levels for missing patches, which are then deployed based on the severity. Choose one of the following options: • **Critical Only**: To check if critical software patches are installed on the endpoints in your deployment. • **Important and Critical**: To check if important and critical software patches are installed on the endpoints in your deployment. • **Moderate, Important, and Critical**: To check if moderate, important, and critical software patches are installed on the endpoints in your deployment. • **Low To Critical**: To check if low, moderate, important, and critical software patches are installed on the endpoints in your deployment. • **All**: To install the missing patches for all severity levels.

Related Topics

Create Patch Management Conditions, on page 1162

Disk Encryption Condition Settings

The following table describes the fields in the **Disk Encryption Condition** window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Disk Encryption Condition**.

Table 172: Disk Encryption Condition Settings

Field Name	Usage Guidelines
Name	Enter the name of the disk encryption condition that you want to create.
Description	Enter a description for the disk encryption condition.
Operating System	Select an operating system of the end point, whose disk is to be checked for encryption. You can select the Windows OS or macOS. You can also select more than one version of an operating system to create the disk encryption condition.
Vendor Name	Choose a vendor name from the drop-down list. The data encryption products of a vendor, and their supported version, the encryption state check, and the minimum compliant module support are retrieved and displayed in the **Products for Selected Vendor** table. The list in the table changes according to the selected operating system.

Field Name	Usage Guidelines

Location	Enabled only when an option is checked in the **Products for Selected Vendor** section. Select any one of the following options:
	• **Specific Location**: To check if the specified disk drive is encrypted in the end point, (for example, C: for Windows OS) or a specified volume label is encrypted, (for example, Mackintosh HD for macOS).
	• **System Location**: To check if the default Windows OS system drive or macOS hard drive is encrypted in the end point.
	• **All Internal Drives**: To check the internal drives. Includes all hard disks that are mounted and encrypted, and all internal partitions. Excludes read only drives, system recovery disk/partition, boot partition, network partitions, and the different physical disk drives that are external to the endpoint (including but not limited to disk drives connected via USB and Thunderbolt). Encryption software products that are validated include:
	  ◦ Bit-locker-6.*x*/10.*x*
	  ◦ Checkpoint 80.*x* on Windows 7

Encryption State	The Encryption State checkbox is disabled when the selected product does not support encryption state check. The repeater is displayed only when the checkbox is checked. You can select the Fully Encrypted option to check if the client's disk drive is wholly encrypted. If you create a condition, for example for TrendMicro, and select two vendors—one with the Encryption State "Yes" and another with the Encryption State "No", then the Encryption State will be disabled because one of the Vendor Encryption States is "No". **Note** You can click the repeater to add more Locations and the relationship between each location is the logical AND operator.

Related Topics

Create Disk Encryption Conditions, on page 1163

USB Condition Settings

The following table describes the fields in the **USB Condition** window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Posture** > **Policy Elements** > **USB**. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **USB Condition**

The USB check is a predefined condition and supports only Windows OS.

Table 173: USB Condition Settings

Field Name	Usage Guidelines
Name	USB_Check
Description	Cisco predefined check

Field Name	Usage Guidelines
Operating System	Windows
Compliance Module	A display-only field for ISE posture compliance module support for version 4.x (and later).

Related Topics

Simple Posture Conditions, on page 1157

Hardware Attributes Condition Settings

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Hardware Attributes Condition** to access the **Hardware Attributes Condition** window. The following table describes the fields in the **Hardware Attributes Condition** window.

Field Name	Usage Guidelines
Name	Hardware_Attributes_Check: The default name assigned to the condition.
Description	Cisco predefined check that collects hardware attributes from clients.
Operating System	Windows All or Mac OS
Compliance Module	4.x or later

Posture External DataSource Condition

You can configure conditions to match an endpoints UDID with an external datasource. Currently, only Active Directory is supported. The scripts required on the posture agent to send UDID to Active Directory are not included with ISE.

Configure Posture Policies

A posture policy is a collection of posture requirements that are associated with one or more identity groups and operating systems. The Dictionary Attributes are optional conditions that can be used along with the identity groups and the operating systems to define different policies for the devices.

Cisco ISE provides an option to configure the grace time for the devices that are noncompliant. If a device is found to be noncompliant, Cisco ISE looks for the previously known good state in the posture assessment result cache and provides grace time for the device accordingly. The device is granted access to the network during the grace period. You can configure the grace time period in minutes, hours, or days (up to a maximum of 30 days).

See the section "Posture Policy" in ISE Posture Prescriptive Deployment Guide for more information.

Note Profiler policy evaluation will not work if both 'Endpoint policies' and 'Logical Profiles' are configured under Other Conditions in **Policy** > **Posture**.

Note

- When the grace period is extended or reduced, if the device goes through the posture flow again (for example, if the **Delayed Notification** option is enabled, **Re-Scan** option is selected, device disconnects or reconnects to a network), the new grace period and delayed notification will be applied.
- Grace period is not applicable for the temporal agent.
- Grace period is not supported for Linux agent.
- When a device matches multiple posture policies, with each policy having a different grace period, the device gets the maximum grace period configured among the different policies.
- The Acceptable Use Policy (AUP) is not displayed when the device is in the grace period.

Before you begin

- You must understand the Acceptable Use Policy (AUP).
- You must understand periodic reassessments (PRA).
- You must use AnyConnect agent 4.7 or higher to see compliance-related notifications. For more information about configuring the AnyConnect agent, see Create AnyConnect Configuration, on page 1238.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Posture** or **Work Centers** > **Posture** > **Posture Policy**.

Step 2 Use the drop-down arrow to add a new policy.

Step 3 To edit the profile, either double-click a policy or click Edit at the end of the row.

Step 4 From the **Rule Status** drop-down list, choose **Enabled** or **Disabled**.

Step 5 Choose the drop-down under **Policy Options**, and specify the **Grace Period Settings** in minutes, hours, or days.

The valid values are:

- 1 to 90 days
- 1 to 2,160 hours
- 1 to 129,600 minutes

By default, this setting is disabled.

Note Even if the posture assessment result is noncompliant, if the device is found to be previously compliant and the cache is not yet expired, the device is granted access for the amount of time specified in the **Grace Period Settings**.

Step 6 (Optional) Drag the slider named **Delayed Notification** to delay the grace period prompt from being displayed to the user until a specific percentage of grace period has elapsed. For example, if the notification delay period is set to 50% and the configured grace period is 10 minutes, Cisco ISE checks the posture status after 5 minutes and displays the grace period notification if the endpoint is found to be noncompliant. Grace period notification is not displayed if the endpoint status is compliant. If the notification delay period is set to 0%, the user is prompted immediately at the beginning of the grace period to remediate the problem. However, the endpoint is granted access until the grace period expires. The default value for this field is 0%. The valid range is from 0 to 95%.

Step 7 In the **Rule Name** field, enter the name of the policy.

Note It is a best practice to configure a posture policy with each requirement as a separate rule in order to avoid unexpected results.

Step 8 From the **Identity Groups** column, select the desired identity group.

You can create posture policies based on user or end-point identity groups.

Step 9 From the **Operating Systems** column, select the operating system.

Step 10 From the **Compliance Module** column, select the required compliance module:

- **4.x or Later**: Supports antimalware, disk encryption, patch management, and USB conditions.
- **3.x or Earlier**: Supports antivirus, antispyware, disk encryption, and patch management conditions
- **Any Version**—: upports file, service, registry, application, and compound conditions.

Step 11 From the **Posture Type** column, select the Posture Type.

- **AnyConnect**—Deploys the AnyConnect agent to monitor and enforce Cisco ISE policies that require client interaction.
- **AnyConnect Stealth**—Deploys the AnyConnect agent to monitor and enforce Cisco ISE posture policies without any client interaction.
- **Temporal Agent**—A temporary executable file that is run on the client to check the compliance status.

Step 12 In **Other Conditions**, you can add one or more dictionary attributes and save them as simple or compound conditions to a dictionary.

Note The dictionary simple conditions and compound conditions that you create in the **Posture Policy** window are not displayed while configuring an authorization policy.

Step 13 Specify the requirements in the **Requirements** field.

Step 14 Click **Save**.

Configure AnyConnect Workflow

To configure the AnyConnect agent, perform the following steps in Cisco ISE:

Before you begin

In the following Cisco ISE releases, the bug CSCvs39880 results in garbage collection processes that impacted memory space and file replication from a primary PSN to secondary PSNs. Because of this bug, in the following Cisco ISE releases, uploading an agent package in a large Cisco ISE deployment can take about 7 hours and about 40 minutes in a small deployment.

The following are the affected Cisco ISE releases:

3.1 Patch 4 and earlier

3.0 Patch 6 and earlier

2.7 Patch 7 and earlier

In the later Cisco ISE releases, this bug has been fixed resulting in an agent package upload time of about 5 minutes.

Step 1 Create an AnyConnect agent profile.

Step 2 Create an AnyConnect configuration for AnyConnect packages.

Step 3 Create a client provisioning policy.

Step 4 (Optional) Create custom posture condition.

Step 5 (Optional) Create custom remediation action.

Step 6 (Optional) Create custom posture requirements.

Step 7 Create a posture policy.

Step 8 Configure the client provisioning policy.

Step 9 Create an authorization profile.

Step 10 Configure the authorization policies.

Step 11 Download and launch AnyConnect.

a) Connect to the SSID.
b) Launch a Browser and you will be redirected to the Client Provisioning Portal.
c) Click **Start**. This checks if the AnyConnect agent is installed and running.
d) Click **This Is My First Time Here**.
e) Choose **Click Here to Download and Launch AnyConnect**.
f) Save the Cisco Anyconnect .exe or .dmg file for Windows or macOS respectively. For Windows, run the .exe file and for macOS, double-click the .dmg file and run the app.

Note Cisco ISE does not support ARM64 version of AnyConnect for AnyConnect posture flow. Ensure that you do not use the ARM64 version of AnyConnect in the client provisioning policy, otherwise it might cause failure on the client side. Restart the client if AnyConnect is not working properly because of this issue.

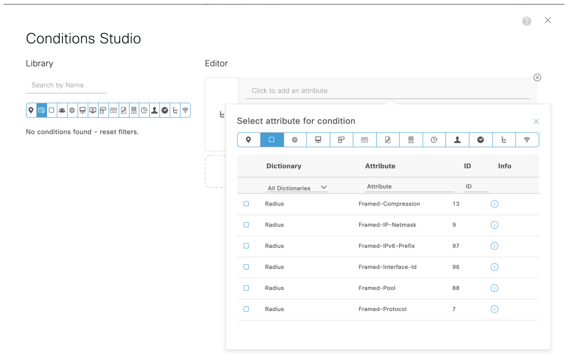
Prerequisite for Certificate-Based Conditions

Client Provisioning and Posture Policy rules may include conditions based on certificate attributes. A prerequisite for certificate-based conditions in either the Client Provisioning or Posture Policy is to ensure that there is s a matching Authorization Policy rule based on the same certificate attribute.

For example, you should use the same attribute as shown in the figures, the Issuer – Common Name attribute is used in both Client Provisioning or posture and authorization policies.

Figure 60: Cisco Provisioning Policy

Figure 61: Conditions Studio



Conditions Studio

Library

Search by Name

No conditions found - reset filters.

Editor

Click to add an attribute

Select attribute for condition

	Dictionary	Attribute	ID	Info
	All Dictionaries	Attribute	ID	
☐	Radius	Framed-Compression	13	ⓘ
☐	Radius	Framed-IP-Netmask	9	ⓘ
☐	Radius	Framed-IPv6-Prefix	97	ⓘ
☐	Radius	Framed-Interface-Id	96	ⓘ
☐	Radius	Framed-Pool	88	ⓘ
☐	Radius	Framed-Protocol	7	ⓘ

Note ISE server certificate must be trusted in the System Certificate store for AnyConnect 4.6 MR2 and above. Any posture check or remediation that requires elevated privileges will not work if the server is untrusted.

- Windows OS: The server certificate must be added to the System Certificate store.
- MAC OS: The server certificate must be added to the System Keychain. It is recommended that you use the command-line utility to trust the certificate. Adding the certificate to the System Keychain using the Keychain Access app might not work if it is already present in the Login Keychain.

Default Posture Policies

The Cisco ISE software comes with a number of pre-configured posture policies that make it easier for you to create the posture policies and profiles. These policies are disabled by default. You can enable these policies based on your requirements. Following are some of the default posture policies.

Rule Name	Description	Requirements
Default_Antimalware_Policy_Mac	Checks if endpoints have any of the supported vendor's antimalware software (that is recognized by AnyConnect) installed and running in their devices.	Any_AM_Installation
Default_Antimalware_Policy_Win	Checks if endpoints have any of the supported vendor's antimalware software (that is recognized by AnyConnect) installed and running in their devices.	Any_AM_Installation_Win

Rule Name	Description	Requirements
Default_AppVis_Policy_Mac	Gathers information and reports all the applications that are installed on a given endpoint.	Default_AppVis_Requirement_Mac
Default_AppVis_Policy_Win	Gathers information and reports all the applications that are installed on a given endpoint.	Default_AppVis_Requirement_Win
Default_Firewall_Policy_Mac	Checks if endpoints have any of the supported vendor's Firewall program (that is recognized by AnyConnect) installed.	Default_Firewall_Requirement_Mac
Default_Firewall_Policy_Win	Checks if endpoints have any of the supported vendor's Firewall program (that is recognized by AnyConnect) installed.	Default_Firewall_Requirement_Win
Default_USB_Block_Win	Ensures that the endpoint device does not have any USB storage devices connected.	USB_Block

Client Posture Assessment

To ensure that the imposed network security measures remain relevant and effective, Cisco ISE enables you to validate and maintain security capabilities on any client machine that accesses the protected network. By employing posture policies that are designed to ensure that up-to-date security settings or applications are available on client machines, the Cisco ISE administrator can ensure that any client machine that accesses the network meets, and continues to meet, the defined security standards for enterprise network access. Posture compliance reports provide Cisco ISE with a snapshot of the compliance level of the client machine at the time of user login, as well as any time a periodic reassessment occurs.

Posture assessment and compliance occurs using one of the following agent types available in Cisco ISE:

- AnyConnect ISE Agent: A persistent agent that can be installed on Windows or Mac OS X client to perform posture compliance functions.
- Cisco Temporal Agent: A temporary executable file that is run on the client to check the compliance status. The agent is removed from the client machine after the login session is terminated. By default, the agent resides in the Cisco ISE ISO image, and is uploaded to Cisco ISE during installation.

Posture Assessment Options

The following table provides a list of posture assessment (posture conditions) options that are supported by the Cisco ISE Posture Agents for Windows and MacOS, and the Web Agent for Windows.

Table 174: Posture Assessment Options

ISE Posture Agent for Windows	Cisco Temporal Agent for Windows	ISE Posture Agent for MacOS	Cisco Temporal Agent for MacOS
Operating System/Service Packs/Hotfixes	—	—	—
Service Check	Service Check (Temporal agent 4.5)	Service Check	Daemon checks are not supported
Registry Check	Registry Check (Temporal agent 4.5)	—	—
File Check	File Check (Temporal agent 4.5)	File Check	File Check (Temporal agent 4.5)
Application Check	Application Check (Temporal agent 4.5)	Application Check	Application Check (Temporal agent 4.5)
Antivirus Installation	Antimalware Installation	Antivirus Installation	Antimalware Installation
Antivirus Version/ Antivirus Definition Date	OPSWAT version 4 is used, hence no Antivirus/Antispyware support; only Antimalware is supported	Antivirus Version/ Antivirus Definition Date	OPSWAT version 4 is used, hence no Antivirus/Antispyware support; only Antimalware is supported
Antispyware Installation	OPSWAT version 4 is used, hence no Antivirus/Antispyware support; only Antimalware is supported	Antispyware Installation	OPSWAT version 4 is used, hence no Antivirus/Antispyware support; only Antimalware is supported
Antispyware Version/ Antispyware Definition Date	OPSWAT version 4 is used, hence no Antivirus/Antispyware support; only Antimalware is supported	Antispyware Version/ Antispyware Definition Date	OPSWAT version 4 is used, hence no Antivirus/Antispyware support; only Antimalware is supported
Patch Management Check	Only Patch Management installation check	Patch Management Check	—
Windows Update Running	—	—	—
Windows Update Configuration	—	—	—
WSUS Compliance Settings	—	—	—

Posture Remediation Options

The following table provides a list of posture remediation options that are supported by the Cisco ISE Posture Agents for Windows and MacOS, and the Web Agent for Windows.

Table 175: Posture Remediation Options

ISE Posture Agent for Windows	ISE Posture Agent for MacOS
Message Text (Local Check)	Message Text (Local Check)
URL Link (Link Distribution)	URL Link (Link Distribution)
File Distribution	—
Launch Program	—
Antivirus Definition Update	Antivirus Live Update
Antispyware Definition Update	Antispyware Live Update
Patch Management Remediation	—
Windows Update	—
WSUS	—

ISE Community Resource

Cisco ISE and SCCM Integration Workflow

Custom Conditions for Posture

A posture condition can be any one of the following simple conditions: a file, a registry, an application, a service, or a dictionary condition. One or more conditions from these simple conditions form a compound condition, which can be associated with a posture requirement.

After an initial posture update, Cisco ISE also creates Cisco-defined simple and compound conditions. Cisco-defined simple conditions use the pc_ as and compound conditions use pr_ as.

A user-defined condition or a Cisco-defined condition includes both simple and compound conditions.

Posture service makes use of internal checks based on antivirus and antispyware (AV/AS) compound conditions. Hence, posture reports do not reflect the exact AV/AS compound-condition names that you have created. The reports display only the internal check names of AV/AS compound conditions.

For example, if you have created an AV compound condition named "MyCondition_AV_Check" to check any Vendor and any Product, the posture reports will display the internal check, that is “av_def_ANY”, as the condition name, instead of "MyCondition_AV_Check".

Posture Endpoint Custom Attributes

You can use the posture endpoint custom attributes to create client provisioning and posture policies. You can create a maximum of 100 endpoint custom attributes. The following types of endpoint custom attributes are supported: Int, String, Long, Boolean, Float, IP, and Date.

Endpoint custom attributes can be used to allow or block devices based on certain attributes or to assign certain privileges based on the posture or client provisioning policies.

Create Posture Policy Using Endpoint Custom Attributes

To create a posture policy using endpoint custom attributes:

Step 1 Create the endpoint custom attributes.

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **Settings** > **Endpoint Custom Attributes**.

b) Enter the **Attribute Name** (for example, deviceType) and Data Type (for example, String) in the **Endpoint Custom Attributes** area.

c) Click **Save**.

Step 2 Assign values to the custom attributes.

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Context Visibility** > **Endpoints**.

b) Assign the custom attribute values.

- Check the required MAC address check box, and then click **Edit**.
- Or, click the required MAC address, and then click **Edit** in the **Endpoints** page.

c) Ensure that the custom attribute that you created is displayed in the **Custom Attributes** area in the **Edit Endpoint** dialog box.

d) Click **Edit** and enter the required attribute value (for example, deviceType = Apple-iPhone).

e) Click **Save**.

Step 3 Create a posture policy using the custom attributes and values.

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Posture** > **Posture Policy**.

b) Create the required policy. Choose the custom attributes by clicking **Other Conditions** and select the required dictionary (for example, choose Endpoints > deviceType, the custom attribute that you created in Step 1). For more information, see the Configure Cisco Temporal Agent Workflow, on page 1213.

c) Click **Save**.

To create a client provisioning policy using endpoint custom attributes:

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Posture** > **Client Provisioning** > **Client Provisioning Policy**.
2. Create the required policy.
    - Create the required rule (for example, Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117).
    - Choose the custom attributes by clicking **Other Conditions** and selecting the required dictionary.

Custom Posture Remediation Actions

A custom posture remediation action is a file, a link, an antivirus or antispyware definition updates, launching programs, Windows updates, or Windows Server Update Services (WSUS) remediation types.

Add an Antispyware Remediation

You can create an antispyware remediation, which updates clients with up-to-date file definitions for compliance after remediation.

The AS Remediations window displays all the antivirus remediations along with their name and description and their modes of remediation.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture**.

Step 2 Click **Remediation Actions**.

Step 3 Click **AS Remediation**.

Step 4 Click **Add**.

Step 5 Modify the values in the **New AS Remediations** window.

Step 6 Click **Submit**.

Add an Antivirus Remediation

You can create an antivirus remediation, which updates clients with up-to-date file definitions for compliance after remediation.

The AV Remediations window displays all the antivirus remediations along with their name and description and their modes of remediation.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture**.

Step 2 Click **Remediation Actions**.

Step 3 Click **AV Remediation**.

Step 4 Click **Add**.

Step 5 Modify the values in the **New AV Remediation** window.

Step 6 Click **Submit**.

Add a File Remediation

A file remediation allows clients to download the required file version for compliance. The client agent remediates an endpoint with a file that is required by the client for compliance.

You can filter, view, add, or delete file remediations in the File Remediations window, but you cannot edit file remediations. The File Remediations window displays all the file remediations along with their name and description and the files that are required for remediation.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture**.

Step 2 Click **Remediation Actions**.

Step 3 Click **File Remediation**.

Step 4 Click **Add**.

Step 5 Enter the name and description of the file remediation in the **Name** and **Description** fields.

Step 6 Modify the values in the **New File Remediation** window.

Step 7 Click **Submit**.

Add a Script Remediation

You can create and upload posture remediation scripts into Cisco ISE to solve non-compliance issues in endpoints.

Before you begin

- Establish trust to fetch posture policies. For more information, see Establish Trust to Execute Script Condition, on page 1199
- Download the script. For more information, see Script Download, on page 1200

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture**.

Step 2 Click **Remediation Actions**.

Step 3 Click **Script Remediations**.

Step 4 Click **Add**.

Step 5 Enter the **Name** and **Description** of the script.

Step 6 Choose the **Operating System** and **Remediation Type** from the corresponding drop-down lists.

If you choose the **Windows** operating system, the **Script Type** and **Windows PowerShell Execution policy** fields are displayed. Choose the required script type and execution policy by clicking the corresponding radio buttons.

Step 7 From the **Remediation Type** drop-down list, choose **Automatic** or **Manual**.

Note

- Only automatic remediation is supported for Linux agent. Manual remediation is not supported.
- Only shell scripts are supported for Linux agent.

Step 8 Enter the **Interval** and **Retry Count**. The valid range is 0 to 999.

Step 9 Click **Choose File**, next to **File To Upload** and select the script that you want to upload from your local system.

Step 10 To run the script as an administrator, click the **Administrator/ Root** radio button. To run the script as a logged-in user, click the **Logged-in User** radio button.

Step 11 Click **Submit**.

Step 12 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Endpoints and Users** > **Posture Script Remediation** to check the status of the remediation script execution.

One of the following statuses is displayed: :

- Remediation script execution was successful.
- Remediation was attempted, and the script exited with failure.
- Remediation was not attempted (default).
- Remediation attempt failed. The script failed an integrity check as the policy included might have been tampered with.
- Remediation attempt failed. Client failed to download the script.
- Remediation attempt failed. The script failed an integrity test as the script might be corrupt or has been tampered with.
- Remediation attempt failed. The script was executed but did not exit in time (timeout).
- Remediation attempt failed. A generic internal system failure occurred.
- Remediation attempt failed. The script type is not supported.
- Remediation attempt failed. Failure with launching the script.
- Certificate verification failure. Client could not verify the server certificate presented by Cisco ISE.

Establish Trust to Execute Script Condition

You must establish trust to be able to execute the scripts on endpoints and make sure that the Cisco ISE server is not compromised. A Cisco ISE environment can have one or more PSNs configured. Every PSN has a valid certificate chain. The certificate chain starts with any certificate, followed by an intermediate certificate or a root CA certificate. You can use any certificate in the certificate chain for fingerprint verification.

You can configure the SHA-256 fingerprint of any certificate in the certificate chain in the AnyConnectLocalPolicy’s profile editor. For example, the following command generates the SHA-256 fingerprint of a certificate with the name input.cer:

```
openssl x509 -inform DER -in <input.cer> -out <output.crt>
openssl x509 -in <output.crt> -fingerprint -noout -sha256
```

The following is an example of the output:

```
openssl x509 -in 535-pos.crt -fingerprint -noout -sha256
SHA256
Fingerprint=B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5
```

The following example shows the new tag in AnyConnectLocalPolicy.xml:

```
<TrustedISECertFingerprints>
<fingerprint>
<algorithm>SHA-256</algorithm>
<hash>B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5</hash>
</fingerprint>
</TrustedISECertFingerprints>
```

Note An SHA-256 fingerprint can be added with or without a colon. You can add the fingerprint in either of the following formats: `B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5` or `B9427F8509183040060BDB9C4836F0609075ABD3E983AB1ABF018F6EF0119AB5`. Fingerprints are not case-sensitive.

The agent matches the Cisco ISE certificate fingerprint with the trusted certificate fingerprint (present in AnyConnectLocalPolicy.xml) while fetching the script. If an endpoint does not have a valid certificate fingerprint, the script is not executed on the endpoint.

Note If fingerprints are configured in AnyConnectLocalPolicy.xml, they are used to validate Cisco ISE trust for all flows. If the certificate is not trusted or if there is a fingerprint mismatch, no error messages are displayed. However, the following error message is included in the **Posture Script Condition** report (**Operations > Reports > Endpoints and Users**):

```
Condition Script certificate verification failed. Client could not verify the server
certificate presented by Cisco ISE.
```

Script Download

When a posture check fails and when the relevant remediation action is triggered, AnyConnect downloads the script from the HTTPS URL configured in the posture policy. The following conditions must be met for the script to get downloaded:

- Trusted fingerprints should exist in AnyConnectLocalPolicy.xml.
- The fingerprint presented by the HTTPS URL should match the trusted certificate fingerprint present in AnyConnectLocalPolicy.xml.

Add a Launch Program Remediation

You can create a launch program remediation, where the client agent remediates clients by launching one or more applications for compliance.

The Launch Program Remediations page displays all the launch program remediations along with their name and description and their modes of remediation.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture**.

Step 2 Click **Remediation Actions**.

Step 3 Click **Launch Program Remediation**.

Step 4 Click **Add**.

Step 5 Modify the values in the **New Launch Program Remediation** page.

Step 6 Click **Submit**.

Troubleshoot Launch Program Remediation

Problem

When an application is launched as a remediation using Launch Program Remediation, the application is successfully launched (observed in the Windows Task Manager), however, the application UI is not visible.

Solution

The Launch program UI application runs with system privileges, and is visible in the Interactive Service Detection (ISD) window. To view the Launch program UI application, ISD should be enabled for the following OS:

- Windows Vista: ISD is in stop state by default. Enable ISD by starting ISD service in services.msc.
- Windows 7: ISD service is enabled by default.
- Windows 8/8.1: Enable ISD by changing "NoInteractiveServices" from 1 to 0 in the registry: \HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Control \ Windows.

Add a Link Remediation

A link remediation allows clients to click a URL to access a remediation window or resource. The client agent opens a browser with the link and allow the clients to remediate themselves for compliance.

The Link Remediation window displays all the link remediations along with their name and description and their modes of remediation.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture**.

Step 2 Click **Remediation Actions.**

Step 3 Click **Link Remediation**.

Step 4 Click **Add**.

Step 5 Modify the values in the **New Link Remediation** window.

Step 6 Click **Submit**.

Add a Patch Management Remediation

You can create a patch management remediation, which updates clients with up-to-date file definitions for compliance after remediation.

The Patch Management Remediation window displays the remediation type, patch management vendor names, and various remediation options.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture**.

Step 2 Click **Remediation Actions**.

Step 3 Click **Patch Mangement Remediation**.

Step 4 Click **Add**.

Step 5 Modify the values in the **Patch Management Remediation** window.

Step 6 Click **Submit** to add the remediation action to the **Patch Management Remediations** window.

Add a Windows Server Update Services Remediation

You can configure Windows clients to receive the latest WSUS updates from a locally administered or a Microsoft-managed WSUS server for compliance. A Windows Server Update Services (WSUS) remediation installs latest Windows service packs, hotfixes, and patches from a locally managed WSUS server or a Microsoft-managed WSUS server.

You can create a WSUS remediation where the client agent integrates with the local WSUS Agent to check whether the endpoint is up-to-date for WSUS updates.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture**.

Step 2 Click **Remediation Actions**.

Step 3 Click **Windows Server Update Services Remediation**.

Step 4 Click **Add**.

Step 5 Modify the values in the **New Windows Server Update Services Remediation** window.

Step 6 Click **Submit**.

Add a Windows Update Remediation

The Windows Update Remediations page displays all the Windows update remediations along with their name and description and their modes of remediation.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > > **Posture.**.

Step 2 Click **Remediation Actions.**

Step 3 Click **Windows Update Remediation**.

Step 4 Click **Add**.

Step 5 Modify the values in the **New Windows Update Remediation** window.

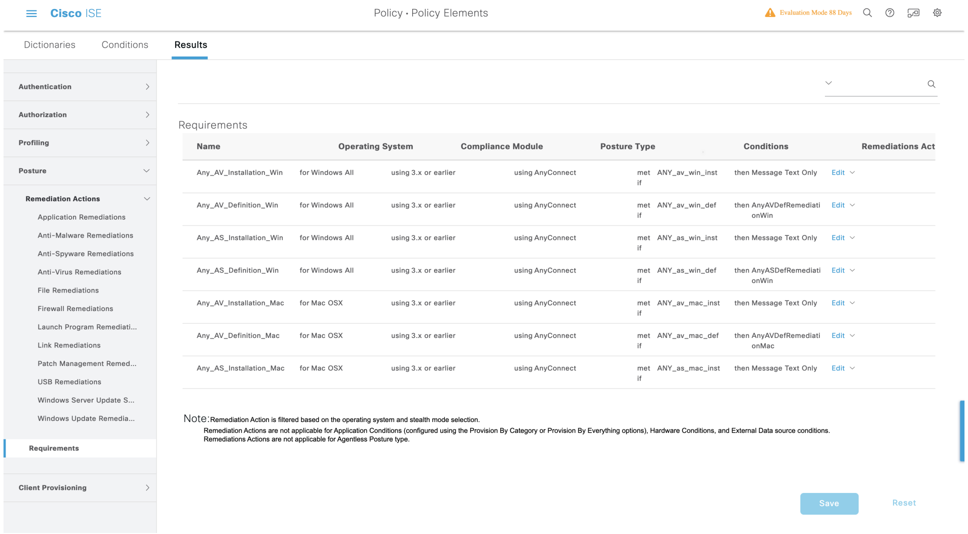
Step 6 Click **Submit**.

Posture Assessment Requirements

A posture requirement is a set of compound conditions with an associated remediation action that can be linked with a role and an operating system. All the clients connecting to your network must meet mandatory requirements during posture evaluation to become compliant on the network.

Posture-policy requirements can be set to mandatory, optional, or audit types in posture policies. If requirements are optional and clients fail these requirements, then the clients have an option to continue during posture evaluation of endpoints.

Figure 62: Posture Policy Requirement Types


Cisco ISE
Policy • Policy Elements
Evaluation Mode 88 Days
Dictionaries
Conditions
Results
Authentication
Authorization
Profiling
Posture
Remediation Actions
Application Remediations
Anti-Malware Remediations
Anti-Spyware Remediations
Anti-Virus Remediations
File Remediations
Firewall Remediations
Launch Program Remediati...
Link Remediations
Patch Management Remed...
USB Remediations
Windows Server Update S...
Windows Update Remedia...
Requirements
Client Provisioning
Save
Reset

Requirements

Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Act	
Any_AV_Installation_Win	for Windows All	using 3.x or earlier	using AnyConnect	met if ANY_av_win_inst	then Message Text Only	Edit
Any_AV_Definition_Win	for Windows All	using 3.x or earlier	using AnyConnect	met if ANY_av_win_def	then AnyAVDefRemediationWin	Edit
Any_AS_Installation_Win	for Windows All	using 3.x or earlier	using AnyConnect	met if ANY_as_win_inst	then Message Text Only	Edit
Any_AS_Definition_Win	for Windows All	using 3.x or earlier	using AnyConnect	met if ANY_as_win_def	then AnyASDefRemediationWin	Edit
Any_AV_Installation_Mac	for Mac OSX	using 3.x or earlier	using AnyConnect	met if ANY_av_mac_inst	then Message Text Only	Edit
Any_AV_Definition_Mac	for Mac OSX	using 3.x or earlier	using AnyConnect	met if ANY_av_mac_def	then AnyAVDefRemediationMac	Edit
Any_AS_Installation_Mac	for Mac OSX	using 3.x or earlier	using AnyConnect	met if ANY_as_mac_inst	then Message Text Only	Edit

Note: Remediation Action is filtered based on the operating system and stealth mode selection.
Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware Conditions, and External Data source conditions.
Remediations Actions are not applicable for Agentless Posture type.

Mandatory Requirements

During policy evaluation, the agent provides remediation options to clients who fail to meet the mandatory requirements defined in the posture policy. End users must remediate to meet the requirements within the time specified in the remediation timer settings.

For example, you have specified a mandatory requirement with a user-defined condition to check the existence of C:\temp\text.file in the absolute path. If the file does not exist, the mandatory requirement fails and the user will be moved to Non-Compliant state.

Optional Requirements

During policy evaluation, the agent provides an option to clients to continue, when they fail to meet the optional requirements specified in the posture policy. End users are allowed to skip the specified optional requirements.

For example, you have specified an optional requirement with a user-defined condition to check for an application running on the client machine, such as Calc.exe. Although, the client fails to meet the condition, the agent prompts an option to continue further so that the optional requirement is skipped and the end user is moved to Compliant state.

Audit Requirements

Audit requirements are specified for internal purposes and the agent does not prompt any message or input from end users, regardless of the pass or fail status during policy evaluation.

For example, you are in the process of creating a mandatory policy condition to check if end users have the latest version of the antivirus program. If you want to find out the non-compliant end users before actually enforcing it as a policy condition, you can specify it as an audit requirement.

Visibility Requirements

During policy evaluation, the agent reports compliance data for visibility requirements, every five to ten minutes.

Client System Stuck in Noncompliant State

If a client machine is unable to remediate a mandatory requirement, the posture status changes to “noncompliant” and the agent session is quarantined. To get the client machine past this “noncompliant” state, you need to restart the posture session so that the agent starts posture assessment on the client machine again. You can restart the posture session as follows:

- In wired and wireless Change of Authorization (CoA) in an 802.1X environment:
    - You can configure the Reauthentication timer for a specific authorization policy when you create a new authorization profile in the New Authorization Profiles window.
    - Wired users can get out of the quarantine state once they disconnect and reconnect to the network. In a wireless environment, the user must disconnect from the wireless lan controller (WLC) and wait until the user idle timeout period has expired before attempting to reconnect to the network.
- In a VPN environment—Disconnect and reconnect the VPN tunnel.

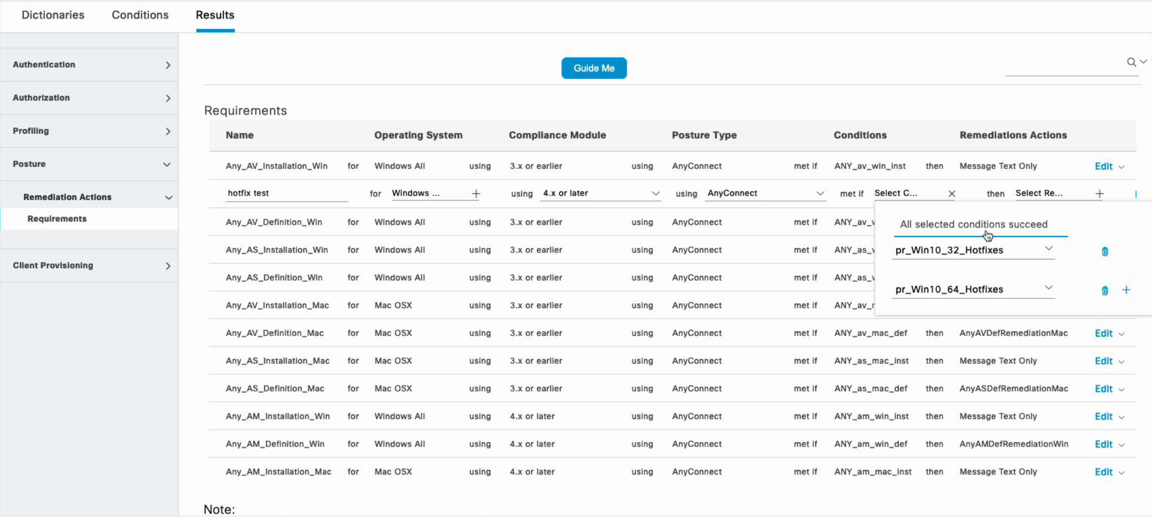
Create Client Posture Requirements

You can create a requirement in the Requirements window where you can associate user-defined conditions and Cisco defined conditions, and remediation actions. Once created and saved in the Requirements window, user-defined conditions and remediation actions can be viewed from their respective list windows.

Note

To create a Posture Requirement to validate all Windows 10 hotfixes in the environment, you must configure the Conditions area of your Requirement to include both pr_Win10_32_Hotfixes and pr_Win10_64_Hotfixes. At the top of the conditions, ensure **All selected conditions succeed** is selected. If the configuration is successful, **pr_Win10_32_Hotfixes & pr_Win10_64_Hotfixes** will be displayed. To view the details of the validated conditions for an endpoint, from the main menu, choose **Operations** > **Reports** > **Reports** > **Endpoints and Users** > **Posture Assessment by Endpoints**. Click the endpoint to view the corresponding posture details.

Figure 63: Validating Posture Requirements in Windows 10



Requirements

Name		Operating System		Compliance Module		Posture Type		Conditions		Remediations Actions	
Any_AV_Installation_Win	for	Windows All	using	3.x or earlier	using	AnyConnect	met if	ANY_av_win_inst	then	Message Text Only	Edit
hotfix test	for	Windows ...	using	4.x or later	using	AnyConnect	met if	Select C...	then	Select Re...	
Any_AV_Definition_Win	for	Windows All	using	3.x or earlier	using	AnyConnect	met if	ANY_av_v			
Any_AS_Installation_Win	for	Windows All	using	3.x or earlier	using	AnyConnect	met if	ANY_as_v			
Any_AS_Definition_Win	for	Windows All	using	3.x or earlier	using	AnyConnect	met if	ANY_as_v			
Any_AV_Installation_Mac	for	Mac OSX	using	3.x or earlier	using	AnyConnect	met if	ANY_av_r			
Any_AV_Definition_Mac	for	Mac OSX	using	3.x or earlier	using	AnyConnect	met if	ANY_av_mac_def	then	AnyAVDefRemediationMac	Edit
Any_AS_Installation_Mac	for	Mac OSX	using	3.x or earlier	using	AnyConnect	met if	ANY_as_mac_inst	then	Message Text Only	Edit
Any_AS_Definition_Mac	for	Mac OSX	using	3.x or earlier	using	AnyConnect	met if	ANY_as_mac_def	then	AnyASDefRemediationMac	Edit
Any_AM_Installation_Win	for	Windows All	using	4.x or later	using	AnyConnect	met if	ANY_am_win_inst	then	Message Text Only	Edit
Any_AM_Definition_Win	for	Windows All	using	4.x or later	using	AnyConnect	met if	ANY_am_win_def	then	AnyAMDefRemediationWin	Edit
Any_AM_Installation_Mac	for	Mac OSX	using	4.x or later	using	AnyConnect	met if	ANY_am_mac_inst	then	Message Text Only	Edit

All selected conditions succeed
pr_Win10_32_Hotfixes
pr_Win10_64_Hotfixes

Note:

Before you begin

- You must have an understanding of acceptable use policies (AUPs) for a posture.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture** > **Requirements**.

Step 2 Enter the values in the **Requirements** window.

Step 3 Click **Done** to save the posture requirement in read-only mode.

Step 4 Click **Save**.

Posture Reassessment Configuration Settings

The following table describes the fields in the Posture Reassessment Configurations window, which you can use to configure posture reassessment. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **Reassessments**.

Table 176: Posture Reassessment Configuration Settings

Field Name	Usage Guidelines
Configuration Name	Enter the name of PRA configuration.
Configuration Description	Enter a description for PRA configuration.
Use Reassessment Enforcement?	Check the check box to apply the PRA configurations for the user identity groups.
Enforcement Type	Choose the action to be enforced: • **Continue**: The user continues to have the privileged access without any user intervention to remediate the client irrespective of the posture requirement. • **Logoff**: If the client is not compliant, the user is forced to logoff from the network. When the client logs in again, the compliance status is unknown. • **Remediate**: If the client is not compliant, the agent waits for a specified time for the remediation to happen. Once the client has remediated, the agent sends the PRA report to the policy service node. If the remediation is ignored on the client, then the agent sends a logoff request to the policy service node to force the client to logoff from the network. If the posture requirement is set to mandatory, then the RADIUS session will be cleared as a result of the PRA failure action and a new RADIUS session has to start for the client to be postured again. If the posture requirement is set to optional, then the agent on the client allows the user to click the continue option from the agent. The user can continue to stay in the current network without any restriction.
Interval	Enter a time interval in minutes to initiate PRA on the clients after the first successful login. The default value is 240 minutes. Minimum value is 60 minutes and maximum is 1440 minutes.
Grace time	Enter a time interval in minutes to allow the client to complete remediation. The grace time cannot be zero, and should be greater than the PRA interval. It can range between the default minimum interval (5 minutes) and the minimum PRA interval. The minimum value is 5 minutes and the maximum value is 60 minutes. **Note** The grace time is enabled only when the enforcement type is set to remediate action after the client fails the posture reassessment.
Select User Identity Groups	Choose a unique group or a unique combination of groups for your PRA configuration.
PRA configurations	Displays existing PRA configurations and user identity groups associated to PRA configurations.

Related Topics

- Posture Lease, on page 1149
- Periodic Reassessments, on page 1150
- Posture Assessment Options, on page 1193
- Posture Remediation Options, on page 1195
- Custom Conditions for Posture, on page 1195
- Custom Posture Remediation Actions, on page 1197
- Configure Periodic Reassessments, on page 1150

Custom Permissions for Posture

A custom permission is a standard authorization profile that you define in Cisco ISE. Standard authorization profiles set access privileges based on the matching compliance status of the endpoints. The posture service broadly classifies the posture into unknown, compliant, and noncompliant profiles. The posture policies and the posture requirements determine the compliance status of the endpoint.

You must create three different authorization profiles for an unknown, compliant, and noncompliant posture status of endpoints that can have different set of VLANs, DACLs, and other attribute value pairs. These profiles can be associated with three different authorization policies. To differentiate these authorization policies, you can use the Session:PostureStatus attribute along with other conditions.

Unknown Profile

If no matching posture policy is defined for an endpoint, then the posture compliance status of the endpoint may be set to unknown. A posture compliance status of unknown can also apply to an endpoint where a matching posture policy is enabled but posture assessment has not yet occurred for that endpoint and, therefore no compliance report has been provided by the client agent.

Note We recommend you to use posture with redirection for all Cisco network access devices.

Compliant Profile

If a matching posture policy is defined for an endpoint, then the posture compliance status of the endpoint is set to compliant. When the posture assessment occurs, the endpoint meets all the mandatory requirements that are defined in the matching posture policy. For an endpoint that is postured compliant, it can be granted privileged network access on your network.

Noncompliant Profile

The posture compliance status of an endpoint is set to noncompliant when a matching posture policy is defined for that endpoint but it fails to meet all the mandatory requirements during posture assessment. An endpoint that is postured noncompliant matches a posture requirement with a remediation action, and it should be granted limited network access to remediation resources in order to remediate itself.

Configure Standard Authorization Policies

You can define two types of authorization policies on the Authorization Policy window, standard exceptions authorization policies. The standard authorization policies that are specific to posture are used to make policy decisions based on the compliance status of endpoints.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Sets**.

Step 2 In the **View** column, click the arrow icon adjacent the corresponding Default Policy.

Step 3 In the **Actions** column, click the cog icon, and then from the dropdown list, choose a new authorization policy.
A new row appears in the **Policy Sets** table.

Step 4 Enter a rule name.

Step 5 From the **Conditions** column, click the (+) symbol.

Step 6 Create the required conditions on the **Conditions Studio Page**. In the **Editor** section, click the **Click To Add an Attribute** text box, and select the required Dictionary and Attribute.

You can drag and drop a Library condition to the **Click To Add An Attribute** text box.

Step 7 Click **Use** to create a new standard authorization policy in read-only mode.

Step 8 Click **Save**.

Best Practices for Network Drive Mapping with Posture

During posture assessment of a Windows endpoint, the endpoint user may encounter a delay in accessing the desktop. This may be due to Windows trying to restore the file server drive letter mappings before providing the user access to the desktop. The best practices to avoid the delay during posture are:

- Endpoints should be able to reach the Active Directory server because the file server drive letter cannot be mapped without reaching the AD. When posture (with AnyConnect ISE posture agent) triggers, it blocks access to AD, causing delay in login. Use Posture Remediation ACLs to provide access to AD servers before posture is completed.
- You should set a delay for the login script until posture completes and then you have to set the Persistence attribute to NO. Windows tries to reconnect all the network drives during login and this cannot be done until AnyConnect ISE posture agent gains full network access.

Configure AnyConnect Stealth Mode Workflow

The process of configuring AnyConnect in the stealth mode involves a series of steps. You should perform the following steps in Cisco ISE.

Step 1 Create an AnyConnect agent profile, see Create an AnyConnect Agent Profile.

Step 2 Create an AnyConnect configuration for AnyConnect packages, see Create an AnyConnect Configuration for AnyConnect Packages.

Step 3 Upload a Open DNS Profile in Cisco ISE, see Upload an Open DNS Profile in Cisco ISE.

Step 4 Create a Client Provisioning Policy, see Create a Client Provisioning Policy.

Step 5 Create a Posture Condition, see Create a Posture Condition.

Step 6 Create Posture Remediation, see Create Posture Remediation

Step 7 Create Posture Requirement in Clientless Mode, see Create Posture Requirement in Stealth Mode.

Step 8 Create Posture Policy, see Create Posture Policy.

Step 9 Configure authorization profile.

  a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.
  b) Click **Add** and enter the **Name** of the profile.
  c) In Common Tasks, enable **Web Redirection (CWA, MDM, NSP, CPP)** and choose **Client provisioning (Posture)** from the drop-down list, enter the redirect **ACL** name and choose the Client Provisioning Portal **Value**. You can edit or create a new Client Provisioning Portal in **Work Centers** > **Posture** > **Client Provisioning** > **Client Provisioning Portal**.

Step 10 Configure authorization policies.

  a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Sets**
  b) Click > and choose **Authorization Policy** and click on + icon to create a new authorization rule that features **Session:Posture Status EQUALS Unknown** condition and the authorization profiled configured previously.
  c) Above the previous rule, create a new authorization rule that features **Session:Posture Status EQUALS NonCompliant** condition and another one that features **Session:Posture Status EQUALS Compliant** condition.

Create an AnyConnect Agent Profile

Before you begin

You must upload the AnyConnect packages for MAC and Windows OS and the AnyConnect compliance modules.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Step 2 From the **Add** drop-down list, choose **AnyConnect Posture Profile**.

Step 3 From the **Posture Agent Profile Settings** drop-down list, choose **AnyConnect**.

Step 4 In the **Name** field, type the required name (for example, AC_Agent_Profile).

Step 5 In the **Agent Behavior** section, select the **Stealth Mode** parameter as **Enabled**.

Step 6 Click **Save**.

What to do next

You should create the AnyConnect configuration for the AnyConnect packages.

Create an AnyConnect Configuration for AnyConnect Packages

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Step 2 From the **Add** drop-down list, choose **AnyConnect Configuration**.

Step 3 From the **Select AnyConnect Package** drop-down list, choose the required AnyConnect package.

Step 4 In the **Configuration Name** text box, type the required Name.

Step 5 In the **Compliance Module** drop-down list, choose the required compliance module.

Step 6 In the **AnyConnect Module Selection** section, check the **ISE Posture** and **Network Access Manager** check boxes.

Step 7 In the **Profile Selection** section, from the **ISE Posture** drop-down list, choose the AnyConnect agent profile.

Step 8 From the **Network Access Manager** drop-down list, choose the required AnyConnect agent profile.

What to do next

You should upload the Open DNS profile to be pushed to the client.

Upload an Open DNS Profile in Cisco ISE

The Open DNS profile is pushed to the client.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Step 2 From the **Add** drop-down list, choose **Agent Resources From Local Disk**.

Step 3 From the **Category** drop-down list, choose **Customer Created Packages**.

Step 4 From the **Type** drop-down list, choose **AnyConnect Profile** .

Step 5 In the **Name** text box, type the required name (for example, OpenDNS).

Step 6 Click **Browse** and locate the JSON file from the local disk.

Step 7 Click **Submit**.

What to do next

You should create the client provisioning policy.

Create a Client Provisioning Policy

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Client Provisioning**.

Step 2 Create the required rule (for example, Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117).

What to do next

You should create the posture condition.

Create a Posture Condition

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **File Condition**.

Step 2 Enter the required name (for example, filechk).

Step 3 From the **Operating Systems** drop-down list, choose Windows 7 (All).

Step 4 From the **File Type** drop-down list, choose FileExistence.

Step 5 From the **File Path** drop-down list, choose ABSOLUTE_PATH C:\test.txt.

Step 6 From the **File Operator** drop-down list, choose DoesNotExist.

What to do next

You should create the posture remediation.

Create Posture Remediation

The file condition checks if test.txt file exists on the endpoint. If it does not exist, the remediation is to block the USB port and prevent the installation of the file using a USB device.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Remediation Actions** > **USB Remediations**.

Step 2 Enter the required name (for example, clientless_mode_block).

Step 3 Click **Submit**.

What to do next

You should create the posture requirement.

Create Posture Requirement in Stealth Mode

When you create a Remediation action from the Requirements page, only the remediations that are applicable to stealth mode are displayed: Anti-Malware, Launch Program, Patch Management, USB, Windows Server Update Services, and Windows Update.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Step 2 Create the required posture requirement (for example, Name=win7Req for Operating Systems=Windows7(All) using Compliance Module=4.x or later using Posture Type=AnyConnect Stealth met if Condition=filechk then Remediation Actions=clientless_mode_block).

What to do next

You should create the posture policy.

Create Posture Policy

Before you begin

Ensure that the posture policy requirement and the policy are created in the clientless mode.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Posture**

Step 2 Create the required rule. For example, if Identity Groups=Any and Operating Systems=Windows 7(All) and Compliance Module=4.x or later and Posture Type=AnyConnect Stealth then Requirements=win7Req.

Note For Client Provisioning without URL redirection, configuring the conditions with attributes specific to Network Access or Radius will not work and matching of the client provisioning policy might fail due to the non-availability of session information for the specific user in the Cisco ISE server. However, Cisco ISE allows configuring conditions for the externally added identity groups.

Enable AnyConnect Stealth Mode Notifications

Cisco ISE provides several new failure notifications for AnyConnect stealth mode deployments. Enabling failure notifications in stealth mode helps you to identify issues with wired, wireless, or VPN connections. To enable notifications in stealth mode:

Note AnyConnect version 4.5.0.3040 and higher supports stealth mode notifications.

Before you begin

Configure AnyConnect in stealth mode.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose Choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Step 2 Choose **Add** > **AnyConnect ISE Posture Profile**.

Step 3 From the **Select a Category** drop-down list, choose **AnyConnect** .

Step 4 From the **Agent Behavior** section, choose **Enabled** for the **Enable notifications in stealth mode** option.

Configure Cisco Temporal Agent Workflow

The process of configuring the Cisco temporal agent involves a series of steps. You should perform the following steps in Cisco ISE.

Step 1 Create Posture Condition

Step 2 Create Posture Requirements

Step 3 Create the Posture Policy

Step 4 Configure the Client Provisioning Policy

Step 5 Configure authorization profile.

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.

b) Click **Add** and enter the **Name** of the profile.

c) In Common Tasks, enable **Web Redirection (CWA, MDM, NSP, CPP)** and choose **Client provisioning (Posture)** from the drop-down list, enter the redirect **ACL** name and choose the Client Provisioning Portal **Value**. You can edit or create a new Client Provisioning Portal in **Work Centers** > **Posture** > **Client Provisioning** > **Client Provisioning Portal**.

Step 6 Configure authorization policies.

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Sets**.

b) Click **>** and choose **Authorization Policy** and click on **+** icon to create a new authorization rule that features **Session:Posture Status EQUALS Unknown** condition and the authorization profiled configured previously.

c) Above the previous rule, create a new authorization rule that features **Session:Posture Status EQUALS NonCompliant** condition and another one that features **Session:Posture Status EQUALS Compliant** condition.

Step 7 Download and Launch Cisco Temporal Agent

Create Posture Condition

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **File Condition**.

Step 2 Enter the required name (for example, filecondwin).

Step 3 From the **Operating Systems** drop-down list, choose Windows 7 (All).

Step 4 From the **File Type** drop-down list, choose FileExistence.

Step 5 From the **File Path** drop-down list, choose ABSOLUTE_PATH C:\test.txt.

Step 6 From the **File Operator** drop-down list, choose DoesNotExist.

Create Posture Requirements

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture** > **Requirements**.

Step 2 From the **Edit** drop-down list, choose **Insert New Requirement**.

Step 3 Enter the **Name**, **Operating Systems**, and **Compliance Module** (for example, Name filereqwin, Operating Systems Windows All, Compliance Module 4.x or later).

Step 4 In the **Posture Type** drop-down, choose **Temporal Agent**.

Step 5 Select the required condition (for example, filecondwin).

Note For the Cisco Termporal Agent, you can only view Patch Management conditions containing the **Installation** check type in the **Requirements** page.

Step 6 Select the **Message Text Only** remediation action.

Note The temporal agent is supported by AnyConnect 4.x or later.

Create the Posture Policy

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Posture**.

Step 2 Create the required rule (for example, Name=filepolicywin, Identity Groups=Any, Operating Systems=Windows All, Compliance Module=4.x or later, Posture Type=Temporal Agent, and Requirements=filereqwin).

Configure the Client Provisioning Policy

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Client Provisioning**.

Step 2 Create the required rule (for example, Rule Name=Win, Identity Groups=Any, Operating Systems=Windows All, Other Conditions=Conditions, Results=CiscoTemporalAgentWindows4.5).

Download and Launch Cisco Temporal Agent

Step 1 Connect to the SSID.

Step 2 Launch a Browser and you will be redirected to the Client Provisioning Portal.

Step 3 Click **Start**. This checks if the Cisco Temporal agent is installed and running.

Step 4 Click **This Is My First Time Here**.

Step 5 Choose **Click Here to Download and Launch Cisco Temporal Agent**.

Step 6 Save the Cisco Temporal Agent .exe or .dmg file for Windows or macOS respectively. For Windows, run the .exe file and for macOS, double-click the .dmg file and run the acisetempagent app.

The Cisco Temporal Agent scans the client and displays the results, such as Red cross marks for non-compliant checks.

Posture Troubleshooting Tool

The Posture Troubleshooting tool helps you find the cause of a posture-check failure to identify the following:

- Which endpoints were successful in posture and which were not.
- If an endpoint failed in posture, what steps failed in the posture process.
- Which mandatory and optional checks passed and failed.

You determine this information by filtering requests based on parameters, such as username, MAC address, and posture status.

Configure Endpoint Login Credentials

The **Endpoint Login Configuration** window is where you configure login credentials so Cisco ISE can log in to clients. The login credentials that are configured in this window are used by the following Cisco ISE features:

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Endpoint Scripts** > **Settings**.

The following tabs are displayed:

- **Windows Domain User**: Configure the domain credentials that Cisco ISE must use to log in to a client via SSH. Click the **Plus** icon and enter as many Windows logins as you need. For each domain, enter the required values in the **Domain**, **Username**, and **Password** fields. If you configure domain credentials, the local user credentials that are configured in the **Windows Local User** tab are ignored.
- **Windows Local User**: Configure the local account that Cisco ISE uses to access the client via SSH. The local account must be able to run Powershell and Powershell remote.
- **MAC Local User**: Configure the local account that Cisco ISE uses to access the client via SSH. The local account must be able to run Powershell and Powershell remote. In the **Username** field, enter the Account Name of the local account. To view a Mac OS Account Name, run the following command in the Terminal:

  ```
  whoami
  ```

Endpoint Scripts Settings

This page configures options for Endpoint Scripts and Agentless Posture.

- **Upload endpoint script execution logs to ISE**: Enabled by default, you can upload endpoint scripts to Cisco ISE. Disabling this disables endpoint scripts, you cannot upload or run endpoint scripts.

- **Endpoint script execution verbose logging**: Enable verbose logging for debugging.
- **Endpoints processor batch size**: You can adjust this accommodate network loads and system performance.
- **Endpoints processing concurrency for MAC**
- **Endpoints processing concurrency for Windows**
- **Maximum retry attempts for OS identification**
- **Delay between retries for OS identification (msec)**
- **Endpoint pagination batch size**
- **Log retention period on Endpoints (Days)**
- **Connection Time out (sec)**
- **Max-retry attempts for Connection**
- **Port Number for Powershell**: Change this to use a nonstandard port number.
- **Port Number for SSH Connection**: Change this to use a nonstandard port number.

Configure Client Provisioning in Cisco ISE

Enable client provisioning to allow users to download client provisioning resources and configure agent profiles. You can configure agent profiles for Windows, Mac OS X, and Linux clients, and native supplicant profiles for personal devices. If you disable client provisioning, users attempting to access the network will receive a warning message indicating that they are not able to download client provisioning resources.

Before you begin

If you are using a proxy and hosting client provisioning resources on a remote system, verify that the proxy allows clients to access that remote location.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Client Provisioning** or **Work Centers** > **Posture** > **Settings** > **Software Updates** > **Client Provisioning**.

Step 2 From the **Enable Provisioning** drop-down list, choose **Enable** or **Disable**.

Step 3 From the **Enable Automatic Download** drop-down list, choose **Enable**.

Feed downloads include all the available client provisioning resources. Some of these resources may not be pertinent to your deployment. Cisco recommends manually downloading resources whenever possible instead of setting this option.

Step 4 Specify the URL where Cisco ISE searches for system updates in the **Update Feed URL** text box. For example, the default URL for downloading client-provisioning resources is https://www.cisco.com/web/secure/spa/provisioning-update.xml.

Step 5 When there is no client provisioning resource for a device, choose one of the following options:

- **Allow Network Access**: Users are allowed to register their device on the network without having to install and launch the native supplicant wizard.

- **Apply Defined Authorization Policy**: Users must try to access the Cisco ISE network via standard authentication and authorization policy application (outside of the native supplicant provisioning process). If you enable this option, the user device goes through standard registration according to any client-provisioning policy applied to the user's ID. If the user's device requires a certificate to access the Cisco ISE network, you must also provide detailed instructions to the user describing how to obtain and apply a valid certificate using the customizable user-facing text fields.

Step 6 Click **Save**.

Note If the ISE certificates are cached in the HTTP Strict Transport Security (HSTS) store of the endpoint, client provisioning portal redirection might fail and you might see the following error message:

```
You cannot visit hostname.domain.com right now because the website uses HSTS. Network errors
and attacks are temporary, so this page will probably work later.
```

To resolve this issue, delete the browser cache on the endpoint or navigate to chrome://net-internals/#hsts and delete the self-signed ISE certificates.

What to do next

Configure client provisioning resource policies.

Client Provisioning Resources

Client provisioning resources are downloaded to endpoints after the endpoint connects to the network. Client provisioning resources consist of compliance and posture agents for desktops, and native supplicant profiles for phones and tablets. Client provisioning policies assign these provisioning resources to endpoints to start a network session.

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy Elements** > **Results** > **Client Provisioning** > **Resources**. The following resource types can be added to the list by clicking the **Add** button:

- **Agent resources from Cisco Site**: Select the AnyConnect and supplicant provisioning wizards you want to make available for client provisioning policies. Cisco periodically updates this list of resources, adding new ones and updating existing ones. You can also set up ISE to download all the Cisco resources and resource updates automatically, see Configure Client Provisioning in Cisco ISE, on page 1216 for more information.
- **Agent resources from local disk**: Select resources on your PC that you want to upload to ISE, see Add Cisco Provided Client Provisioning Resources from a Local Machine, on page 1219.
-
- **Native Supplicant Profile**: Configure a supplicant profile for phones and tablets that contain settings for your network. For more information, see Create Native Supplicant Profiles.
- **AnyConnect ISE Posture Profile**: Configure the AnyConnect ISE Posture here when you don't want to create and distribute agent XML profiles. For more information about the AnyConnect ISE Posture agent and ISE Posture Profile Editor, see the AnyConnect Administrators Guide for your version of

AnyConnect https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-installation-and-configuration-guides-list.html.

After creating client provisioning resources, create client provisioning policies that apply the client provisioning resources to the endpoints. See Configure Client Provisioning Resource Policies, on page 1245.

Related Topics

Configure Client Provisioning in Cisco ISE, on page 1216
Add Client Provisioning Resources from Cisco, on page 1218
Add Cisco Provided Client Provisioning Resources from a Local Machine, on page 1219
Add Customer Created Resources for AnyConnect from a Local Machine, on page 1220

Add Client Provisioning Resources from Cisco

You can add client provisioning resources from Cisco.com for Cisco Web agent, AnyConnect Windows, MacOS, and Linux clients. Depending on the resources that you select and available network bandwidth, Cisco ISE can take a few minutes to download client provisioning resources to Cisco ISE.

Before you begin

- Ensure that you have configured the correct proxy settings in Cisco ISE.
- Enable client provisioning in Cisco ISE.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Step 2 Choose **Add** > **Agent resources from Cisco site**.

Step 3 Select one or more required client provisioning resources from the list available in the **Download Remote Resources** dialog box.

Step 4 Click **Save**.

Note the following while installing the Linux agent:

- If you are using self-signed certificates:
  - You must enable the SSH agent to copy the ISE certificate to the Linux agent.
    - For RHEL:
      1. Export the certificate from Cisco ISE GUI.

Attention For Red Hat Linux, you must add the IP address to the SAN field of the self-signed certificate.

      2. Copy <certificate>.pem to /etc/pki/ca-trust/source/anchors/ and rename the file to <certificate>.crt.
      3. Run the following command: **sudo update-ca-trust extract**

4. Go to /etc/pki/tls/certs/
5. Run the following command: **openssl x509 -in ca-bundle.crt -text -noout**

- For Ubuntu:
  1. Export the certificate from Cisco ISE GUI.
  2. Copy <certificate>.pem to /usr/local/share/ca-certificates/ and rename it to <certificate>.crt.
  3. Run the following command: **sudo update-ca-certificates**

     To verify whether the CA certificate is installed properly, go to /etc/ssl/certs/ca-certificates.crt and check the certificate present in this file.

Note Certificate import is not required, if the ISE certificate is issued by a trusted CA.

- Initiate dot1x redirect or non-redirect flow.
- If you are using RHEL, ensure that yum is updated with subscription manager. Update apt-get if you are using Ubuntu.

  For more information about the system requirements for Linux agent, see the Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.9.

What to do next

After you have successfully added client provisioning resources to Cisco ISE, you can begin to configure client provisioning resource policies.

Add Cisco Provided Client Provisioning Resources from a Local Machine

You can add client provisioning resources from the local disk, which you previously downloaded from Cisco.

Before you begin

Be sure to upload only current, supported resources to Cisco ISE. Older, unsupported resources are likely to cause serious issues for client access.

If you are downloading the resource files manually from the Cisco.com, see the Section “Cisco ISE Offline Updates” in the Cisco ISE Release Notes.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**

Step 2 Choose **Add** > **Agent resources from local disk**.

Step 3 Choose **Cisco Provided Packages** from the **Category** drop-down list.

Step 4 Click **Browse** to the directory on your local machine where the resource file that you want to download to Cisco ISE resides.

You can add AnyConnect or Cisco Web Agent resources that you previously downloaded from Cisco to your local machine.

Step 5 Click **Submit**.

What to do next

After you have successfully added client provisioning resources to Cisco ISE, you can configure client provisioning resource policies.

Add Customer Created Resources for AnyConnect from a Local Machine

Add customer created resources like AnyConnect customization and localization packages and AnyConnect profiles from the local machine to Cisco ISE.

Before you begin

Ensure that customer created resources for AnyConnect are zipped files and available in your local disk.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client provisioning** > **Resources**.

Step 2 Choose **Add** > **Agent Resources from local disk**.

Step 3 Choose **Customer Created Packages** from the **Category** drop-down list.

Step 4 Enter the name and description for AnyConnect resources.

Step 5 Click **Browse** to the directory on your local machine where the resource file that you want to download to Cisco ISE resides.

Step 6 Choose the following AnyConnect resources to upload to Cisco ISE:

- AnyConnect customization bundle
- AnyConnect localization bundle
- AnyConnect profile
- Advanced Malware Protection (AMP) Enabler Profile

Step 7 Click **Submit**.
The Uploaded AnyConnect Resources table displays AnyConnect resources that you add to Cisco ISE.

What to do next

Create AnyConnect agent configuration.

Create Native Supplicant Profiles

You can create native supplicant profiles to enable users to bring their own devices into the Cisco ISE network. When the user signs in, Cisco ISE uses the profile that you associated with that user's authorization requirements to choose the necessary supplicant provisioning wizard. The wizard runs and sets up the user’s personal device to access the network.

Note The provisioning wizard only configures interfaces which are active. Because of this, users with Wired and Wireless connections will not be provisioned for both interfaces, unless they are both active.

Before you begin

- Open up TCP port 8905 to enable the installation of Cisco AnyConnect Agent, Cisco Web Agent, and supplicant provisioning wizard. For more information about port usage, see the “Cisco ISE Appliance Ports Reference” appendix in the *Cisco Identity Services Engine Hardware Installation Guide*.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Step 2 Choose **Add** > **Native Supplicant Profile**.

Step 3 Create a profile, using the procedure described in Native Supplicant Profile Settings, on page 1221.

What to do next

Enable self-provisioning capabilities that allow employees to directly connect their personal devices to the network, as described in the Support for multiple Guest Portals section.

Native Supplicant Profile Settings

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources** > **Add** > **Native Supplicant Profile**. The following settings are displayed.

- **Name**: Enter the name of the native supplicant profile that you are creating.
- **Operating System**: Choose which operating system(s) this profile should apply to from the drop-down list.

Each profile defines the settings for a network connection that Cisco ISE will apply to the client's native supplicant.

Wireless Profile

Configure a wireless profile, one for each SSID that you want to make available to the client:

- **SSID Name**: Enter the name of the SSID that the client will connect to.
- **Proxy Auto-Config File URL**: If the client will connect to a proxy to get the network configuration for its supplicant, enter the URL of that proxy server.
- **Proxy Host/IP**: If the client will connect to a proxy to get the network configuration for its supplicant, enter the Host/IP of that proxy server.

- **Proxy Port**: If the client will connect to a proxy to get the network configuration for its supplicant, enter the port of that proxy server.
- **Security**: Choose either **WPA** or **WPA2**.
- **Allowed Procotol**: Choose either **PEAP** or **EAP-TLS**.
- **Certificate Template**: For TLS, choose one of the certificate templates. The certificate templates are defined in **Administration** > **System Certificates** > **Certificate Authority** > **Certificate Templates**.

Optional Settings

If you expand **Optional**, the following fields are displayed.

Windows Setings

- **Authentication Mode**: Choose **User**, **Machine** or **both** as credentials for authorization.
- **Do not prompt user to authorize new servers or trusted certification authorities**: If this option is enabled, the user is not prompted to authorize. User certificates are automatically accepted.
- **Use a different user name for the connection**: This is applicable only for wireless profiles. Use a different user name for the connection.
- **Connect even if the network is not broadcasting its name (SSID)**: This is applicable only for wireless profiles. Connect to a network even when its SSID is not being broadcasted.

iOS Settings

- **Enable if target network is hidden**: Check this check box if the target network is hidden.

Android Settings

- **Certificate Enrollment Protocol:** : Click either of these radio buttons to choose the Certificate Enrollment Protocol: **Enrollment over Secure Transport (EST)** or **Simple Certificate Enrollment Protocol (SCEP)**. If you choose the EST protocol, Cisco ISE will ask for additional password inputs from Android users when issuing certificates.

Wired Profile

- **Allowed Protocol**: Choose either **PEAP** or **EAP-TLS**.
- **Certificate Template**: For TLS, choose one of the certificate templates. The certificate templates are defined in **Administration** > **System Certificates** > **Certificate Authority** > **Certificate Templates**.

Optional Settings

If you expand **Optional**, the following fields are also available for Windows clients.

- **Authentication Mode**: Choose **User**, **Machine** or **both** as credentials for authorization.
- **Automatically use logon name and password (and domain if any)**: If you selected **User** for **Authentication Mode**, use the logon and password to without prompting the user, if that information is available.

- **Enable Fast Reconnect**: Allow a PEAP session to resume without checking user credentials when the session resume feature is enabled in the PEAP protocol options, which is configured on **Administration** > **System** > **Settings** > **Protocols** > **PEAP**.
- **Enable Quarantine Checks**: Check if the client has been quarantined.
- **Disconnect if server does not present cryptobinding TLV**: Disconnect if cryptobinding TLV is not supported for the network connection.
- **Do not prompt user to authorize new servers or trusted certification authorities**: Automatically accept user certificates; do not prompt the user.

Client Provisioning Without URL Redirection for Different Networks

Client provisioning without URL redirection is required when the third party NAC does not support CoA. You can perform client provisioning with and without URL redirection.

Note For client provisioning with URL redirection, if the client machine has proxy settings configured, ensure that you add Cisco ISE to the list of exceptions in the browser settings. This setting is applicable for all flows, BYOD, MDM, Guest, and Posture that use URL redirection. For example, on Windows machines, do the following:

1. From Control Panel, click **Internet Properties**.
2. Select the **Connections** tab.
3. Click **LAN settings**.
4. Click **Advanced** from the Proxy server area.
5. Enter the IP addresses of the Cisco ISE nodes in the **Exceptions** box.
6. Click **OK**.

Given below are the steps you perform to provision an endpoint without redirection for different networks.

Dot1X EAP-TLS

1. Connect the Cisco ISE network with provisioned certification.
2. Open a browser window and type in the provisioning URL: provisioning.cisco.com.
3. Log into the CP portal via internal user, AD, LDAP, or SAML.

   AnyConnect performs posture. The endpoint moves to the right network based on posture compliance.

Dot1X PEAP

1. Connect the Cisco ISE network with User Name and Password through NSP
2. Open a browser window and type in the provisioning URL: provisioning.cisco.com.

3. Log into the CP portal via internal user, AD, LDAP, or SAML

   AnyConnect performs posture. The endpoint moves to the right network based on posture compliance.

MAB (Wired Networks)

1. Connect the Cisco ISE network.
2. Open a browser window and type in the provisioning URL: provisioning.cisco.com.
3. Log into the CP portal via internal user, AD, LDAP, or SAML.

   AnyConnect performs posture. The endpoint moves to the right network based on posture compliance.

MAB (Wireless Networks)

1. Connect the Cisco ISE network
2. Open a browser window and type in the provisioning URL: provisioning.cisco.com.
3. Log into the CP portal via internal user, AD, LDAP, or SAML.

   AnyConnect performs posture. Posture starts for wireless 802.1X only.

AMP Enabler Profile Settings

The following table describes the fields in the Advanced Malware Protection (AMP) Enabler Profile window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Click the **Add** drop-down arrow and select the **AMP Enabler Profile**.

Table 177: AMP Enabler Profile Page

Field Names	Usage Guidelines
Name	Enter the name of the AMP enabler profile that you want to create.
Description	Enter a description for the AMP enabler profile.
Install AMP Enabler	• **Windows Installer**: Specify the URL of the local server that hosts the AMP for Windows OS software. The AnyConnect module uses this URL to download the .exe file to the endpoint. The file size is approximately 25 MB. • **Mac Installer**: Specify the URL of the local server that hosts the AMP for macOS software. The AnyConnect module uses this URL to download the .pkg file to the endpoint. The file size is approximately 6 MB. The **Check** button communicates with the server to verify if the URL is valid. If the URL is valid, a "File found" message is displayed or else an error message is displayed.
Uninstall AMP Enabler	Uninstalls the AMP for endpoint software from the endpoint.

Field Names	Usage Guidelines
Add to Start Menu	Adds a shortcut for the AMP for endpoint software in the Start menu of the endpoint, after the AMP for endpoint software is installed on the endpoint.
Add to Desktop	Adds an icon for the AMP for endpoint software on the desktop of the endpoint, after the AMP for endpoint software is installed on the endpoint.
Add to Context Menu	Adds the Scan Now option in the right-click context menu of the endpoint, after the AMP for endpoint software is installed on the endpoint.

Create an AMP Enabler Profile Using the Embedded Profile Editor

You can create the AMP enabler profile using the Cisco ISE embedded profile editor or the standalone editor.

To create the AMP enable profile using the Cisco ISE embedded profile editor:

Before you begin

- Download the AMP for Endpoint software from the SOURCEfire portal and host it on a local server.
- Import the certificate of the server that hosts the AMP for endpoint software to the ISE certificate store. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Certificates** > **Trusted Certificates**.
- Ensure that the **AMP Enabler** options are selected in the **AnyConnect Module Selection** and **Profile Selection** sections in the **AnyConnect Configuration** window (**Policy** > **Policy Elements** > **Results** > **Client provisioning** > **Resources** > **Add** > **AnyConnect Configuration** > **Select AnyConnect Package**).
- You must log in to the SOURCEfire portal, create policies for endpoint groups, and download the AMP for endpoint software. The software comes preconfigured with the policies that you have chosen. You must download two images, namely, the redistributable version of the AMP for endpoint software for Windows OS and AMP for endpoint software for macOS. The downloaded software is hosted on a server that is accessible from the enterprise network.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provision** > **Resources**.

Step 2 Click the **Add** drop-down.

Step 3 Choose **AMP Enabler Profile** to create a new AMP enabler profile.

Step 4 Enter the appropriate values in the fields.

Create an AMP Enabler Profile Using the Standalone Editor

To create an AMP enabler profile using the AnyConnect standalone editor.

Before you begin

You can create an AMP enabler profile by uploading the XML format of the profile using the AnyConnect 4.1 standalone editor.

- Download the AnyConnect standalone profile editor for Windows and Mac OS from Cisco.com.
- Launch the standalone profile editor and enter the fields as specified in the AMP Enabler Profile Settings.
- Save the profile as an XML file in your local disk.
- Ensure that the **AMP Enabler** options are selected in the **AnyConnect Module Selection** and **Profile Selection** sections in the **AnyConnect Configuration** window (**Policy** > **Policy Elements** > **Results** > **Client provisioning** > **Resources** > **Add** > **AnyConnect Configuration** > **Select AnyConnect Package**).

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client provisioning** > **Resources**

Step 2 Click **Add**.

Step 3 Choose **Agent resources from local disk**.

Step 4 Choose **Customer Created Packages** from the **Category** drop-down.

Step 5 Choose **AMP Enabler Profile** from the **Type** drop-down.

Step 6 Enter a **Name** and **Description**.

Step 7 Click **Browse** and select the saved profile (XML file) from the local disk. The following example shows a customized install file.

```
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <FAConfiguration>
 <Install>
 <WindowsConnectorLocation>
https://fa_webserver/ACFA_Mac_FireAMPSetup.exe
</WindowsConnectorLocation>
 <MacConnectorLocation>
https://fa_webserver/ACFA_Mac_FireAMPSetup.exe
</MacConnectorLocation>
 <StartMenu>true</StartMenu>
 <DesktopIcon>false</DesktopIcon>
 <ContextIcon>true</ContextIcon>
 </Install>
 </FAConfiguration>
</FAProfile>
```

The following example shows a customized uninstall file.

```
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <FAConfiguration>
 <Uninstall>
 </Uninstall>
 </FAConfiguration>
</FAProfile>
```

Step 8 Click **Submit**.
The newly created AMP Enabler profile is displayed in the **Resources** page.

Troubleshoot Common AMP Enabler Installation Errors

When you enter the SOURCEfire URL in the Windows or MAC Installer text box and click **Check**, you might encounter any of the following errors:

- Error Message: The certificate for the server containing the Mac/Windows installer file is not trusted by ISE. Add a trust certificate to **Administration** > **Certificates** > **Trusted Certificates**.

  This error message appears if you have not imported the SOURCEfire trusted certificate in to the Cisco ISE certificate store. Obtain a SOURCEfire trusted certificate and import it in to the Cisco ISE trusted certificate store (Administration > Certificates > Trusted Certificates).

- Error Message: The installer file is not found at this location, this may be due to a connection issue. Enter a valid path in the Installer text box or check your connection.

  This error message appears when the server hosting the AMP for Endpoint software is down or if there is a typographic error in the Windows Installer or MAC Installer text box.

- Error Message: The Windows/Mac installer text box does not contain a valid URL.

  This error message appears when you enter a syntactically incorrect URL format.

Cisco ISE Support for Onboarding Chromebook Devices

Chromebook devices are managed devices (managed by the Google domain), unlike other devices (Apple, Windows, Android) and have limited onboarding support. Cisco ISE supports the onboarding of Chromebook devices on a network. Onboarding refers to the process of delivering the required settings and files to an endpoint such that it is able to connect securely to a network after authenticating with Cisco ISE. This process includes certificate provisioning and/or native supplicant provisioning. However, in Chromebook devices, you can only perform certificate provisioning. Native supplicant provisioning is done via the Google Admin Console.

Unmanaged Chromebook devices cannot be onboarded to a secure network.

The entities involved in the Chromebook onboarding process are the:

- Google Administrator
- ISE Administrator
- Chromebook User/Device
- Google Admin Console (Managed by the Google Administrator)

The Google administrator:

- Secures the following licenses:
  1. Google Apps Administrator license for the Google Admin Console configuration—URL: https://admin.google.com. The Google Admin Console enables an administrator to manage Google services for people in an organization.
  2. Chromebook device management license—URL: https://support.google.com/chrome/a/answer/2717664?hl=en. A Chromebook device management license is used to configure settings and enforce policies for a specific Chromebook device. It gives

the Google Administrator access to device settings to control user access, customize features, configure network access, and more.

- Facilitates provisioning and enrolling of Chromebook devices with a Google device license.
- Manages Chromebook devices through the Google Admin Console.
- Sets up and manages the Wi-Fi network configuration for each Chromebook user.
- Manages the Chromebook devices by configuring applications and forced extensions to be installed on the Chromebook device. Onboarding the Chromebook device requires the Cisco Network Setup Assistant extensions to be installed in the Chromebook device. This allows the Chromebook device to connect to Cisco ISE and install the ISE certificate. The extension is forcibly installed because the action of certificate installation is allowed only for managed devices.
- Ensures that the Cisco ISE certificates are installed in the Google Admin Console to provide server validation and secure connection. The Google administrator decides whether a certificate should be generated for a device or a user. Cisco ISE provides options to:
    - Generate the certificate for a single user who does not share the Chromebook device.
    - Generate a certificate for a Chromebook device that is shared by multiple users. Refer to Step 5 in the Configure the Network and Force Extensions in the Google Admin Console section for the required additional configuration.

  The Google Administrator installs the ISE server certificate so that ISE is trusted to perform the certificate provisioning on the Chromebook device and also to allow EAP-TLS certificate-based authentication. Google Chrome version 37 and higher supports certificate-based authentication for Chromebook devices. The google administrator needs to load the ISE provisioning application in the Google Admin Console and make it available to the Chromebook devices to get the certificate from ISE.

- Ensures that the recommended Google host names are allowed in the ACL definition list configured in the WLC for SSL secure connections. Refer to the recommended and allowed host names in the Google Support page.

The ISE Administrator:

- Defines the native supplicant profile for the Chromebook OS that includes the certificate template structure.
- Creates the necessary authorization rules and client provisioning policies in Cisco ISE for Chromebook users.

The Chromebook User:

- Wipes out the Chromebook device and enrolls it to the Google domain to secure the enforced policy that was defined by the Google administrator.
- Receives the Chromebook device polices and the Cisco Network Setup Assistant forced extension installed by the Google Admin Console.
- Connects to the provisioned SSID, as defined by the Google administrator, opens the browser, displays the BYOD pages, and starts the onboarding process.
- The Cisco Network Setup Assistant installs a client certificate in the Chromebook device, which allows the device to perform EAP-TLS certificate-based authentication.

The Google Admin Console:

The Google Admin Console supports Chromebook device management and allows configuring a secure network and pushing Cisco Network Setup Assistant certificate management extensions to the Chromebook. The extension sends an SCEP request to Cisco ISE and installs the client certificate to allow secure connection and access to the network.

Best Practices for Using Chromebook Device in a Shared Environment

When a Chromebook device is used in a shared environment, such as schools and libraries, the Chromebook device is shared by different users. Some of the best practices that Cisco recommends include:

- When onboarding a Chromebook device with a specific user (student or professor) name, the user's name will be populated in the Common Name (CN) in the Subject field of the certificate. Also, the shared Chromebook is listed in the My Devices portal under that specific user. Therefore, it is recommended for shared devices to use a shared credential when onboarding, so that devices show up only under the specific user’s My Devices portal listing. The shared account can be administered by the administrator or professor as a separate account to control shared devices.
- The Cisco ISE administrator can create a custom certificate template for shared Chromebook devices and use it in the policy. For example, instead of using the standard certificate template that matches the Subject-Common Name (CN) value, you can specify a Name (for example, chrome-shared-grp1) in the certificate and the same name can be assigned to the Chromebook device. A policy can be designed to match the name to allow or deny access to a Chromebook device.
- The Cisco ISE administrator can create an endpoint group with all the Chromebook devices’ MAC addresses that needs to go through Chromebook onboarding (devices for which access need to be restricted). The authorization rule should call this out along with device type Chromebook—this would allow access to be redirected to the NSP.

Chromebook Onboarding Process

The Chromebook onboarding process involves a series of steps:

Step 1 Configure the Network and Force Extensions in the Google Admin Console .

Step 2 Configure Cisco ISE for Chromebook Onboarding.

Step 3 Wipe a Chromebook Device.

Step 4 Enroll Chromebook to the Google Admin Console.

Step 5 Connect Chromebook to the Cisco ISE Network for BYOD On Boarding.

Configure the Network and Force Extensions in the Google Admin Console

The Google administrator performs the following steps.

Step 1 Log in to the Google Admin Console.

a) Enter the following URL: https://admin.google.com in the browser.

b) Enter the required username and password.

c) In the **Welcome to Admin Console** window, click **Device Management**.
d) On the **Device Management** window, click **Network**.

Step 2 Set up the Wi-Fi network for managed devices.

a) In the **Networks** window, click **Wi-Fi**.
b) Click **Add Wi-Fi** to add the required SSIDs. See Google Admin Console - Wi-Fi Network Settings for more information.

   For MAB flows, create two SSIDs, one for the open network, and the other for certificate authentication. When you connect to the open network, Cisco ISE ACLs redirect you to the credentialed guest portal for authentication. After successful authentication, ACLs redirect you to the BYOD portal.

   If the ISE certificate is issued by an intermediate CA, then you must map the intermediate certificate to the "Server certificate authority", instead of to the Root CA.

c) Click **Add**.

Step 3 Create the forced extensions.

a) In the **Device Management** window, under the **Device Settings** , click **Chrome Management**.
b) Click **User Settings**.
c) Scroll down, and in the **Apps and Extensions** section, in the **Force-Installed Apps and Extensions** option, click **Manage Force-Installed Apps**.

Step 4 Install the forced extensions.

a) In the **Force-Installed Apps and Extensions** window, click **Chrome Web Store**.
b) In the **Search** text box, type "Cisco Network Setup Assistant" to locate the extension.

   The forced Cisco Network Setup Assistant extension of the Chromebook device requests the certificate from Cisco ISE, and installs the ISE certificate on the Chromebook device. The extension must be configured as force-installed because certificate installation is only allowed for managed devices. If the extension was not installed during the enrollment process, the Cisco ISE certificate cannot be installed.

c) Click **Add** to force install apps.
d) Click **Save**.

Step 5 (Optional) Define the configuration file to install a certificate in a Chromebook device which is shared by multiple users.

a) Copy and paste the following code in a Notepad file and save it to your local disk.

```
{
  "certType": {
    "Value": "system"
  }
}
```

b) Choose **Device Management** > **Chromebook Management** > **App Management**.
c) Click the **Cisco Network Setup Assistant** extension.
d) Click **User Settings** and choose your domain.
e) Click **Upload Configuration File** and choose the .txt file that you saved in your local disk.

   Note In order for the Cisco Network Setup Assistant to create a certificate for a device that is shared by multiple users, you must add the Notepad file in the Google Admin Console. Otherwise, the Cisco NSA creates a certificate for a single user.

f) Click **Save**.

Step 6 (Optional) Install a certificate for a single user who does not share the Chromebook.

a) Choose **Device Management** > **Network** > **Certificates**.
b) In the **Certificates** window, click **Add Certificate** and upload the Cisco ISE certificate file.

What to do next

Configure Cisco ISE for Chromebook on board.

Configure Cisco ISE for Chromebook Onboarding

Before you begin

The Cisco ISE administrator must create the required policy. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Sets** window.

Given below is an example of an authorization policy:

Rule Name: Full_Access_After_Onboarding, Conditions: If RegisteredDevices AND Wireless_802.1x AND Endpoints:BYODRegistration EQUALS Yes AND Certificate: Subject Alternative Name Equals RadiusCalling-Station-ID AND Network Access: EAP-Authentication EQUALS EAP-TLS Then CompliantNetworkAccess.

The CompliantNetworkAccess is an authorization result that is configured. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles** window.

Step 1 Configure the Native Supplicant Profile (NSP) on Cisco ISE.

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

   The Chromebook device is displayed in the Client Provisioning page for a fresh Cisco ISE installation. However, for upgrade, you should download posture updates. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration > System > Settings > Posture > Updates** window.

b) Click **Add** > **Native Supplicant Profile**.
c) Enter the **Name** and **Description**.
d) In the **Operating System** field, choose **Chrome OS All**.
e) In the **Certificate Template** field, select the required certificate template.
f) Click **Submit**. Observe that the SSID is provisioned via the Google Admin Console and not through the native supplicant provisioning flow.

Step 2 Map the NSP in the Client Provisioning page.

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Client Provisioning**.
b) Define the result.

   - Choose the in-built Native Supplicant configuration (Cisco-ISE-Chrome-NSP) in the **Results** of the client provisioning policy.

- Or, create a new rule and ensure to choose the **Result** created for the Chromebook device.

Wipe a Chromebook Device

The Chromebook device must be wiped after the Google Admin Console is configured by the Google Administrator. The Chromebook user must wipe the device, which is a one-time process, to force extensions and configure the network settings. You can refer to the following URL: https://support.google.com/chrome/a/answer/1360642 for further information.

The Chromebook user performs the following steps:

Step 1 Press **Esc-Refresh-Power** key combination. The screen displays a yellow exclamation point (!).

Step 2 Press **Ctrl -D** key combination to begin dev mode, then press **Enter** key. The screen displays a red exclamation point.

Step 3 Press **Ctrl -D** key combination. The Chromebook deletes its local data, returning to its initial state. The deletion takes approximately 15 minutes.

Step 4 When the transition completes, press the **Spacebar** key, then press the **Enter** key to return to verified mode.

Step 5 Enroll the Chromebook before signing in.

What to do next

Enroll Chromebook to the Google Admin Console.

Enroll Chromebook to the Google Admin Console

In order to provision a Chromebook device, the Chromebook user must first enroll in the Google Admin Console page and receive device policies and forced extensions.

Step 1 Turn on the Chromebook device and follow the onscreen instructions until you see the sign on screen. Do not sign in yet.

Step 2 Before signing in to the Chromebook device, press **Ctrl-Alt-E** key combination. The **Enterprise Enrolment** screen appears.

Step 3 Enter your email address and click **Next**.
You will receive the following message: Your device has successfully been enrolled for enterprise management.

Step 4 Click **Done**.

Step 5 Enter the username and password from your Google admin welcome letter, or the username and password for an existing Google Apps user on your account that has eligibility to enroll.

Step 6 Click **Enroll Device**. You will receive a confirmation message that the device has been successfully enrolled.

Note that the Chromebook enrollment is a one-time process.

Connect Chromebook to the Cisco ISE Network for BYOD On Boarding

The procedure is for Dual SSID—To connect to a 802.x network using the EAP-TLS protocol, the Chromebook user performs the following steps:

Note If you are using Dual SSID—When connecting from 802.x PEAP to an EAP-TLS network, connect to the network by entering your credentials in the network supplicant, not the web browser.

Step 1 In the Chromebook, click **Settings**.

Step 2 In the **Internet Connection** section, click **Provisioning Wi-Fi Network**, and then click your network.

Step 3 The credentialed guest portal opens.

a. On the Sign On page, enter the **Username** and **Password**.

b. Click **Sign-on**.

Step 4 In the BYOD Welcome page, click **Start**.

Step 5 In the **Device Information** field, enter a name and a description for your device. For example, "Personal Devices: Jane's Chromebook Used for School or Shared Devices: Library Chromebook #1 or Classroom 1 Chromebook #1".

Step 6 Click **Continue**.

Step 7 Click **Yes** in the **Cisco Network Setup Assistant** dialog box to install the certificate to access the secure network.

If the Google Administrator configured secure Wi-Fi, the network connection should happen automatically. If it does not, choose the secure SSID from the list of available networks.

Chromebook users who have already enrolled in the domain, and have the Cisco Network Setup Assistant extension, can update the extension without waiting for the auto update. Manually update the extension by performing the following steps.

a. In your Chromebook, open the browser and enter the following **URL: chrome://Extensions**.

b. Check the **Developer Mode** check box.

c. Click **Update Extensions Now**.

d. Verify that the Cisco Network Setup Assistant extension version is 2.1.0.35 and higher.

Google Admin Console - Wi-Fi Network Settings

The Wi-Fi network configuration is used to configure an SSID in a customer network or to match the certificate using certificate attributes (for EAP-TLS). When the certificate is installed in the Chromebook, it is synchronized with the Google admin settings. Connection is established only when one of the defined certificate attributes matches the SSID configuration.

Listed below are the mandatory fields, specific to EAP-TLS, PEAP, and Open network flows, which the Google administrator configures to set up the Wi-Fi network in the Google Admin Console page (**Device Management** > **Network** > **Wi-Fi** > **Add Wi-Fi**) for each Chromebook user.

Field	EAP-TLS	PEAP	Open
Name	Enter the name of the network connection.	Enter the name of the network connection.	Enter the name of the network connection.
Service Set Identifier (SSID)	Enter the SSID (for example, tls_ssid).	Enter the SSID (for example, tls_ssid).	Enter the SSID (for example, tls_ssid).
This SSID Is Not Broadcast	Select the option.	Select the option.	Select the option.
Automatically Connect	Select the option.	Select the option.	Select the option.
Security Type	WPA/WPA2 Enterprise (802.1x)	WPA/WPA2 Enterprise (802.1x)	Open
Extensible Authentication Protocol	EAP-TLS	PEAP	—
Inner Protocol	—	• Automatic • MSCHAP v2 (Select the option) • MD5 • PAP • MSCHAP • GTC	—
Outer Identity	—	—	—
Username	Optional, either set a fixed value or use variables from the user login: ${LOGIN_ ID} or ${LOGIN_EMAIL}.	Enter the PEAP credentials to authenticate against ISE (internal ISE user/AD/other ISE identities) and the Password field.	—
Server Certificate Authority	Select the ISE certificate (imported from Device Management > Network > Certificates).	Select the ISE certificate (imported from Device Management > Network > Certificates).	—
Restrict Access to this Wi-Fi Network by Platform	• Select Mobile Devices. • Select Chromebooks.	• Select Mobile Devices. • Select Chromebooks.	—

Field	EAP-TLS	PEAP	Open
Client Enrollment URL	Enter a URL to which the Chromebook device browser is redirected for users who are not enrolled. Configure ACLs on the Wireless LAN Controller for redirecting unenrolled users.	—	—
Issuer Pattern	An attribute in the certificate. Select at least one attribute from either the Issuer Pattern or Subject Pattern that should match installed certificate attributes. Specify certificate attributes that will be matched with the Chromebook device to accept the certificate. • Common Name: Refers to the Subject field of the certificate or the wildcard domain in the Subject field of the certificate, which must match the FQDN of the node. • Locality: Refers to the test locality (City) that is associated with the certificate subject. • Organization: Refers to the organization name that is associated with the certificate subject. • Organizational Unit: Refers to the organizational unit name that is associated with the certificate subject.	—	—

Field	EAP-TLS	PEAP	Open
Subject Pattern	An attribute in the certificate. Select at least one attribute from either the Issuer Pattern or Subject Pattern that should match installed certificate attributes. Specify certificate attributes that will be matched with the Chromebook device to accept the certificate. • Common Name: Refers to the Subject field of the certificate or the wildcard domain in the Subject field of the certificate, which must match the FQDN of the node. • Locality: Refers to the test locality (City) that is associated with the certificate subject. • Organization: Refers to the organization name that is associated with the certificate subject. • Organizational Unit: Refers to the organizational unit name that is associated with the certificate subject.	—	—
Proxy Settings	• Direct Internet Connection (Selected) • Manual Proxy Configuration • Automatic Proxy Configuration	• Direct Internet Connection (Selected) • Manual Proxy Configuration • Automatic Proxy Configuration	—

Field	EAP-TLS	PEAP	Open
Apply Network	By User	By User	—

Monitor Chromebook Device Activities in Cisco ISE

Cisco ISE provides various reports and logs to view information related to the authentication and authorization of Chromebook devices. You can run these reports either on demand or on regular basis. You can view the authentication method (for example, 802.1x) and authentication protocol (for example, EAP-TLS). In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **RADIUS** > **Live Logs** window. You can also identify the number of end points that are classified as Chromebook devices. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Identities** > **Endpoints** window.

Troubleshoot Chromebook Device Onboarding

This section describes problems that you may encounter while onboarding your Chromebook device.

- Error: Unable to install the extension from the webstore—You cannot install the extension from the webstore. It will be automatically installed on your Chromebook device by the network administrator.
- Error: Completed the installation of the certificate, however, unable to connect to the secure network—Verify on the Admin Console that the installed certificate matches defined Issuer/Subject attribute pattern. You can get information about installed certificate from: chrome://settings/certificates
- Error: Displays an error message "Obtain Network Certificate", when trying to manually connect to the secure network on the Chromebook—Click Get New Certificate, the browser opens and redirects you to the ISE BYOD flow to install the certificate. However, if you are unable to connect to the secure network, verify on the Admin Console that the installed certificate matches the defined Issuer/Subject attribute pattern.
- Error: Clicked Get New Certificate but is forwarded to the www.cisco.com site—User needs to be connected to the provisioning SSID, in order to be redirected to ISE and commence the certificate installation process. Be sure that the correct access list is defined for this network.
- Error: Displays an error message "Only managed devices can use this extension. Contact helpdesk or network administrator"—Chromebook is a managed device and the extension must be configured as a forced install to gain access to the Chrome OS APIs to install the certificate on the device. Although, the extension can be installed manually by downloading it from the Google web store, an unenrolled Chromebook user cannot install the certificate.

  An unenrolled Chromebook device can secure a certificate if the user belongs to the Domain Users group. The extension tracks the domain user on any device. However, the domain user can produce user-based authentication keys for an unenrolled device.
- Error: Unclear of the order in which SSIDs are connected in the Google Admin Console—
  - If several SSIDs (PEAP and EAP-TLS) are configured on the Google Admin Console, after the certificate is installed and the attributes are matched, the Chrome OS automatically connects to the SSID with certificate-based authentication regardless of the order in which the SSIDs are configured.
  - If two EAP-TLS SSIDs match the same attribute, the connection depends on other factors such as signal strength and other network level signals, which cannot be controlled by the user or admin.

- If multiple EAP-TLS certificates are installed on the Chromebook device and all of them match the certificate pattern configured on the Admin Console, the newest certificate will be used for the connection.

Cisco AnyConnect Secure Mobility

Cisco ISE uses an integrated module in Cisco AnyConnect for Cisco ISE posture requirements.

Note AnyConnect does not support CWA flow. You can't provision AnyConnect from the Guest portal using the **Require guest device compliance** field in the **Work CentersGuest Access** > **Portals & Components** > **Guest Portals** > **Create, Edit, or Duplicate** > **Portal Behavior and Flow Settings** > **Guest Device Compliance Settings** window. Instead, provision AnyConnect on the Client Provisioning portal. This method results in redirection as configured in authorization permissions.

When you integrate Cisco ISE with the Cisco AnyConnect agent, Cisco ISE:

- Serves as a staging server to deploy Cisco AnyConnect Version 4.0 and future releases
- Interacts with the AnyConnect posture component for Cisco ISE posture requirements
- Supports deployment of Cisco AnyConnect profiles, customization and language packages, and OPSWAT library updates for Windows and Mac OS X operating systems
- Supports Cisco AnyConnect and legacy agents at the same time

Note When switching network mediums, you must change the default gateway so the posture module can detect the changed network and reassess the client.

Create AnyConnect Configuration

AnyConnect configuration includes AnyConnect software and its associated configuration files. This configuration can be used in the client provisioning policy that allows users to download and install AnyConnect resources on the clients. If you use both ISE and an ASA to deploy AnyConnect, then the configurations must match on both headends.

To push the ISE posture module when connected to a VPN, Cisco recommends that you install the AnyConnect agent through Cisco Adaptive Security Appliance (ASA), which uses the Cisco's Adaptive Security Device Manager (ASDM) GUI tool. ASA does the installation using the VPN downloader. With the download, the ISE posture profile is pushed via ASA, and the discovery host needed for later provisioning the profile is available before the ISE posture module contacts ISE. Whereas with ISE, the ISE posture module will get the profile only after ISE is discovered, which could result in errors. Therefore, ASA is recommended to push the ISE posture module when connected to a VPN.

Note When Cisco ISE is integrated with ASA, ensure that the Accounting mode is set to **Single** in ASA. Accounting data is sent to only one accounting server in Single mode.

Before you begin

Before configuring an AnyConnect configuration object, you must:

1. Download the AnyConnect Headend Deployment package and compliance module from Cisco Software download page.
2. Upload these resources to Cisco ISE (see Add Cisco Provided Client Provisioning Resources from a Local Machine, on page 1219).
3. (Optional) Add the customization and localization bundles (see Add Customer Created Resources for AnyConnect from a Local Machine, on page 1220).
4. Configure an AnyConnect posture agent profile (see Create a Posture Agent Profile, on page 1240).

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provision** > **Resources**.

Step 2 Click **Add** to create an AnyConnect configuration.

Step 3 Choose **AnyConnect Configuration**.

Step 4 Choose an AnyConnect Package, which you previously uploaded. For example, AnyConnect DesktopWindows xxx.x.xxxxx.x .

Step 5 Enter the name for the current AnyConnect Configuration. For example, AC Config xxx.x.xxxxx.x.

Step 6 Choose the compliance module, which you previously uploaded. For example, AnyConnect ComplianceModulewindows x.x.xxxx.x.

Step 7 Check one or more AnyConnect module check boxes. For example, choose one or more modules from the following: ISE Posture, VPN, Network Access Manager, Web Security, AMP Enabler, ASA Posture, Start Before Log on (only for Windows OS), and Diagnostic and Reporting Tool.

Note Un-checking the VPN module under AnyConnect Module Selection does not disable the VPN tile in the provisioned client. You must configure VPNDisable_ServiceProfile.xml to disable the VPN tile on AnyConnect GUI. In a system where AnyConnect is installed at the default location, you can find this file under C:\Program Files\Cisco. If AnyConnect is installed at a different location, then the file will be available under <AnyConnect Installed path>\Cisco.

Step 8 Choose AnyConnect profiles for selected AnyConnect modules. For example, ISE Posture, VPN, NAM, and Web Security.

Step 9 Choose AnyConnect customization and localization bundles.

Step 10 Click **Submit**.

Create a Posture Agent Profile

Use this procedure to create an AnyConnect posture agent profile, where you can specify parameters that define the agent behavior for the posture protocol.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Step 2 Click **Add**.

Step 3 Choose **AnyConnect Posture Profile**.

Step 4 Enter **Name** of the profile.

Step 5 Configure parameters for the following:

- Cisco ISE posture agent behavior
- Client IP Address Changes
- Cisco ISE posture protocol

Step 6 Click **Submit**.

Client IP Address Refresh Configuration

The following table describes the fields in the NAC AnyConnect Posture Profile window, which allows you to configure parameters for the client to renew or refresh its IP address after VLAN change. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Resilts** > **Client Provisioning** > **Resources** > **Add** > **AnyConnect Posture Profile**.

Field Name	Default Value	Usage Guidelines
VLAN detection interval	0, 5	This setting is the interval at which the agent check for the VLAN change. For the Mac OS X agent, the default value is 5. By default, the access to authentication VLAN change feature is enabled with VlanDetectInteval as 5 seconds for Mac OS X. The valid range is 5 to 900 seconds. 0 —Access to Authentication VLAN change feature is disabled. 1 to 5—Agent sends an Internet Control Message Protocol (ICMP) or Address Resolution Protocol (ARP) query every 5 seconds. 6 to 900—An ICMP or ARP query is sent every x seconds.

Field Name	Default Value	Usage Guidelines
Enable VLAN detection without UI (Not applicable for a Mac OS X client)	No	This setting enables or disables VLAN detection even when the user is not logged in. No—VLAN detect feature is disabled. Yes—VLAN detect feature is enabled.
Retry detection count	3	If the Internet Control Message Protocol (ICMP) or Address Resolution Protocol (ARP) polling fails, this setting configures the agent to retry x times before refreshing the client IP address.
Ping or ARP	0 The valid range is 0 to 2.	This setting specifies the method used for detecting the client IP address change. 0—Poll using ICMP 1—Poll using ARP 2—Poll using ICMP first, then (if ICMP fails) ARP
Maximum timeout for ping	1 The valid range is 1 to 10 seconds.	Poll using ICMP, and if there is no response within the specified time, then declare an ICMP polling failure.
Enable agent IP refresh	Yes (Default)	This setting specifies whether or not the client machine to renew or refresh its IP address after the switch (or WLC) changes the VLAN for the login session of the client on the respective switch port.
DHCP renew delay	0 The valid range is 0 to 60 seconds.	This setting specifies that the client machine waits before attempting to request for a new IP address from the network DHCP server.
DHCP release delay	0 The valid range is 0 to 60 seconds.	The setting specifies that the client machine waits before releasing its current IP address.

Note Merge parameter values with existing agent profile settings or overwrite them to appropriately configure clients on Windows and Mac OS X clients for refreshing IP addresses.

Posture Protocol Settings

The following table describes the fields in the AnyConnect Posture Profile window, which allows you to configure posture protocol settings for AnyConnect. For more information, see the Cisco AnyConnect Secure Mobility Client Administrator Guide for your version of AnyConnect.

Field Name	Default Value	Usage Guidelines
PRA Retransmission Time	120 seconds	This is the agent retry period if there is a Passive Reassessment communication failure.
Retransmission Delay	60 seconds	Time (in seconds) to wait before retrying.
Retransmission Limit	4	Number of retries allowed for a message.
Discovery Host	—	Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that HTTP traffic to the Client Provisioning portal.
Discovery Backup Server List	—	Choose the PSNs from the drop-down list. AnyConnect probes this server list to find the PSN node on which posture must be performed. If you don't select any PSN, all the PSNs in the node group or cluster are sent to AnyConnect as the backup server list.
Server Name Rules	—	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to.
Call Home List	—	Enter a comma-separated list of IP addresses and ports with colon in between the IP address and the port.
Back-off Timer	30 sec	This setting enables the AnyConnect agent to continuously to reach the discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this maximum time limit is reached. The valid range is from 10 to 600 seconds.

Continuous Endpoint Attribute Monitoring

You can use the AnyConnect agent to continuously monitor different endpoint attributes to improve the overall visibility of an endpoint. The AnyConnect agent monitors applications that are installed and running on an endpoint. You can turn on and off the feature and configure how often the data should be monitored. By default, data is collected every 5 minutes and is stored in the database. During initial posture, AnyConnect reports a complete list of running and installed applications. After initial posture, the AnyConnect agent scans the applications every X minutes and sends the differences from the last scan to the server. The server displays the complete list of running and installed applications.

Posture State Synchronization

Sometimes, Cisco ISE might move a client or an endpoint to Pending state because of a change in network configuration. However, AnyConnect cannot detect this change, and retains the client or endpoint in Compliant state. Thus, there is a mismatch in posture status and ideally, Cisco ISE must be probed in this scenario to obtain the correct posture status. You can do this by configuring AnyConnect to probe Cisco ISE at specified intervals so that when the posture status of a client or endpoint is pending, this probing will prevent the client or endpoint from being stuck in Pending state in Cisco ISE.

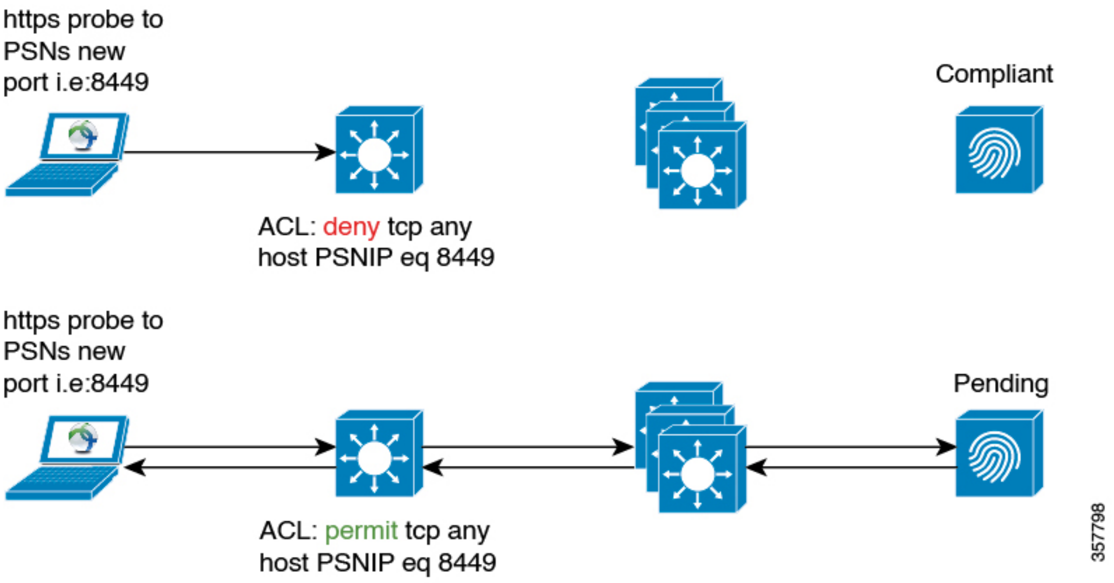
The posture state synchronization is supported for Windows, Linux, and MacOS clients.

The posture state synchronization includes the following steps:

1. The client tries to connect to the network.
2. The PSN performs the posture flow. The endpoint is moved to Compliant state if the client is compliant with the posture policies.
3. The AnyConnect agent receives Posture Probing Backup List and Posture State Synchronization Interval configuration details from Cisco ISE.
4. The AnyConnect agent starts probing Cisco ISE, at specified intervals.

   For example, Cisco ISE shows the posture status as pending and AnyConnect shows the posture status as Compliant. When AnyConnect probes Cisco ISE and learns the new state, a reassesment could be triggered.

Figure 64: Posture State Synchronization



Note If the status of a client has moved to **Pending** for whatever reason, the AnyConnect agent will receive a probing request from the client. It will probe and receive the correct client state from Cisco ISE and then move the client to the correct state.

Configure Posture State Synchronization

Step 1 Configure **Posture Probing Backup List** and **Posture State Synchronization Interval** in the **AnyConnect Posture Profile**. To do this:

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

b) From the **Add** drop-down list, choose **AnyConnect Posture Profile**.

c) In the **Agent Behavior** area, configure the following settings:

- **Posture Probing Backup List**: From this drop-down list, choose the PSNs that AnyConnect must probe for endpoint posture compliance status. You can choose up to six PSNs.

  AnyConnect sends probes to these PSNs to check whether the posture compliance status for an endpoint is still valid. If you don't choose any PSN, the connected PSN and any two backup servers are used as backups for posture state synchronization.

- **Posture State Synchronization Interval**: Define the frequency at which AnyConnect synchronizes the posture status with Cisco ISE. The valid range is from 0 to 300. If you enter 0, posture state synchronization probing is disabled. The posture state synchronization port must be blocked for compliant authorization profiles when this value is greater than 0.

Step 2 Configure port 8449 for bidirectional communication. To do this:

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Client Provisioning Portals** > **Portal Behavior and Flow Settings**.

b) Click **Portal Settings**.

c) In the **Bidirectional Port** field, ensure that port 8449 is set for bidirectional communication.

By default, port 8449 is used for bidirectional communication.

Step 3 Configure an ACL to block posture state synchronization probe from reaching Cisco ISE when the client posture status is compliant. To do this:

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Downloadable ACLs**.

b) Configure the ACL.

Ensure that only the clients in Pending state are allowed to reach the configured PSNs over the bidirectional port. This will avoid unwanted traffic from clients that are in Compliant state. The following is an example of ACL:

```
deny tcp any host <ip address> eq 8449
deny tcp any host <ip address> eq 8449
deny tcp any host <ip address> eq 8449
permit ip any any
```

If ACL is not configured, the Posture Configuration Detection alarm is triggered on the Cisco ISE dashboard. ACL should only be configured on policy sets that are complaint. The main purpose of this alarm is to prevent heavy traffic to Cisco ISE.

Note Ensure that the firewall does not block the communication on the corresponding port when a client is in Pending state.

Cisco Web Agent

The Cisco Web Agent provides temporal posture assessment for client machines.

Users can launch the Cisco Web Agent executable, which installs the Web Agent files in a temporary directory on the client machine via ActiveX control or Java applet.

After users log in to the Cisco Web Agent, the Web Agent gets the requirements that are configured for the user role and the operating system from the Cisco ISE server, checks the host registry, processes, applications, and services for required packages and sends a report back to the Cisco ISE server. If requirements are met on the client machine, the user is allowed network access. If requirements are not met, the Web Agent presents a dialog to the user for each requirement that is not satisfied. The dialog provides the user with instructions and the action to take for the client machine to meet the requirement. Alternatively, if the specified requirements are not met, users can choose to accept the restricted network access while they try to remediate the client system so that it meets requirements for the user login role.

Note ActiveX is supported only on the 32-bit versions of Internet Explorer. You cannot install ActiveX on a Firefox web browser or on a 64-bit version of Internet Explorer.

Configure Client Provisioning Resource Policies

For clients, the client provisioning resource policies determine which users receive which version of resources (agents, agent compliance modules, and agent customization packages or profiles) from Cisco ISE upon login and user session initiation.

For AnyConnect, resources can be selected from the **Client Provisioning Resources** window to create an AnyConnect configuration that you can use in the **Client Provisioning Policy** window. AnyConnect configuration specifies the AnyConnect software and its association with different configuration files that includes AnyConnect binary package for Windows, macOS, and Linux clients, compliance module, module profiles, customization, and language packages.

Before you begin

- Before you can create effective client-provisioning resource policies, ensure that you have added resources to Cisco ISE. When you download the agent compliance module, it always overwrites the existing one, if any, available in the system.

- Check the native supplicant profile that is used in the client provisioning policy and ensure that the wireless SSID is correct. For iOS devices, if the network that you are trying to connect is hidden, check the **Enable if target network is hidden** check box in the **iOS Settings** area.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Client Provisioning**.

Step 2 From the **Behavior** drop-down list, choose one of the following options:

- **Enable**: Ensures Cisco ISE uses this policy to help fulfill client-provisioning functions when users log in to the network and conform to the client-provisioning policy guidelines.
- **Disable**: Cisco ISE does not use the specified resource policy to fulfill client-provisioning functions.
- **Monitor**: Disables the policy and “watches” the client-provisioning session requests to see how many times Cisco ISE tries to invoke based on the “Monitored” policy.

Step 3 Enter a name for the new resource policy in the **Rule Name** text box.

Step 4 Specify one or more Identity Groups to which a user who logs into Cisco ISE might belong.

You can choose to specify the **Any** identity group type, or choose one or more groups from a list of existing Identity Groups that you have configured.

Step 5 Use the **Operating Systems** field to specify one or more operating systems that might be running on the client machine or device through which the user is logging into Cisco ISE.

Note Though the option to select macOS 10.6, 10.7, and 10.8 is available in the **Client Provisioning** window in Cisco ISE GUI, these versions are not supported by AnyConnect.

Step 6 In the **Other Conditions** field, specify a new expression that you want to create for this particular resource policy.

Step 7 For client machines, use the **Agent Configuration** option to specify which agent type, compliance module, agent customization package, and profile to make available and provision on the client machine.

It is mandatory to include the client provisioning URL in authorization policy to enable the agent to popup in the client machines. This prevents request from any random clients and ensures that only clients with proper redirect URL can request for posture assessment.

Step 8 Click **Save**.

What to do next

After you have successfully configured one or more client provisioning resource policies, you can start to configure Cisco ISE to perform posture assessment on client machines during login.

Configure Cisco ISE Posture Agent in the Client Provisioning Policy

For client machines, configure the agent type, compliance module, agent customization package, and/or profile to make available and provision for users to download and install on the client machine.

Before you begin

You must add client provisioning resources for AnyConnect in Cisco ISE.

Step 1 Choose an available agent from the **Agent** drop-down list and specify whether the agent upgrade (download) defined here is mandatory for the client machine by enabling or disabling the **Is Upgrade Mandatory** option, as appropriate.

The **Is Upgrade Mandatory** setting only applies to agent downloads. Agent profile, compliance module, and agent customization package updates are always mandatory.

Step 2 Choose an existing agent profile from the **Profile** drop-down list.

Step 3 Choose an available compliance module to download to the client machine using the **Compliance Module** drop-down list.

Step 4 Choose an available agent customization package for the client machine from the **Agent Customization Package** drop-down list.

Configure Native Supplicants for Personal Devices

Employees can connect their personal devices to the network directly using native supplicants, which are available for Windows, Mac OS, iOS, and Android devices. For personal devices, specify which Native Supplicant configuration to make available and provision on the registered personal device.

Before you begin

Create native supplicant profiles so that when user log in, based on the profile that you associate with that users authorization requirements, Cisco ISE provides the necessary supplicant provisioning wizard to set up the users personal devices to access the network.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose Choose **Policy** > **Client Provisioning**.

Step 2 Choose **Enable**, **Disable**, or **Monitor** from the behavior drop-down list.

Step 3 Enter a name for the new resource policy in the Rule Name text box.

Step 4 Specify the following:

- Use the **Identity Groups** field to specify one or more Identity Groups to which a user who logs into Cisco ISE might belong.
- Use the **Operating System** field to specify one or more operating systems that might be running on the personal device through which the user is logging into Cisco ISE.
- Use the **Other Conditions** field to specify a new expression that you want to create for this particular resource policy.

Step 5 For personal devices, use **Native Supplicant Configuration** to choose the specific **Configuration Wizard** to distribute to these personal devices.

Step 6 Specify the applicable **Wizard Profile** for the given personal device type.

Step 7 Click **Save**.

Client Provisioning Reports

You can access the Cisco ISE monitoring and troubleshooting functions to check on overall trends for successful or unsuccessful user login sessions, gather statistics about the number and types of client machines logging into the network during a specified time period, or check on any recent configuration changes in client provisioning resources.

Client Provisioning Requests

The **Operations** > **Reports** > **ISE Reports** > **Endpoints and Users** > **Client Provisioning** report displays statistics about successful and unsuccessful client provisioning requests. When you choose **Run** and specify one of the preset time periods, Cisco ISE combs the database and displays the resulting client provisioning data.

Supplicant Provisioning Requests

The **Operations** > **Reports** > **ISE Reports** > **Endpoints and Users** > **Supplicant Provisioning** window displays information about recent successful and unsuccessful user device registration and supplicant provisioning requests. When you choose **Run** and specify one of the preset time periods, Cisco ISE combs the database and displays the resulting supplicant provisioning data.

The Supplicant Provisioning report provides information about a list of endpoints that are registered through the device registration portal for a specific period of time, including data like the Logged at Date and Time, Identity (user ID), IP Address, MAC Address (endpoint ID), Server, profile, Endpoint Operating System, SPW Version, Failure Reason (if any), and the Status of the registration.

Client Provisioning Event Logs

You can search event log entries to help diagnose a possible problem with client login behavior. For example, you may need to determine the source of an issue where client machines on your network are not able to get client provisioning resource updates upon login. You can use logging entries for Posture and Client Provisioning Audit and Posture and Client Provisioning Diagnostics.

Portal Settings for Client Provisioning Portals

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Client Provisioning Portals** > **Create, Edit, Duplicate, or Delete** > **Portal Behavior and Flow Settings**.

Portal Settings

- **HTTPS Port**: Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the **Blocked List** Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you make any change to this page. If you make any change to this page, you must update the port setting to comply with this restriction.
- **Allowed Interfaces**: Select the PSN interfaces which can run a portal. Only a PSN with an available allowed interface on a PSN can create a portal. You can configure any combination of physical and

bonded interfaces. This is a PSN-wide configuration; all portals can only run on these interfaces, this interface configuration is pushed to all the PSNs.

  - You must configure the Ethernet interfaces using IP addresses on different subnets.
  - The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
  - The portal certificate Subject Name/Alternate Subject Name must resolve to the interface IP.
  - Configure ip host x.x.x.x yyy.domain.com in ISE CLI to map secondary interface IP to FQDN, which will be used to match Certificate Subject Name/Alternate Subject Name.
  - If only the bonded NIC is selected, when the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond set upon that PSN, then the PSN logs an error and exits. It will NOT attempt to start the portal on the physical interface.
  - **NIC Teaming** or bonding is an O/S configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based on the portal settings configuration:
    - If both physical NICs and the corresponding bonded NIC are configured - When the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.

- **Certificate Group Tag**: Select the group tag of the certificate group to use for the portal’s HTTPS traffic.
- **Authentication Method**: Choose which identity source sequence (ISS) or Identity Provider (IdP) to use for user authentication. The ISS is a list of Identity Stores that are searched in sequence to verify user credentials. Some examples include: Internal Guest Users, Internal Users, Active Directory, and LDAP.

  Cisco ISE includes a default client provisioning Identity Source Sequence for Client Provisioning Portals, Certificate_Request_Sequence.
- **Fully Qualified Domain Name (FQDN)**: Enter at least one unique FQDN and/or hostname for your Client Provisioning portal. For example, you can enter provisionportal.yourcompany.com, so that when the user enters either of those into a browser, they will reach the Client Provisioning Portal.
  - Update DNS to ensure that the FQDN of the new URL resolves to a valid Policy Services Node (PSN) IP address. Optionally, this address could point to a load balancer virtual IP address that serves a pool of PSNs.
  - To avoid certificate warning messages due to name mismatches, include the FQDN of the customized URL, or a wildcard, in the subject alternative name (SAN) attribute of the local server certificate of the Cisco ISE PSN.

Note For Client Provisioning without URL redirection, the portal name that is entered in the Fully Qualified Domain Name (FQDN) field must be configured in the DNS configuration. This URL must be communicated to the users to enable Client Provisioning without URL redirection.

- **Idle Timeout**: Enter the time in minutes that you want Cisco ISE to wait before it logs out the user if there is no activity in the portal. The valid range is from 1 to 30 minutes..

Note In the Client Provisioning Portal, you can define the port number and the certificate so that the host allows you to download the same certificate for Client Provisioning and Posture. If the portal certificate is signed by the officials certificate authority, you will not receive any security warning. If the certificate is self-signed, you will receive one security warning for both the portals and Cisco AnyConnect Posture component.

Login Page Settings

- Enable Login: Select this check box to enable the login step in the Client Provisioning Portal
- Maximum failed login attempts before rate limiting: Specify the number of failed login attempts from a single browser session before Cisco ISE starts to artificially slow down the rate at which login attempts can be made, preventing additional login attempts. The time between attempts after this number of failed logins is reached is specified in **Time between login attempts when rate limiting**.
- Time between login attempts when rate limiting: Set the length of time in minutes that a user must wait before attempting to log in again, after failing to log in the number of times defined in **Maximum failed login attempts before rate limiting**.
- Include an AUP (on page/as link): Display your company’s network-usage terms and conditions, either as text on the page currently being displayed for the user or as a link that opens a new tab or window with AUP text.
- Require acceptance: Require users to accept an AUP before they can access the portal. The **Login** button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not be able to access the portal.
- Require scrolling to end of AUP: This option displays only if **Include an AUP on page** is enabled. Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP.

Acceptable Use Policy (AUP) Page Settings

- Include an AUP: Display your company’s network-usage terms and conditions on a separate page to the user.
- Require scrolling to end of AUP: Ensure that the user has read the AUP completely. The Accept button activates only after the user has scrolled to the end of the AUP.
- On first login only: Display an AUP when the user logs into the network or portal for the first time only.
- On every login: Display an AUP each time the user logs into the network or portal.

- Every ______ days (starting at first login): Display an AUP periodically after the user first logs into the network or portal.

Post-Login Banner Page Settings

Include a Post-Login Banner page: Display additional information after the users successfully log in and before they are granted network access.

Change Password Settings

Allow internal users to change their own passwords: Allow employees to change their passwords after they log in to the Client Provisioning Portal. This only applies to employees whose accounts are stored in the Cisco ISE database and not to those stored in external databases, such as Active Directory or LDAP.

HTML Support for Client Provisioning Portal Language Files

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Client Provisioning Portals** > **Edit** > **Portal Page Customization** > **Pages**. You can use the **View HTML Source** icon in the mini-editor and add HTML code in your content.

These dictionary keys in the portal's language properties files support HTML in their text.

Note This is not a complete list of the dictionary keys in the files.

- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_client_provision_posture_agent_check_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_contact_optional_content_1

- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_client_provision_optional_content_1
- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_client_provision_posture_agent_scan_message

Portal Settings for Client Provisioning Portals

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Client Provisioning Portals** > **Create, Edit, Duplicate, or Delete** > **Portal Behavior and Flow Settings**.

Portal Settings

- **HTTPS Port**: Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the **Blocked List** Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you make any change to this page. If you make any change to this page, you must update the port setting to comply with this restriction.
- **Allowed Interfaces**: Select the PSN interfaces which can run a portal. Only a PSN with an available allowed interface on a PSN can create a portal. You can configure any combination of physical and bonded interfaces. This is a PSN-wide configuration; all portals can only run on these interfaces, this interface configuration is pushed to all the PSNs.
    - You must configure the Ethernet interfaces using IP addresses on different subnets.
    - The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
    - The portal certificate Subject Name/Alternate Subject Name must resolve to the interface IP.
    - Configure ip host x.x.x.x yyy.domain.com in ISE CLI to map secondary interface IP to FQDN, which will be used to match Certificate Subject Name/Alternate Subject Name.
    - If only the bonded NIC is selected, when the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond set upon that PSN, then the PSN logs an error and exits. It will NOT attempt to start the portal on the physical interface.
    - **NIC Teaming** or bonding is an O/S configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the

bonded connection continues the connection. A NIC is selected for a portal based on the portal settings configuration:

  - If both physical NICs and the corresponding bonded NIC are configured - When the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.

- **Certificate Group Tag**: Select the group tag of the certificate group to use for the portal's HTTPS traffic.
- **Authentication Method**: Choose which identity source sequence (ISS) or Identity Provider (IdP) to use for user authentication. The ISS is a list of Identity Stores that are searched in sequence to verify user credentials. Some examples include: Internal Guest Users, Internal Users, Active Directory, and LDAP.

  Cisco ISE includes a default client provisioning Identity Source Sequence for Client Provisioning Portals, Certificate_Request_Sequence.

- **Fully Qualified Domain Name (FQDN)**: Enter at least one unique FQDN and/or hostname for your Client Provisioning portal. For example, you can enter provisionportal.yourcompany.com, so that when the user enters either of those into a browser, they will reach the Client Provisioning Portal.
  - Update DNS to ensure that the FQDN of the new URL resolves to a valid Policy Services Node (PSN) IP address. Optionally, this address could point to a load balancer virtual IP address that serves a pool of PSNs.
  - To avoid certificate warning messages due to name mismatches, include the FQDN of the customized URL, or a wildcard, in the subject alternative name (SAN) attribute of the local server certificate of the Cisco ISE PSN.

Note For Client Provisioning without URL redirection, the portal name that is entered in the Fully Qualified Domain Name (FQDN) field must be configured in the DNS configuration. This URL must be communicated to the users to enable Client Provisioning without URL redirection.

- **Idle Timeout**: Enter the time in minutes that you want Cisco ISE to wait before it logs out the user if there is no activity in the portal. The valid range is from 1 to 30 minutes..

Note In the Client Provisioning Portal, you can define the port number and the certificate so that the host allows you to download the same certificate for Client Provisioning and Posture. If the portal certificate is signed by the officials certificate authority, you will not receive any security warning. If the certificate is self-signed, you will receive one security warning for both the portals and Cisco AnyConnect Posture component.

Login Page Settings

- Enable Login: Select this check box to enable the login step in the Client Provisioning Portal
- Maximum failed login attempts before rate limiting: Specify the number of failed login attempts from a single browser session before Cisco ISE starts to artificially slow down the rate at which login attempts

can be made, preventing additional login attempts. The time between attempts after this number of failed logins is reached is specified in **Time between login attempts when rate limiting**.

- Time between login attempts when rate limiting: Set the length of time in minutes that a user must wait before attempting to log in again, after failing to log in the number of times defined in **Maximum failed login attempts before rate limiting**.
- Include an AUP (on page/as link): Display your company's network-usage terms and conditions, either as text on the page currently being displayed for the user or as a link that opens a new tab or window with AUP text.
- Require acceptance: Require users to accept an AUP before they can access the portal. The **Login** button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not be able to access the portal.
- Require scrolling to end of AUP: This option displays only if **Include an AUP on page** is enabled. Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP.

Acceptable Use Policy (AUP) Page Settings

- Include an AUP: Display your company's network-usage terms and conditions on a separate page to the user.
- Require scrolling to end of AUP: Ensure that the user has read the AUP completely. The Accept button activates only after the user has scrolled to the end of the AUP.
- On first login only: Display an AUP when the user logs into the network or portal for the first time only.
- On every login: Display an AUP each time the user logs into the network or portal.
- Every ______ days (starting at first login): Display an AUP periodically after the user first logs into the network or portal.

Post-Login Banner Page Settings

Include a Post-Login Banner page: Display additional information after the users successfully log in and before they are granted network access.

Change Password Settings

Allow internal users to change their own passwords: Allow employees to change their passwords after they log in to the Client Provisioning Portal. This only applies to employees whose accounts are stored in the Cisco ISE database and not to those stored in external databases, such as Active Directory or LDAP.

HTML Support for Client Provisioning Portal Language Files

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Client Provisioning Portals** > **Edit** > **Portal Page Customization** > **Pages**. You can use the **View HTML Source** icon in the mini-editor and add HTML code in your content.

These dictionary keys in the portal's language properties files support HTML in their text.

Note This is not a complete list of the dictionary keys in the files.

- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_client_provision_posture_agent_check_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_contact_optional_content_1
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_client_provision_optional_content_1
- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_client_provision_posture_agent_scan_message

CHAPTER 14

Threat Containment

- Threat Centric NAC Service, on page 1257
- Trusted Certificate Settings, on page 1274
- Maintenance Settings, on page 1276
- General TrustSec Settings, on page 1279
- Network Resources, on page 1282
- Device Portal Management, on page 1304

Threat Centric NAC Service

Threat Centric Network Access Control (TC-NAC) feature enables you to create authorization policies based on the threat and vulnerability attributes received from the threat and vulnerability adapters.

Threat severity levels and vulnerability assessment results can be used to dynamically control the access level of an endpoint or a user.

You can configure the vulnerability and threat adapters to send high-fidelity Indications of Compromise (IoC), Threat Detected events, and CVSS scores to Cisco ISE, so that threat-centric access policies can be created to change the privilege and context of an endpoint accordingly.

Cisco ISE supports the following adapters:

- SourceFire FireAMP (now known as Cisco Secure Endpoint)
- Cognitive Threat Analytics (CTA) adapter
- Qualys

Note Only the Qualys Enterprise Edition is currently supported for TC-NAC flows.

- Rapid7 Nexpose
- Tenable Security Center

When a threat event is detected for an endpoint, you can select the MAC address of the endpoint on the **Compromised Endpoints** window and apply an ANC policy, such as Quarantine. Cisco ISE triggers CoA for that endpoint and applies the corresponding ANC policy. If ANC policy is not available, Cisco ISE triggers CoA for that endpoint and applies the original authorization policy. You can use the **Clear Threat and**

Vulnerabilities option on the **Compromised Endpoints** window to clear the threat and vulnerabilities associated with an endpoint (from Cisco ISE system database).

The following attributes are listed under the Threat dictionary:

- CTA-Course_Of_Action (values can be Internal Blocking, Eradication, or Monitoring)
- Qualys-CVSS_Base_Score
- Qualys-CVSS_Temporal_Score
- Rapid7 Nexpose-CVSS_Base_Score
- Tenable Security Center-CVSS_Base_Score
- Tenable Security Center-CVSS_Temporal_Score

The valid range is from 0 to 10 for both Base Score and Temporal Score attributes.

When a vulnerability event is received for an endpoint, Cisco ISE triggers CoA for that endpoint. However, CoA is not triggered when a threat event is received.

You can create an authorization policy by using the vulnerability attributes to automatically quarantine the vulnerable endpoints based on the attribute values. For example:

```
Any Identity Group & Threat:Qualys-CVSS_Base_Score > 7.0 -> Quarantine
```

To view the logs of an endpoint that is automatically quarantined during CoA events, choose **Operations** > **Threat-Centric NAC Live Logs**. To view the logs of an endpoint that is quarantined manually, choose **Operations** > **Reports** > **Audit** > **Change Configuration Audit**.

Note the following points while enabling the Threat Centric NAC service:

- The Threat Centric NAC service requires a Cisco ISE Premier license.
- Threat Centric NAC service can be enabled on only one node in a deployment.
- You can add only one instance of an adapter per vendor for Vulnerability Assessment service. However, you can add multiple instances of FireAMP adapter.
- You can stop and restart an adapter without losing its configuration. After configuring an adapter, you can stop the adapter at any point of time. The adapter would remain in this state even when the ISE services are restarted. Select the adapter and click **Restart** to start the adapter again.

Note When an adapter is in Stopped state, you can edit only the name of the adapter instance; you cannot edit the adapter configuration or the advanced settings.

You can view the threat information for the endpoints on the following pages:

- **Home page > Threat dashboard**
- **Context Visibility > Endpoints > Compromised Endpoints**

The following alarms are triggered by the Threat Centric NAC service:

- Adapter not reachable (syslog ID: 91002): Indicates that the adapter cannot be reached.

- Adapter Connection Failed (syslog ID: 91018): Indicates that the adapter is reachable but the connection between the adapter and source server is down.
- Adapter Stopped Due to Error (syslog ID: 91006): This alarm is triggered if the adapter is not in the desired state. If this alarm is displayed, check the adapter configuration and server connectivity. Refer to the adapter logs for more details.
- Adapter Error (syslog ID: 91009): Indicates that the Qualys adapter is unable to establish a connection with or download information from the Qualys site.

The following reports are available for the Threat Centric NAC service:

- **Adapter Status**: The Adapter Status report displays the status of the threat and vulnerability adapters.
- **COA Events**: When a vulnerability event is received for an endpoint, Cisco ISE triggers CoA for that endpoint. The CoA Events report displays the status of these CoA events. It also displays the old and new authorization rules and the profile details for these endpoints.
- **Threat Events**: The Threat Events report provides a list of all the threat events that Cisco ISE receives from the various adapters that you have configured. Vulnerability Assessment events are not included in this report.
- **Vulnerability Assessment**: The Vulnerability Assessment report provides information about the assessments that are happening for your endpoints. You can view this report to check if the assessment is happening based on the configured policy.

You can view the following information from **Operations > Reports > Diagnostics > ISE Counters > Threshold Counter Trends**:

- Total number of events received
- Total number of threat events
- Total number of vulnerability events
- Total number of CoAs issued (to PSN)

The values for these attributes are collected every 5 minutes, so these values represent the count for the last 5 minutes.

The Threat dashboard contains the following dashlets:

- **Total Compromised Endpoints** dashlet displays the total number of endpoints (both connected and disconnected endpoints) that are currently impacted on the network.
- **Compromised Endpoints Over Time** dashlet displays a historical view of the impact on endpoints for the specified time period.
- **Top Threats** dashlet displays the top threats based on the number of endpoints impacted and the severity of the threat.
- You can use the **Threats Watchlist** dashlet to analyze the trend of selected events.

The size of the bubbles in the **Top Threats** dashlet indicates the number of endpoints impacted and the light shaded area indicates the number of disconnected endpoints. The color as well as the vertical scale indicate the severity of the threat. There are two categories of threat—Indicators and Incidents. The severity attribute for Indicator is "Likely_Impact" and the severity attribute for Incident is "Impact_Qualification".

The Compromised Endpoint window displays the matrix view of the endpoints that are impacted and the severity of the impact for each threat category. You can click on the device link to view the detailed threat information for an endpoint.

The Course Of Action chart displays the action taken (Internal Blocking, Eradication, or Monitoring) for the threat incidents based on the CTA-Course_Of_Action attribute received from the CTA adapter.

The Vulnerability dashboard on the Home page contains the following dashlets:

- **Total Vulnerable Endpoints** dashlet displays the total number of endpoints that have a CVSS score greater than the specified value. Also displays the total number of connected and disconnected endpoints that have a CVSS score greater than the specified value.
- **Top Vulnerability** dashlet displays the top vulnerabilities based on the number of endpoints impacted or the severity of the vulnerability. The size of the bubbles in the Top Vulnerability dashlet indicates the number of endpoints impacted and the light shaded area indicates the number of disconnected endpoints. The color as well as the vertical scale indicates the severity of the vulnerability.
- You can use the **Vulnerability Watchlist** dashlet to analyze the trend of selected vulnerabilities over a period of time. Click the search icon in the dashlet and enter the vendor-specific id ("qid" for Qualys ID number) to select and view the trend for that particular ID number.
- The **Vulnerable Endpoints Over Time** dashlet displays a historical view of the impact on endpoints over time.

The Endpoint Count By CVSS graph on the **Vulnerable Endpoints** window shows the number of endpoints that are affected and their CVSS scores. You can also view the list of affected endpoints on the **Vulnerable Endpoints** window. You can click the device link to view the detailed vulnerability information for each endpoint.

Threat Centric NAC service logs are included in the support bundle. Threat Centric NAC service logs are located at support/logs/TC-NAC/

Note Cisco ISE does not support on-demand scanning with credentials on endpoints.

Enable Threat Centric NAC Service

To configure vulnerability and threat adapters, you must first enable the Threat Centric NAC service. This service can be enabled on only one Policy Service Node in your deployment.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 2 Check the check box next to the PSN on which you want to enable the Threat Centric NAC service and click **Edit**.

Step 3 Check the **Enable Threat Centric NAC Service** check box.

Step 4 Click **Save**.

Related Topics

Add SourceFire FireAMP Adapter, on page 1261
Configure Cognitive Threat Analytics Adapter, on page 1262
Configure Authorization Profiles for CTA Adapter, on page 1263

Configure Authorization Policy using the Course of Action Attribute, on page 1264

Threat Centric NAC Service, on page 1257

Add SourceFire FireAMP Adapter

Before you begin

- You must have an account with SourceFire FireAMP.
- You must deploy FireAMP clients on all endpoints.
- You must enable Threat Centric NAC service on the deployment node (see Enable Threat Centric NAC Service, on page 1260).
- FireAMP adapter uses SSL for REST API calls (to the AMP cloud) and AMQP to receive the events. It also supports the use of proxy. FireAMP adapter uses port 443 for communication.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Threat Centric NAC** > **Third Party Vendors**.

Step 2 Click **Add**.

Step 3 Select **AMP : Threat** from the **Vendor** drop-down list.

Step 4 Enter a name for the adapter instance.

Step 5 Click **Save**.

Step 6 Refresh the Vendor Instances listing window. You can configure the adapter only after the adapter status changes to **Ready to Configure** on the Vendor Instances listing window.

Step 7 Click the **Ready to configure** link.

Step 8 (Optional) If you have configured a SOCKS proxy server to route all the traffic, enter the hostname and the port number of the proxy server.

Step 9 Select the cloud to which you want to connect. You can select US cloud or EU cloud.

Step 10 Select the event source to which you want to subscribe. The following options are available:

- **AMP events only**
- **CTA events only**
- **CTA and AMP events**

Step 11 Click the FireAMP link and login as admin in FireAMP. Click **Allow** in the **Applications** pane to authorize the Streaming Event Export request.
You will be redirected back to Cisco ISE.

Step 12 Select the events (for example, suspicious download, connection to suspicious domain, executed malware, java compromise) that you want to monitor.

When you change the advanced settings or reconfigure an adapter, if there are any new events added to the AMP cloud, those events are also listed in the **Events Listing** window.

You can choose a log level for the adapter. The available options are: **Error**, **Info**, and **Debug**.

The summary of the adapter instance configuration will be displayed in the **Configuration Summary** window.

Configure Cognitive Threat Analytics Adapter

Before you begin

- You must enable Threat Centric NAC service on the deployment node (see Enable Threat Centric NAC Service, on page 1260).
- Log in to Cisco Cognitive Threat Analytics (CTA) portal via http://cognitive.cisco.com/login and request CTA STIX/TAXII service. For more information, see Cisco ScanCenter Administrator Guide.
- Cognitive Threat Analytics (CTA) adapter uses TAXII protocol with SSL to poll the CTA cloud for detected threats. It also supports the use of proxy.
- Import the adapter certificate in to the Trusted Certificate Store. Choose **Administration > System > Certificates > Trusted Certificates > Import** to import the certificate.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Threat Centric NAC** > **Third Party Vendors**.

Step 2 Click **Add**.

Step 3 Select **CTA : Threat** from the **Vendor** drop-down list.

Step 4 Enter a name for the adapter instance.

Step 5 Click **Save**.

Step 6 Refresh the Vendor Instances listing page. You can configure the adapter only after the adapter status changes to **Ready to Configure** on the Vendor Instances listing page.

Step 7 Click the **Ready to configure** link.

Step 8 Enter the following details:

- **CTA STIX/TAXII service URL**: URL of the CTA cloud service. By default, the following URL is used: https://taxii.cloudsec.sco.cisco.com/skym-taxii-ws/PollService/
- **CTA feed name**: Enter the feed name of the CTA cloud service.
- **CTA username and password**: Enter the username and password for the CTA cloud service.
- **Proxy host and port (optional)**: If you have configured a proxy server to route all the traffic, enter the hostname and the port number of the proxy server.
- **Polling interval**: Time interval between each poll. Default value is 30 minutes.
- **First Poll Duration in hours**: Age of the data to be pulled at the first poll. Default value is 2 hours. Maximum value is 12 hours.
- **Incident Type**: The following options are available:
  - **CTA events only**
  - **AMP events only**

- **CTA and AMP events**

Step 9 Click **Next**.

Step 10 Click **Advanced Settings** to configure the following options:

- **Impact Qualification**: Select the severity level of the incident to be polled. The following options are available:
    - **1 - Insignificant**
    - **2 - Distracting**
    - **3 - Painful**
    - **4 - Damaging**
    - **5 - Catastrophic**

  For example, if you have selected "3-Painful", incidents with this severity level (3-Painful) and above (in this case, 4-Damaging and 5-Catastrophic) are polled.
- **Logging level**: Choose a log level for the adapter. The available options are: Error, Info, and Debug.

Step 11 Click **Finish**.

Note CTA works with user identities listed in the web proxy logs as IP addresses or usernames. Specifically, in the case of IP addresses, the IP address of a device that is available through the proxy logs may collide with the IP address of another device on the internal network. For example, roaming users connected via AnyConnect and a split-tunnel directly to the internet could acquire a local IP range address (for example, 10.0.0.X address), which may collide with an address in an overlapping private IP range used in an internal network. We recommend that you take into account the logical network architecture while defining the policies to avoid quarantine actions being applied on mismatched devices.

Configure Authorization Profiles for CTA Adapter

For each threat event, the CTA adapter returns one of the following values for the Course of Action attribute: Internal Blocking, Monitoring, or Eradication. You can create authorization profiles based on these values.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Authorization** > **Authorization Profiles**.

Step 2 Click **Add**.

Step 3 Enter a name and description for the authorization profile.

Step 4 Select the Access Type.

Step 5 Enter the required details and click **Submit**.

Configure Authorization Policy using the Course of Action Attribute

You can use the CTA-Course_Of_Action attribute to configure authorization policies for the endpoints for which threat events are reported. This attribute is available in the Threat directory.

You can also create exception rules based on the CTA-Course_Of_Action attribute.

Step 1 Choose **Policy** > **Policy Sets**
You can edit an existing policy rule or create a new exception rule for the endpoints with threat events.

Step 2 Create a condition to check for the CTA-Course_Of_Action attribute value and assign the appropriate authorization profile. For example:

Network_Access_Authentication_Passed AND ThreatCTA-Course_Of_Action CONTAINS Internal Blocking then blocking (authorization profile)

Note "Internal Blocking" is the recommended Course of Action attribute to be used for quarantining the endpoints.

Step 3 Click **Save**.

When a threat event is received for an endpoint, Cisco ISE checks if there is any matching authorization policy for the endpoint and triggers CoA only if the endpoint is active. If the endpoint is offline, threat event details are added to the Threat Events report (Operations > Reports > Threat Centric NAC > Threat Events).

Note Sometimes CTA sends multiple risks and their associated Course of Action attributes in one incident. For example, it can send "Internal Blocking" and "Monitoring" (course of action attributes) in one incident. In this case, if you have configured an authorization policy to quarantine endpoints using "equals" operator, the endpoints will not be quarantined. For example:

```
CTA-Course_Of_Action EQUALS Internal Blocking then Quarantine_Systems (authorization profile)
```

In such cases, you must use "contains" operator in the authorization policy to quarantine the endpoints. For example:

```
CTA-Course_Of_Action CONTAINS Internal Blocking then Quarantine_Systems
```

Support for Vulnerability Assessment in Cisco ISE

Cisco ISE integrates with the following Vulnerability Assessment (VA) Ecosystem Partners to obtain vulnerability results of endpoints that connect to the Cisco ISE network:

- Qualys: Qualys is a cloud-based assessment system with scanner appliances deployed in the network. Cisco ISE allows you to configure an adapter that communicates with Qualys and obtains the VA results. You can configure the adapter from the Admin portal. You need a Cisco ISE administrator account with Super Admin privileges to configure the adapter. The Qualys adapter uses REST APIs to communicate with the Qualys Cloud Service. You need a user account in Qualys with Manager privileges to access the REST APIs. Cisco ISE uses following Qualys REST APIs:
  - Host Detection List API: To check the last scan results of the endpoint
  - Scan API: To trigger an on-demand scan of the endpoint

Qualys enforces limits on the number of API calls that subscribed users can make. The default rate limit count is 300 per 24 hours. Cisco ISE uses Qualys API version 2.0 to connect to Qualys. Refer to the Qualys API V2 User Guide for more information on these API functions.

- Rapid7 Nexpose: Cisco ISE integrates with Rapid 7 Nexpose, a vulnerability management solution, to help detect vulnerabilities and enables you to respond to such threats quickly. Cisco ISE receives the vulnerability data from Nexpose and based on the policies that you configure in ISE, it quarantines the affected endpoints. From the Cisco ISE dashboard, you can view the affected endpoint and take appropriate action.

  Cisco ISE has been tested with Nexpose Release 6.4.1.

- Tenable SecurityCenter (Nessus scanner): Cisco ISE integrates with Tenable SecurityCenter and receives the vulnerability data from Tenable Nessus scanner (managed by Tenable SecurityCenter) and based on the policies that you configure in ISE, it quarantines the affected endpoints. From the Cisco ISE dashboard, you can view the affected endpoints and take appropriate action.

  Cisco ISE has been tested with Tenable SecurityCenter 5.3.2.

The results from the ecosystem partner are converted in to a Structured Threat Information Expression (STIX) representation and based on this value, a Change of Authorization (CoA) is triggered, if needed, and the appropriate level of access is granted to the endpoint.

The time taken to assess endpoints for vulnerabilities depends on various factors and hence VA cannot be performed in real time. The factors that affect the time taken to assess an endpoint for vulnerabilities include:

- Vulnerability assessment ecosystem
- Type of vulnerabilities scanned for
- Type of scans enabled
- Network and system resources allocated by the ecosystem for the scanner appliances

In this release of Cisco ISE, only endpoints with IPv4 addresses can be assessed for vulnerabilities.

Enable and Configure Vulnerability Assessment Service

To enable and configure Vulnerability Assessment Service in Cisco ISE, perform the following tasks:

Step 1 Enable Threat Centric NAC Service, on page 1260.

Step 2 To configure:

- Qualys adapter, see Configure Qualys Adapter, on page 1266.
- Nexpose adapter, see Configure Nexpose Adapter, on page 1269.
- Tenable adapter, see Configure Tenable Adapter, on page 1270.

Step 3 Configure Authorization Profile, on page 1273.

Step 4 Configure Exception Rule to Quarantine a Vulnerable Endpoint, on page 1273.

Enable Threat Centric NAC Service

To configure vulnerability and threat adapters, you must first enable the Threat Centric NAC service. This service can be enabled on only one Policy Service Node in your deployment.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 2 Check the check box next to the PSN on which you want to enable the Threat Centric NAC service and click **Edit**.

Step 3 Check the **Enable Threat Centric NAC Service** check box.

Step 4 Click **Save**.

Related Topics

Add SourceFire FireAMP Adapter, on page 1261
Configure Cognitive Threat Analytics Adapter, on page 1262
Configure Authorization Profiles for CTA Adapter, on page 1263
Configure Authorization Policy using the Course of Action Attribute, on page 1264
Threat Centric NAC Service, on page 1257

Configure Qualys Adapter

Cisco ISE supports the Qualys Vulnerability Assessment Ecosystem. You must create a Qualys adapter for Cisco ISE to communicate with Qualys and obtain the VA results.

Before you begin

- You must have the following user accounts:
  - Admin user account in Cisco ISE with Super Admin privileges to be able to configure a vendor adapter.
  - User account in Qualys with Manager privileges
- Ensure that you have appropriate Qualys license subscriptions. You need access to the Qualys Report Center, Knowledge Base (KBX), and API. Contact your Qualys Account Manager for details.
- Import the Qualys server certificate in to the Trusted Certificates store in Cisco ISE (**Administration** > **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import**). Ensure that the appropriate root and intermediate certificates are imported (or present) in the Cisco ISE Trusted Certificates store.
- Refer to the Qualys API Guide for the following configurations:
  - Ensure that you have enabled CVSS Scoring in Qualys (**Reports** > **Setup** > **CVSS Scoring** > **Enable CVSS Scoring**).
  - Ensure that you add the IP address and subnet mask of your endpoints in Qualys (**Assets** > **Host Assets**).
  - Ensure that you have the name of the Qualys option profile. The option profile is the scanner template that Qualys uses for scanning. We recommend that you use an option profile that includes authenticated scans (this option checks the MAC Address of the endpoint as well).
- Cisco ISE communicates with Qualys over HTTPS/SSL (port 443).

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Threat Centric NAC** > **Third Party Vendors**.

Step 2 Click **Add**.

Step 3 From the **Vendor** drop-down list, choose **Qualys:VA**.

Step 4 Enter a name for the adapter instance. For example, Qualys_Instance.

The listing window appears with a list of configured adapter instances.

Step 5 Refresh the Vendor Instances listing window. The status for the newly added Qualys_Instance adapter should change to **Ready to Configure**.

Step 6 Click the **Ready to Configure** link.

Step 7 Enter the following values in the Qualys configuration screen and click **Next**.

Field Name	Description
REST API Host	The hostname of the server that hosts the Qualys cloud. Contact your Qualys representative for this information.
REST API Port	443
Username	User account in Qualys with Manager privileges.
Password	Password for the Qualys user account.
HTTP Proxy Host	If you have a proxy server configured to route all Internet traffic, enter the hostname of the proxy server.
HTTP Proxy Port	Enter the port number used by the proxy server.

If the connection to the Qualys server is established, the Scanner Mappings window appears with a list of Qualys scanners. The Qualys scanners from your network appear in this window.

Step 8 Choose the default scanner that Cisco ISE will use for on-demand scans.

Step 9 In the **PSN to Scanner Mapping** area, choose one or more Qualys scanner appliance(s) to the PSN node, and click **Next**.

The **Advanced Settings** window appears.

Step 10 Enter the following values in the **Advanced Settings** window. The settings in this window determine whether an on-demand scan will be triggered or the last scan results will be used for VA.

Field Name	Description
Option Profile	Choose the option profile that you want Qualys to use for scanning the endpoint. You can choose the default option profile, Initial Options.
Last Scan Results - Check Settings	
Last scan results check interval in minutes	(Impacts the access rate of Host Detection List API) Time interval in minutes after which the last scan results must be checked again. Valid range is between 1 and 2880.

Field Name	Description
Maximum results before last scan results are checked	(Impacts the access rate of Host Detection List API) If the number of queued scan requests exceeds the maximum number specified here, the last scan results are checked before the time interval specified in **Last scan results check interval in minutes** field. Valid range is between 1 and 1000.
Verify MAC address	True or False. When set to true, the last scan results from Qualys would be used only if it includes the MAC address of the endpoint.
Scan Settings	
Scan trigger interval in minutes	(Impacts the access rate of Scan API) Time interval in minutes after which an on-demand scan is triggered. Valid range is between 1 and 2880.
Maximum requests before scan is triggered	(Impacts the access rate of Scan API) If the number of queued scan requests exceeds the maximum number specified here, an on-demand scan would be triggered before the time interval specified in **Scan trigger interval in minutes** field. Valid range is between 1 and 1000.
Scan status check interval in minutes	Time interval in minutes after which Cisco ISE communicates with Qualys to check the status of the scan. Valid range is between 1 and 60.
Number of scans that can be triggered concurrently	(This option depends on the number of scanners you have mapped to each PSN in the Scanner Mappings screen) Each scanner can process only one request at a time. If you have mapped more than one scanner to the PSNs, then you can increment this value based on the number of scanners you have chosen. Valid range is between 1 and 200.
Scan timeout in minutes	Time in minutes after which the scan request will time out. If a scan request times out, an alarm is generated. Valid range is between 20 and 1440.
Maximum number of IP addresses to be submitted per scanner	Indicates the number of requests that can be queued into a single request to be sent to Qualys for processing. Valid range is between 1 and 1000.
Choose the log level for adapter log files	Choose a log level for the adapter. The available options are ERROR, INFO, DEBUG, and TRACE.

Step 11 Click **Next** to review the Configuration Settings.

Step 12 Click **Finish**.

Configure Nexpose Adapter

You must create a Nexpose adapter for Cisco ISE to communicate with Nexpose and obtain the VA results.

Before you begin

- Ensure that you have enabled the Threat-Centric NAC service in Cisco ISE.
- Log in to Nexpose Security Console and create a user account with the following privileges:
  - Manage sites
  - Create reports
- Import the Nexpose server certificate in to the Trusted Certificates store in Cisco ISE (**Administration** > **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import**). Ensure that the appropriate root and intermediate certificates are imported (or present) in the Cisco ISE Trusted Certificates store.
- Cisco ISE communicates with Nexpose over HTTPS/SSL (port 3780).

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Threat Centric NAC** > **Third Party Vendors**.

Step 2 Click **Add**.

Step 3 From the **Vendor** drop-down list, choose **Rapid7 Nexpose:VA**.

Step 4 Enter a name for the adapter instance. For example, Nexpose.

The listing window appears with a list of configured adapter instances.

Step 5 Refresh the Vendor Instances listing window. The status for the newly added Nexpose adapter should change to **Ready to Configure**.

Step 6 Click the **Ready to Configure** link.

Step 7 Enter the following values in the Nexpose configuration screen and click **Next**.

Field Name	Description
Nexpose Host	The hostname of the Nexpose server.
Nexpose Port	3780.
Username	Nexpose Admin user account.
Password	Password for the Nexpose Admin user account.
HTTP Proxy Host	If you have a proxy server configured to route all Internet traffic, enter the hostname of the proxy server.
HTTP Proxy Port	Enter the port number used by the proxy server.

Step 8 Click **Next** to configure Advanced Settings.

Step 9 Enter the following values in the **Advanced Settings** window. The settings in this window determine whether an on-demand scan will be triggered or the last scan results will be used for VA.

Field Name	Description
Settings for checking latest scan results	
Interval between checking the latest scan results in minutes	Time interval in minutes after which the last scan results must be checked again. Valid range is between 1 and 2880.
Number of pending requests that can trigger checking the latest scan results	If the number of queued scan requests exceeds the maximum number specified here, the last scan results are checked before the time interval specified in Interval between checking the latest scan results in minutes field. Valid range is between 1 and 1000.
Verify MAC address	True or False. When set to true, the last scan results from Nexpose would be used only if it includes the MAC address of the endpoint.
Scan settings	
Scan trigger interval for each site in minutes	Time interval in minutes after which a scan is triggered. Valid range is between 1 and 2880.
Number of pending requests before a scan is triggered for each site	If the number of queued scan requests exceeds the maximum number specified here, a scan would be triggered before the time interval specified in **Scan timeout in minutes** field. Valid range is between 1 and 1000.
Scan timeout in minutes	Time in minutes after which the scan request will time out. If a scan request times out, an alarm is generated. Valid range is between 20 and 1440.
Number of sites for which scans could be triggered concurrently	The number of sites for which scans can be run concurrently. Valid range is between 1 and 200.
Timezone	Choose the time zone based on the time zone that is configured in the Nexpose server.
Http timeout in seconds	Time interval in seconds for Cisco ISE to wait for a response from Nexpose. Valid range is between 5 and 1200.
Choose the log level for adapter log files	Choose a log level for the adapter. The available options are ERROR, INFO, DEBUG, and TRACE.

Step 10 Click **Next** to review the Configuration Settings.

Step 11 Click **Finish**.

Configure Tenable Adapter

You must create a Tenable adapter for Cisco ISE to communicate with Tenable SecurityCenter (Nessus scanner) and obtain the VA results.

Before you begin

You must configure the following in Tenable SecurityCenter before you can configure the Tenable Adapter in Cisco ISE. Refer to Tenable SecurityCenter Documentation for these configurations.

- You must have Tenable Security Center and Tenable Nessus Vulnerability Scanner installed. While registering the Tenable Nessus scanner, ensure that you choose **Managed by SecurityCenter** in the **Registration** field.
- Create a user account with Security Manager privilege in Tenable SecurityCenter.
- Create a repository in SecurityCenter (Log in to Tenable SecurityCenter with Admin credentials and choose **Repository** > **Add**).
- Add the endpoint IP range to be scanned in the repository.
- Add Nessus scanner.
- Create scan zones and assign IP addresses to the scan zones and scanners that are mapped to these scan zones.
- Create a scan policy for ISE.
- Add an active scan and associate it with the ISE scan policy. Configure settings and targets (IP/DNS names).
- Export System and Root certificates from Tenable SecurityCenter and import it in to the Trusted Certificates store in Cisco ISE (**Administration** > **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import**). Ensure that the appropriate root and intermediate certificates are imported (or present) in the Cisco ISE Trusted Certificates store.
- For Tenable SecurityCenter 6.4 and later releases, you must set the **SCAN_DEFAULT_SCAN_TIMEOUT** parameter value (under /opt/sc/src/) to 43200.

Note Cisco ISE communicates with Tenable SecurityCenter over HTTPS/SSL (port 443).

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Threat Centric NAC** > **Third Party Vendors**.

Step 2 Click **Add**.

Step 3 From the **Vendor** drop-down list, choose **Tenable Security Center:VA**.

Step 4 Enter a name for the adapter instance. For example, Tenable.

The listing window appears with a list of configured adapter instances.

Step 5 Refresh the Vendor Instances listing window. The status for the newly added Tenable adapter should change to **Ready to Configure**.

Step 6 Click the **Ready to Configure** link.

Step 7 Enter the following values in the Tenable SecurityCenter configuration window and click **Next**.

Field Name	Description
Tenable SecurityCenter Host	The hostname of the Tenable SecurityCenter.

Field Name	Description
Tenable SecurityCenter Port	443
Username	Username of the user account that has Security Manager privileges in Tenable SecurityCenter.
Password	Password of the user account that has Security Manager privileges in Tenable SecurityCenter.
HTTP Proxy Host	If you have a proxy server configured to route all Internet traffic, enter the hostname of the proxy server.
HTTP Proxy Port	Enter the port number used by the proxy server.

Step 8 Click **Next**.

Step 9 Enter the following values in the **Advanced Settings** window. The settings in this window determine whether an on-demand scan will be triggered or the last scan results will be used for VA.

Field Name	Description
Repository	Choose the repository that you created in Tenable SecurityCenter.
Scan Policy	Choose the scan policy that you have created for ISE in Tenable SecurityCenter.
Settings for checking latest scan results	
Interval between checking the latest scan results in minutes	Time interval in minutes after which the last scan results must be checked again. Valid range is between 1 and 2880.
Number of pending requests that can trigger checking the latest scan results	If the number of queued scan requests exceeds the maximum number specified here, the last scan results are checked before the time interval specified in the **Interval between checking the latest scan results in minutes** field. Valid range is between 1 and 1000. The default is 10.
Verify MAC address	True or False. When set to true, the last scan results from Tenable SecurityCenter would be used only if it includes the MAC address of the endpoint.
Scan Settings	
Scan trigger interval for each site in minutes	Time interval in minutes after which an on-demand scan is triggered. Valid range is between 1 and 2880.
Number of pending requests before a scan is triggered	If the number of queued scan requests exceeds the maximum number specified here, an on-demand scan would be triggered before the time interval specified in **Scan trigger interval for each site in minutes** field. Valid range is between 1 and 1000.

Field Name	**Description**
Scan timeout in minutes	Time in minutes after which the scan request times out. If a scan request times out, an alarm is generated. Valid range is between 20 and 1440.
Number of scans that could run in parallel	The number of scans that can be run concurrently. Valid range is between 1 and 200.
Http timeout in seconds	Time interval in seconds for Cisco ISE to wait for a response from Tenable SecurityCenter. Valid range is between 5 and 1200.
Choose the log level for adapter log files	Choose a log level for the adapter. The available options are ERROR, INFO, DEBUG, and TRACE.

Step 10 Click **Next** to review the Configuration Settings.

Step 11 Click **Finish**.

Configure Authorization Profile

The authorization profile in Cisco ISE now includes an option to scan endpoints for vulnerabilities. You can choose to run the scan periodically and also specify the time interval for these scans. After you define the authorization profile, you can apply it to an existing authorization policy rule or create a new authorization policy rule.

Before you begin

You must have enabled the Threat Centric NAC service and configured a vendor adapter.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Authorization** > **Authorization Profiles**.

Step 2 Create a new authorization profile or edit an existing profile.

Step 3 From the **Common Tasks** area, check the **Assess Vulnerabilities** check box.

Step 4 From the **Adapter Instance** drop-down list, choose the vendor adapter that you have configured. For example, Qualys_Instance.

Step 5 Enter the scan interval in hours in the Trigger scan if the time since last scan is greater than text box. Valid range is between 1 and 9999.

Step 6 Check the **Assess periodically using above interval** check box.

Step 7 Click **Submit**.

Configure Exception Rule to Quarantine a Vulnerable Endpoint

You can use the following Vulnerability Assessment attributes to configure an exception rule and provide limited access to vulnerable endpoints:

- Threat:Qualys-CVSS_Base_Score

- Threat:Qualys-CVSS_Temporal_Score
- Rapid7 Nexpose-CVSS_Base_Score
- Tenable Security Center-CVSS_Base_Score
- Tenable Security Center-CVSS_Temporal_Score

These attributes are available in the Threat directory. Valid value ranges from 0 to 10.

You can choose to quarantine the endpoint, provide limited access (redirect to a different portal), or reject the request.

Step 1 Choose **Policy** > **Policy Sets**.
You can edit an existing policy rule or create a new exception rule to check for VA attributes.

Step 2 Create a condition to check for the Qualys score and assign the appropriate authorization profile. For example:

Any Identity Group & Threat:Qualys-CVSS_Base_Score > 5 -> Quarantine (authorization profile)

Step 3 Click **Save**.

Vulnerability Assessment Logs

Cisco ISE provides the following logs for troubleshooting VA services.

- vaservice.log—Contains VA core information and is available in the node that runs the TC-NAC service.
- varuntime.log—Contains information about the endpoint and the VA flow; is available in the Monitoring node and the node that runs the TC-NAC service.
- vaaggregation.log—Contains hourly aggregation details about the endpoint vulnerability and is available in the Primary Administration Node.

Trusted Certificate Settings

The following table describes the fields in the **Edit** window of a Trusted Certificate. Edit the CA certificate attributes in this window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Trusted Certificates**. Check the check box for the Trusted Certificate you want to edit, and click **Edit**.

Table 178: Trusted Certificate Edit Settings

Field Name	Usage Guidelines
Certificate Issuer	
Friendly Name	Enter a friendly name for the certificate. This is an optional field. If you do not enter a friendly name, a default name is generated in the following format: *common-name#issuer#nnnnn*

Field Name	Usage Guidelines
Status	Choose **Enabled** or **Disabled** from the drop-down list. If the certificate is disabled, Cisco ISE will not use the certificate for establishing trust.
Description	(Optional) Enter a description.
Usage	
Trust for authentication within ISE	Check this check box if you want this certificate to verify server certificates (from other Cisco ISE nodes or LDAP servers).
Trust for client authentication and Syslog	(Applicable only if you check the **Trust for authentication within ISE** check box) Check the check box if you want this certificate to be used to: • Authenticate endpoints that connect to Cisco ISE using the EAP protocol. • Trust a Syslog server.
Trust for certificate based admin authentication	You can check this check box only when **Trust for client authentication and Syslog** is selected. Check this check box to enable usage for certificate-based authentications for admin access. Import the required certificate chains into the Trusted Certificate store.
Trust for authentication of Cisco Services	Check this check box if you want this certificate to be used to trust external Cisco services such as the Feed Service.
Certificate Status Validation	Cisco ISE supports two ways of checking the revocation status of a client or server certificate that is issued by a particular CA. The first way is to validate the certificate using the Online Certificate Status Protocol (OCSP), which makes a request to an OCSP service maintained by the CA. The second way is to validate the certificate against a CRL which is downloaded from the CA into Cisco ISE. Both of these methods can be enabled, in which case OCSP is used first and only if a status determination cannot be made then the CRL is used.
Validate Against OCSP Service	Check the check box to validate the certificate against OCSP services. You must first create an OCSP Service to be able to check this box.
Reject the request if OCSP returns UNKNOWN status	Check the check box to reject the request if certificate status is not determined by the OCSP service. If you check this check box, an unknown status value that is returned by the OCSP service causes Cisco ISE to reject the client or server certificate currently being evaluated.
Reject the request if OCSP Responder is unreachable	Check the check box for Cisco ISE to reject the request if the OCSP Responder is not reachable.
Download CRL	Check the check box for the Cisco ISE to download a CRL.
CRL Distribution URL	Enter the URL to download the CRL from a CA. This field is automatically populated if it is specified in the certificate authority certificate. The URL must begin with “http”, “https”, or “ldap.”

Field Name	Usage Guidelines
Retrieve CRL	The CRL can be downloaded automatically or periodically. Configure the time interval between downloads.
If download failed, wait	Configure the time interval that Cisco ISE must wait Cisco ISE tries to download the CRL again.
Bypass CRL Verification if CRL is not Received	Check this check box, for the client requests to be accepted before the CRL is received. If you uncheck this check box, all client requests that use certificates signed by the selected CA will be rejected until Cisco ISE receives the CRL file.
Ignore that CRL is not yet valid or expired	Check this check box if you want Cisco ISE to ignore the start date and expiration date and continue to use the not yet active or expired CRL and permit or reject the EAP-TLS authentications based on the contents of the CRL. Uncheck this check box if you want Cisco ISE to check the CRL file for the start date in the Effective Date field and the expiration date in the Next Update field. If the CRL is not yet active or has expired, all authentications that use certificates signed by this CA are rejected.

Related Topics

Trusted Certificates Store, on page 301

Edit a Trusted Certificate, on page 306

Maintenance Settings

These windows help you to manage data using the backup, restore, and data purge features.

Repository Settings

The following table describes the fields on the **Repository List** window, which you can use to create repositories to store your backup files. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Maintenance** > **Repository**.

Table 179: Repository Settings

Fields	Usage Guidelines
Repository	Enter the name of the repository. Alphanumeric characters are allowed and the maximum length is 80 characters.
Protocol	Choose one of the available protocols that you want to use.
Server Name	(Required for TFTP, HTTP, HTTPS, FTP, SFTP, and NFS) Enter the hostname or IP address (IPv4 or IPv6) of the server where you want to create the repository. **Note** Ensure that the ISE eth0 interface is configured with an IPv6 address if you are adding a repository with an IPv6 address.

Fields	Usage Guidelines
Path	Enter the path to your repository. The path must be valid and must exist at the time you create the repository. This value can start with two forward slashes (//) or a single forward slash (/) denoting the root directory of the server. However, for the FTP protocol, a single forward slash (/) denotes the FTP of the local device home directory and not the root directory.
Enable PKI authentication	(Optional; applicable only for SFTP repository) Check this check box if you want to enable RSA Public Key Authentication in SFTP repository.
User Name	(Required for FTP, SFTP) Enter the username that has write permission to the specified server. A username can contain alphanumeric and _-. /@\$ characters.
Password	(Required for FTP, SFTP) Enter the password that will be used to access the specified server. Passwords can consist of the following characters: 0 to 9, a to z, A to Z, -, ., |, @, #,$, ^, &, *, (,), +, and =. Note that some of the special characters like !, ?, ~ (that are not included in the list above) are allowed for the FTP and SFTP password configuration via GUI. However, these special characters are not allowed for configuration via CLI or Open API.

Related Topics

Backup and Restore Repositories, on page 384

Create Repositories, on page 385

On-Demand Backup Settings

The following table describes the fields on the **On-Demand Backup** window, which you can use to obtain a backup at any point of time. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Backup & Restore**.

Table 180: On-Demand Backup Settings

Field Name	Usage Guidelines
Type	Choose one of the following: • **Configuration Data Backup**: Includes both application-specific and Cisco ADE operating system configuration data • **Operational Data Backup**: Includes monitoring and troubleshooting data
Backup Name	Enter the name of your backup file.
Repository Name	Repository where your backup file should be saved. You cannot enter a repository name here. You can only choose an available repository from the drop-down list. Ensure that you create the repository before you run a backup.
Encryption Key	This key is used to encrypt and decrypt the backup file.

Related Topics

Backup Data Type, on page 383
On-Demand and Scheduled Backups, on page 389
Backup History, on page 394
Backup Failures, on page 394
Cisco ISE Restore Operation, on page 395
Export Authentication and Authorization Policy Configuration, on page 400
Synchronize Primary and Secondary Nodes in a Distributed Environment, on page 402
Perform an On-Demand Backup, on page 389

Scheduled Backup Settings

The following table describes the fields on the Scheduled Backup window, which you can use to restore a full or incremental backup. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Backup and Restore**.

Table 181: Scheduled Backup Settings

Field Name	Usage Guidelines
Type	Choose one of the following: • **Configuration Data Backup**: Includes both application-specific and Cisco ADE operating system configuration data • **Operational Data Backup**: Includes monitoring and troubleshooting data
Name	Enter a name for your backup file. You can enter a descriptive name of your choice. Cisco ISE appends the timestamp to the backup filename and stores it in the repository. You will have unique backup filenames even if you configure a series of backups. On the Scheduled Backup list window, the backup filename will be prepended with “backup_occur” to indicate that the file is an occurrence **kron** job.
Description	Enter a description for the backup.
Repository Name	Select the repository where your backup file should be saved. You cannot enter a repository name here. You can only choose an available repository from the drop-down list. Ensure that you create the repository before you run a backup.
Encryption Key	Enter a key to encrypt and decrypt the backup file.
Schedule Options	Choose the frequency of your scheduled backup and fill in the other options accordingly.

Related Topics

Backup Data Type, on page 383
On-Demand and Scheduled Backups, on page 389
Backup History, on page 394
Backup Failures, on page 394
Cisco ISE Restore Operation, on page 395
Export Authentication and Authorization Policy Configuration, on page 400

Synchronize Primary and Secondary Nodes in a Distributed Environment, on page 402
Backup Using the CLI, on page 394
Schedule a Backup, on page 392

Schedule Policy Export Settings

The following table describes the fields on the **Schedule Policy Export** window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Backup and Restore** > **Policy Export**.

Table 182: Schedule Policy Export Settings

Field Name	Usage Guidelines
Encryption	
Encryption Key	Enter a key to encrypt and decrypt the export data. This field is enabled only if you select the **Export with Encryption Key** option.
Destination	
Download file to local computer	Allows you to download the policy export file to your local system.
Email file to	You can enter multiple email addresses separated by a comma.
Repository	Select the repository to export policy data to. You can't enter a repository name here. You can only choose an available repository from the drop-down list. Ensure that you create the repository before scheduling a policy export.
Export Now	Click this option to export the data to the local computer or send as an email attachment. You can't export to a repository; you can only schedule a repository export.
Schedule	
Schedule Options	Choose the frequency of the export schedule and enter the other details accordingly.

General TrustSec Settings

Define the global TrustSec settings for Cisco ISE to function as a TrustSec server and provide TrustSec services. To view this window, click the **Menu** icon (☰) and choose **Work Centers > TrustSec > Settings > General TrustSec Settings**.

Verify Trustsec Deployment

This option helps you to verify that the latest TrustSec policies are deployed on all network devices. Alarms are displayed in the Alarms dashlet, under **Work Centers > TrustSec > Dashboard and Home > Summary**, if there are any discrepancies between the policies configured on Cisco ISE and on the network device. The following alarms are displayed in the TrustSec dashboard:

- An alarm displays with an **Info** icon whenever the verification process starts or completes.

- An alarm displays with an **Info** icon if the verification process was cancelled due to a new deployment request.
- An alarm displays with a **Warning** icon if the verification process fails with an error. For example, failure to open the SSH connection with the network device, or if the network device is unavailable, or if there is any discrepancy between the policies configured on Cisco ISE and on the network device.

The **Verify Deployment** option is also available from the below windows. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose:

- **Work Centers** > **TrustSec** > **Components** > **Security Groups**
- **Work Centers** > **TrustSec** > **Components** > **Security Group ACLs**
- **Work Centers** > **TrustSec** > **TrustSec Policy** > **Egress Policy** > **Matrix**
- **Work Centers** > **TrustSec** > **TrustSec Policy** > **Egress Policy** > **Source Tree**
- **Work Centers** > **TrustSec** > **TrustSec Policy** > **Egress Policy** > **Destination Tree**

Automatic Verification After Every Deploy: Check this check box if you want Cisco ISE to verify the updates on all the network devices after every deployment. When the deployment process is complete, the verification process starts after the time you specify in the **Time after Deploy Process** field.

Time After Deploy Process: Specify the time for which you want Cisco ISE to wait for after the deployment process is complete, before starting the verification process. The valid range is 10–60 minutes.

The current verification process is cancelled if a new deployment request is received during the waiting period or if another verification is in progress.

Verify Now: Click this option to start the verification process immediately.

Protected Access Credential (PAC)

- **Tunnel PAC Time to Live** :

  Specify the expiry time for the PAC. The tunnel PAC generates a tunnel for the EAP-FAST protocol. You can specify the time in seconds, minutes, hours, days, or weeks. The default value is 90 days. The following are the valid ranges:

  - 1–157680000 seconds
  - 1–2628000 minutes
  - 1–43800 hours
  - 1–1825 days
  - 1–260 weeks

- **Proactive PAC Update Will Occur After**: Cisco ISE proactively provides a new PAC to a client after successful authentication when a configured percentage of the Tunnel PAC TTL remains. The server starts the tunnel PAC update if the first successful authentication occurs before the PAC expires. This mechanism updates the client with a valid PAC. The default value is 10%.

Security Group Tag Numbering

- **System will Assign SGT Numbers**: Choose this option if you want Cisco ISE to automatically generate the SGT numbers.
- **Except Numbers in Range**: Choose this option to reserve a range of SGT numbers for manual configuration. Cisco ISE will not use the values in this range while generating the SGTs.
- **User Must Enter SGT Numbers Manually**: Choose this option to define the SGT numbers manually.

Security Group Tag Numbering for APIC EPGs

Security Group Tag Numbering for APIC EPGs : Check this check box and specify the range of numbers to be used for the SGTs created based on the EPGs learnt from APIC.

Automatic Security Group Creation

Auto Create Security Groups When Creating Authorization Rules: Check this check box to create the SGTs automatically while creating the authorization policy rules.

If you select this option, the following message displays at the top of the **Authorization Policy** window: `Auto Security Group Creation is On`

The autocreated SGTs are named based on the rule attributes.

Note The autocreated SGTs are not deleted if you delete the corresponding authorization policy rule.

By default, this option is disabled after a fresh install or upgrade.

- **Automatic Naming Options**: Use this option to define the naming convention for the autocreated SGTs.

  (Mandatory) **Name Will Include**: Choose one of the following options:

  - **Rule name**
  - **SGT number**
  - **Rule name and SGT number**

  By default, the **Rule name** option is selected.

  Optionally, you can add the following information to the SGT name:

  - **Policy Set Name** (this option is available only if **Policy Sets** are enabled)
  - **Prefix** (up to 8 characters)
  - **Suffix** (up to 8 characters)

  Cisco ISE displays a sample SGT name in the **Example Name** field, based on your selections.

  If an SGT exists with the same name, ISE appends _*x* to the SGT name, where *x* is the first value, starting with 1 (if 1 is not used in the current name). If the new name is longer than 32 characters, Cisco ISE truncate its to the first 32 characters.

IP SGT static mapping of hostnames

IP SGT Static Mapping of Hostnames: If you use FQDN and hostnames, Cisco ISE looks for the corresponding IP addresses in the PAN and PSN nodes while deploying the mappings and checking the deployment status. You can use this option to specify the number of mappings that are created for the IP addresses returned by the DNS query. You can select one of the following options:

- **Create mappings for all IP addresses returned by a DNS query**
- **Create mappings only for the first IPv4 address and the first IPv6 address that is returned by a DNS query**

TrustSec HTTP Service for Network Devices

- **Enable HTTP Service**: Use HTTP to transfer Trustsec data to network devices over port 9063.
- **Include entire response payload body in Audit**: Enable this option to display the entire TrustSec HTTP response payload body in the audit logs. This option may dramatically decrease performance. When this option is disabled, only HTTP headers, status, and authentication information are logged.

Related Topics

TrustSec Architecture, on page 1071
TrustSec Components, on page 1071
Configure TrustSec Global Settings, on page 1078

Network Resources

Support for Session Aware Networking (SAnet)

Cisco ISE provides limited support for Session Aware Networking (SAnet). SAnet is a session management framework that runs on many Cisco switches. SAnet manages access sessions, including visibility, authentication, and authorization. SAnet uses a service template, which contains RADIUS authorization attributes. Cisco ISE includes a service template inside an authorization profile. Cisco ISE identifies service templates in an authorization profile using a flag that identifies the profile as “Service Template” compatible.

Cisco ISE authorization profiles contain RADIUS authorization attributes that are transformed into a list of attributes. SAnet service templates also contain of RADIUS authorization attributes, but those attributes are not transformed into a list.

For SAnet devices, Cisco ISE sends the name of the service template. The device downloads the content of the service template, unless it already has that content in a cache or statically defined configuration. Cisco ISE sends a CoA notification to the device when a service template changes RADIUS attributes.

Network Devices

The windows described in the following sections enable you to add and manage network devices in Cisco ISE.

Network Device Definition Settings

The following tables describe the fields in the **Network Devices** window, which you can use to configure a network access device in Cisco ISE. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Devices**, and click **Add**.

Network Device Settings

The following table describes the fields in the **New Network Devices** window.

Table 183: Network Device Settings

Field Name	Description
Name	Enter a name for the network device. You can provide a descriptive name to the network device, which is different from the hostname of the device. The device name is a logical identifier. **Note** If needed, the name of a device can be changed after it is configured.
Description	Enter a description for the device.
IP Address or **IP Range**	Choose one of the following from the drop-down list and enter the required values in the fields displayed: • **IP Address**: Enter a single IP address (IPv4 or IPv6 address) and a subnet mask. • **IP Range**: Enter the required IPv4 address range. To exclude IP addresses during authentication, enter an IP address or IP address range in the **Exclude** field. The following are the guidelines for defining the IP addresses and subnet masks, or IP address ranges: • You can define a specific IP address, or an IP range with a subnet mask. If device A has an IP address range defined, you can configure another device, B, with an individual address from the range that is defined in device A. • You can define IP address ranges in all the octets. You can use a hyphen (-) or an asterisk (*) as wildcard to specify a range of IP addresses. For example, *.*.*.*, 1-10.1-10.1-10.1-10, or 10-11.*.5.10-15. • You can exclude a subset of IP address range from the configured range in a scenario where that subset has already been added, for example, 10.197.65.*/10.197.65.1, or 10.197.65.* exclude 10.197.65.1. • You can configure up to 40 IP addresses or IP ranges for each network device. • You cannot define two devices with the same specific IP addresses. • You cannot define two devices with the same IP range. The IP ranges must not overlap either partially or completely.

Field Name	Description
Device Profile	Choose the vendor of the network device from the drop-down list. Use the tooltip next to the drop-down list to see the flows and services that the selected vendor's network devices support. The tooltip also displays the RADIUS Change of Authorization (CoA) port and type of URL redirect that is used by the device. These attributes are defined in the device type's network device profile.
Model Name	Choose the device model from the drop-down list. Use the model name as one of the parameters while checking for conditions in rule-based policies. This attribute is present in the device dictionary.
Software Version	Choose the version of the software running on the network device from the drop-down list. You can use the software version as one of the parameters while checking for conditions in rule-based policies. This attribute is present in the device dictionary.
Network Device Group	In the **Network Device Group** area, choose the required values from the **Location**, **IPsec**, and **Device Type** drop-down lists. If you do not specifically assign a device to a group, it becomes a part of the default device groups (root network device groups), which is **All Locations** by location and **All Device Types** by device type.

Note While using a filter to choose and delete a Network Access Device (NAD) from your Cisco ISE deployment, clear your browser cache to ensure that only chosen NADs are deleted.

RADIUS Authentication Settings

The following table describes the fields in the **RADIUS Authentication Settings** area.

Table 184: Fields in the RADIUS Authentication Settings Area

Field Name	Usage Guidelines
RADIUS UDP Settings	
Protocol	Displays **RADIUS** as the selected protocol.

Field Name	Usage Guidelines
Shared Secret	Enter the shared secret for the network device. The shared secret is the key that is configured on the network device using the **radius-host** command with the **pac** option. **Note** The length of the shared secret must be equal to or greater than the value configured in the **Minimum RADIUS Shared Secret Length** field in the **Device Security Settings** window (**Administration > Network Resources > Network Devices > Device Security Settings**). For a RADIUS server, the best practice is to have 22 characters. For new installations and upgraded deployments, the shared secret length is four characters by default. You can change this value in the **Device Security Settings** window.
Use Second Shared Secret	Specify a second shared secret to be used by the network device and Cisco ISE. **Note** Although Cisco TrustSec devices can take advantage of the dual shared secrets (keys), Cisco TrustSec CoA packets sent by Cisco ISE will always use the first shared secret (key). To enable the use of the second shared secret, choose the Cisco ISE node from which the Cisco TrustSec CoA packets must be sent to the Cisco TrustSec device. Configure the Cisco ISE node to be used for this task in the **Send From** drop-down list in the **Work Centers** > **Device Administration** > **Network Resources** > **Network Devices** > **Add** > **Advanced TrustSec Settings** window. You can select a primary administration node (PAN) or a policy service node (PSN). If the chosen PSN node is down, the PAN sends the Cisco TrustSec CoA packets to the Cisco TrustSec device. **Note** The Second Shared Secret feature for RADIUS Access Request works only for packets containing the **Message-Authenticator** field.
CoA Port	Specify the port to be used for RADIUS CoA. The default CoA port for the device is defined in the network device profile that is configured for a network device (**Administration** > **Network Resources** > **Network Device Profiles** > **Network Resources** > **Network Device Profiles**). Click **Set To Default** to use the default CoA port. **Note** If you modify the CoA port specified in the **Network Devices** window (**Administration** > **Network Resources** > **Network Devices**) under **RADIUS Authentication Settings**, make sure that you specify the same CoA port for the corresponding profile in the **Network Device Profile** window (**Administration** > **Network Resources** > **Network Device Profiles**).
RADIUS DTLS Settings	
DTLS Required	If you check the **DTLS Required** check box, Cisco ISE processes only the DTLS requests from this device. If this option is disabled, Cisco ISE processes both UDP and DTLS requests from this device. RADIUS DTLS provides improved security for Secure Sockets Layer (SSL) tunnel establishment and RADIUS communication.

Field Name	Usage Guidelines
Shared Secret	Displays the shared secret that is used for RADIUS DTLS. This value is fixed and used to compute the Message Digest 5 (MD5) integrity checks.
CoA Port	Specify the port to be used for RADIUS DTLS CoA.
Issuer CA of ISE Certificates for CoA	Choose the Certificate Authority to be used for RADIUS DTLS CoA from the drop-down list.
DNS Name	Enter the DNS name of the network device. If the **Enable RADIUS/DTLS Client Identity Verification** option is enabled in the **RADIUS Settings** window (**Adminstration** > **System** > **Settings** > **Protocols** > **RADIUS**, Cisco ISE compares this DNS name with the DNS name that is specified in the client certificate to verify the identity of the network device.
General Settings	
Enable KeyWrap	Check the **Enable KeyWrap** check box only if KeyWrap algorithms are supported by the network device. The network device must be compatible with AES KeyWrap RFC (RFC 3394). This option is used to increase the RADIUS security through an AES KeyWrap algorithm.
Key Encryption Key	Enter the encryption key that is used for session encryption (secrecy).
Message Authenticator Code Key	Enter the key that is used for keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages.
Key Input Format	Click one of the following radio buttons: • **ASCII**: The value that is entered in the **Key Encryption Key** field must be 16 characters (bytes) in length, and the value that is entered in the **Message Authenticator Code Key** field must be 20 characters (bytes) in length. • **Hexadecimal**: The value that is entered in the **Key Encryption Key** field must be 32 characters (bytes) in length, and the value that is entered in the **Message Authenticator Code Key** field must be 40 characters (bytes) in length. You can specify the key input format that you want to use to enter the Key Encryption Key and Message Authenticator Code Key so that it matches the configuration on the network device. The value that you specify must be the correct (full) length for the key, and shorter values are not permitted.

TACACS Authentication Settings

Table 185: Fields in the TACACS Authentication Settings Area

Field Name	Usage Guidelines
Shared Secret	A string of text that is assigned to a network device when TACACS+ protocol is enabled. The user must enter the text before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
Retired Shared Secret is Active	Displayed when the retirement period is active.
Retire	Retires an existing shared secret instead of ending it. When you click **Retire**, a dialog box is displayed. You can click either **Yes** or **No**.
Remaining Retired Period	(Available only if you click **Yes** in the **Retire** dialog box) Displays the default value that is specified in **Work Centers** > **Device Administration** > **Settings** > **Connection Settings** > **Default Shared Secret Retirement Period.** You can change the default value, as necessary. The old shared secret remains active for the specified number of days.
End	(Available only if you click **Yes** in the **Retire** dialog box) Ends the retirement period and terminates the old shared secret.
Enable Single Connect Mode	Check the **Enable Single Connect Mode** check box to use a single TCP connection for all TACACS communications with the network device. Click one of the following radio buttons: • **Legacy Cisco Devices** • **TACACS Draft Compliance Single Connect Support** **Note** If you disable **Single Connect Mode**, Cisco ISE uses a new TCP connection for every TACACS request.

SNMP Settings

The following table describes the fields in the **SNMP Settings** section.

Table 186: Fields in the SNMP Settings Area

Field Name	Usage Guidelines
SNMP Version	Choose one of the following options from the **SNMP Version** drop-down list: • **1**: SNMPv1 does not support informs. • **2c** • **3**: SNMPv3 is the most secure model because it allows packet encryption when you choose **Priv** in the **Security Level** field. **Note** If you have configured your network device with SNMPv3 parameters, you cannot generate the **Network Device Session Status** summary report that is provided by the monitoring service (**Operations** > **Reports** > **Diagnostics** > **Network Device Session Status**). You can generate this report successfully if your network device is configured with SNMPv1 or SNMPv2c parameters.
SNMP RO Community	(Applicable only for SNMP versions 1 and 2c) Enter the Read Only Community string that provides Cisco ISE with a particular type of access to the device. **Note** The caret (circumflex ^) symbol is not allowed.
SNMP Username	(Only for SNMP Version 3) Enter the SNMP username.
Security Level	(Only for SNMP Version 3) Choose one the following options from the **Security Level** drop-down list: • **Auth**: Enables MD5 or Secure Hash Algorithm (SHA) packet authentication. • **No Auth**: No authentication and no privacy security level. • **Priv**: Enables Data Encryption Standard (DES) packet encryption.
Auth Protocol	(Only for SNMP Version 3 when the security levels **Auth** or **Priv** are selected) Choose the authentication protocol that you want the network device to use from the **Auth Protocol** drop-down list. • **MD5** • **SHA**
Auth Password	(Only for SNMP Version 3 when the **Auth** or **Priv** security levels are selected) Enter the authentication key. It must be at least eight characters in length. Click **Show** to display the authentication password that is already configured for the device. **Note** The caret (circumflex ^) symbol cannot be used.

Field Name	Usage Guidelines
Privacy Protocol	(Only for SNMP Version 3 when **Priv** security level is selected) Choose one of the following options from the **Privacy Protocol** drop-down list: • **DES** • **AES128** • **AES192** • **AES256** • **3DES**
Privacy Password	(Only for SNMP Version 3 when **Priv** security level is selected) Enter the privacy key. Click **Show** to display the privacy password that is already configured for the device. **Note** The caret (circumflex ^) symbol cannot be used.
Polling Interval	Enter the polling interval, in seconds. The default value is 3600.
Link Trap Query	Check the **Link Trap Query** check box to receive and interpret linkup and linkdown notifications that are received through the SNMP trap.
Mac Trap Query	Check the **Link Trap Query** check box to receive and interpret MAC notifications received through the SNMP trap.
Originating Policy Services Node	Choose the Cisco ISE server to be used to poll for SNMP data, from the **Originating Policy Services Node** drop-down list. The default value for this field is **Auto**. Overwrite the setting by choosing a specific value from the drop-down list.

Advanced TrustSec Settings

The following table describes the fields in the **Advanced TrustSec Settings** section.

Table 187: Fields in the Advanced TrustSec Settings Area

Field Name	Usage Guidelines
Device Authentication Settings	
Use Device ID for TrustSec Identification	Check the **Use Device ID for TrustSec Identification** check box if you want the device name to be listed as the device identifier in the **Device ID** field.
Device ID	You can use this field only if you have not checked the **Use Device ID for TrustSec Identification** check box.
Password	Enter the password that you have configured in the Cisco TrustSec device's CLI to authenticate the Cisco TrustSec device. Click **Show** to display the password.
HTTP REST API Settings	

Field Name	Usage Guidelines
Enable HTTP REST API	Check the **Enable HTTP REST API** check box to use the HTTP REST API to provide the required Cisco TrustSec information to the network devices. This enhances the efficiency and ability to download large configurations in a short time as compared to the RADIUS protocol. It also improves reliability by using TCP over UDP.
Username	Enter the username that you have configured in the Cisco TrustSec device's CLI to authenticate the Cisco TrustSec device. The username cannot contain special characters such as space ! % ^ : ; , [{ | }] ` " = < > ?
Password	Enter the password that you have configured in the Cisco TrustSec device's CLI to authenticate the Cisco TrustSec device.
TrustSec Device Notification and Updates	
Device ID	You can use this field only if you have not checked the **Use Device ID for TrustSec Identification** check box.
Password	Enter the password that you have configured in the Cisco TrustSec device's CLI to authenticate the Cisco TrustSec device. Click **Show** to display the password.
Download Environment Data Every <...>	Specify the time interval at which the device must download its environment data from Cisco ISE, by choosing the required values from the drop-down lists in this area. You can choose the time interval in seconds, minutes, hours, days, or weeks. The default value is one day.
Download Peer Authorization Policy Every <...>	Specify the time interval at which the device must download the peer authorization policy from Cisco ISE by choosing the required values from the drop-down lists in this area. You can specify the time interval in seconds, minutes, hours, days, or weeks. The default value is one day.
Reauthentication Every <...>	Specify the time interval at which the device reauthenticates itself against Cisco ISE after the initial authentication, by choosing the required values from the drop-down lists in this area. You can configure the time interval in seconds, minutes, hours, days, or weeks. For example, if you enter 1000 seconds, the device authenticates itself against Cisco ISE every 1000 seconds. The default value is one day.
Download SGACL Lists Every <...>	Specify the time interval at which the device downloads SGACL lists from Cisco ISE, by choosing the required values from the drop-down lists in this area. You can configure the time interval in seconds, minutes, hours, days, or weeks. The default value is one day.
Other TrustSec Devices to Trust This Device (TrustSec Trusted)	Check the **Other TrustSec Devices to Trust This Device** check box to allow all the peer devices to trust this Cisco TrustSec device. If this check box is not checked, the peer devices do not trust this device, and all the packets that arrive from this device are colored or tagged accordingly.

Field Name	Usage Guidelines
Send Configuration Changes to Device	Check the **Send Configuration Changes to Device** check box if you want Cisco ISE to send Cisco TrustSec configuration changes to the Cisco TrustSec device using CoA or CLI (SSH). Click the **CoA** or **CLI (SSH)** radio button, as required. Click the **CoA** radio button if you want Cisco ISE to send the configuration changes to the Cisco TrustSec device using CoA. Click the **CLI (SSH)** radio button if you want Cisco ISE to send the configuration changes to the Cisco TrustSec device using the CLI (using the SSH connection). For more information, see Push Configuration Changes to Non-CoA Supporting Devices, on page 1112.
Send From	From the drop-down list, choose the Cisco ISE node from which the configuration changes must be sent to the Cisco TrustSec device. You can select a PAN or a PSN. If the PSN that you choose is down, the configuration changes are sent to the Cisco TrustSec device using the PAN.
Test Connection	You can use this option to test the connectivity between the Cisco TrustSec device and the selected Cisco ISE node (PAN or PSN).
SSH Key	To use this feature, open an SSHv2 tunnel from Cisco ISE to the network device, and use the device's CLI to retrieve the SSH key. You must copy this key and paste it in the **SSH Key** field for validation. For more information, see SSH Key Validation, on page 1113.
Device Configuration Deployment	
Include this device when deploying Security Group Tag Mapping Updates	Check the **Include this device when deploying Security Group Tag Mapping Updates** check box if you want the Cisco TrustSec device to obtain the IP-SGT mappings using the device interface credentials.
EXEC Mode Username	Enter the username that you use to log in to the Cisco TrustSec device.
EXEC Mode Password	Enter the device password. Click **Show** to view the password. **Note** We recommend that you avoid using the % character in passwords, including in the EXEC modes and Enable mode passwords to avoid security vulnerabilities.
Enable Mode Password	(Optional) Enter the enable password that is used to edit the configuration of the Cisco TrustSec device in privileged EXEC mode. Click **Show** to view the password.
Out Of Band TrustSec PAC	
Issue Date	Displays the issuing date of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device.

Field Name	Usage Guidelines
Expiration Date	Displays the expiration date of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device.
Issued By	Displays the name of the issuer (a Cisco TrustSec administrator) of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device.
Generate PAC	Click the **Generate PAC** button to generate the out-of-band Cisco TrustSec PAC for the Cisco TrustSec device.

Default Network Device Definition Settings

The following table describes the fields in the **Default Network Device** window, with which you configure a default network device that Cisco ISE can use for RADIUS or TACACS+ authentication. Choose one of the following navigation paths:

- **Administration** > **Network Resources** > **Network Devices** > **Default Device**
- **Work Centers** > **Device Administration** > **Network Resources** > **Default Devices**

Table 188: Fields in the Default Network Device Window

Field Name	Usage Guidelines
Default Network Device Status	Choose **Enable** from the **Default Network Device Status** drop-down list to enable the default network device definition. **Note** If the default device is enabled, you must enable either the RADIUS or the TACACS+ authentication settings by checking the relevant check box in the window.
Device Profile	Displays **Cisco** as the default device vendor.
RADIUS Authentication Settings	
Enable RADIUS	Check the **Enable RADIUS** check box to enable RADIUS authentication for the device.
RADIUS UDP Settings	
Shared Secret	Enter a shared secret. The shared secret can be up to 127 characters in length. The shared secret is the key that you have configured on the network device using the **radius-host** command with the **pac** keyword. **Note** The length of the shared secret must be equal to or greater than the value configured in the **Minimum RADIUS Shared Secret Length** field in the **Device Security Settings** window (**Administration** > **Network Resources** > **Network Devices** > **Device Security Settings**). By default, this value is four characters for new installations and upgraded deployments. For the RADIUS server, the best practice is to have 22 characters.
RADIUS DTLS Settings	

Field Name	Usage Guidelines
DTLS Required	If you check the **DTLS Required** check box, Cisco ISE processes only the DTLS requests from this device. If this option is disabled, Cisco ISE processes both UDP and DTLS requests from this device. RADIUS DTLS provides improved security for SSL tunnel establishment and RADIUS communication.
Shared Secret	Displays the shared secret that is used for RADIUS DTLS. This value is fixed and is used to compute the MD5 integrity checks.
Issuer CA of ISE Certificates for CoA	Choose the certificate authority to be used for RADIUS DTLS CoA from the **Issuer CA of ISE Certificates for CoA** drop-down list.
General Settings	
Enable KeyWrap	(Optional) Check the **Enable KeyWrap** check box only if KeyWrap algorithms are supported on the network device, which increases RADIUS security through an AES KeyWrap algorithm.
Key Encryption Key	Enter an encryption key to be used for session encryption (secrecy) when you enable KeyWrap.
Message Authenticator Code Key	Enter the key that is used for keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages when you enable KeyWrap.
Key Input Format	Choose one of the following formats by clicking the corresponding radio button, and enter values in the **Key Encryption Key** and **Message Authenticator Code Key** fields: • **ASCII**: The **Key Encryption Key** must be 16 characters (bytes) in length, and the **Message Authenticator Code Key** must be 20 characters (bytes) in length. • **Hexadecimal**: The **Key Encryption Key** must be 32 bytes in length, and the **Message Authenticator Code Key** must be 40 bytes in length. Specify the key input format that you want to use to enter the Key Encryption Key and Message Authenticator Code Key so that it matches the configuration on the network device. The value that you specify must be the correct (full) length for the key. Shorter values are not permitted.
TACACS Authentication Settings	
Shared Secret	Enter a string of text to assign to a network device when the TACACS+ protocol is enabled. Note that a user must enter the text before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
Retired Shared Secret is Active	Displayed when the retirement period is active.

Field Name	Usage Guidelines
Retire	Retires an existing shared secret instead of ending it. When you click **Retire**, a dialog box is displayed. Click **Yes** or **No**.
Remaining Retired Period	(Optional) Available only if you click **Yes** in the **Retire** dialog box. Displays the default value that is specified in the **Work Centers** > **Device Administration** > **Settings** > **Connection Settings** > **Default Shared Secret Retirement Period** window. You can change the default values. This allows a new shared secret to be entered. The old shared secret remains active for the specified number of days.
End	(Optional) Available only if you select **Yes** in the **Remaining Retired Period** dialog box. Ends the retirement period and terminates the old shared secret.
Enable Single Connect Mode	Check the **Enable Single Connect Mode** check box to use a single TCP connection for all TACACS+ communication with the network device. Click one of the following the radio buttons: • **Legacy Cisco Devices** • **TACACS Draft Compliance Single Connect Support**. **Note** If you disable this field, Cisco ISE uses a new TCP connection for every TACACS+ request.

Device Security Settings

Specify the minimum length for the RADIUS shared secret. For new installation and upgraded deployment, by default, this value is 4 characters. For the RADIUS server, best practice is to have 22 characters.

Note The length of the shared secret entered in the Network Devices page must be equal to or greater than the value configured in the Minimum RADIUS Shared Secret Length field in the Device Security Settings page.

Related Topics

Network Device Definition Settings, on page 905

Network Device Import Settings

The following table describes the fields in the **Import Network Devices** window, which you can use to import network device details into Cisco ISE. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Devices**. In the **Network Devices** window, click **Import**.

Table 189: Import Network Devices Settings

Field Name	Usage Guidelines
Generate a Template	Click **Generate a Template** to create a comma-separated value (CSV) template file. Update the template with network devices information in the CSV format and save it locally. Then, use the edited template to import network devices into any Cisco ISE deployment.
File	Click **Choose File** to choose the CSV file that you have recently created, or previously exported from a Cisco ISE deployment. You can import network devices into another Cisco ISE deployment with new and updated network devices information, by using the **Import** option.
Overwrite Existing Data with New Data	Check the **Overwrite Existing Data with New Data** check box to replace the existing network devices with the devices in your import file. If you do not check this check box, new network device definitions that are available in the import file are added to the network device repository. Duplicate entries are ignored.
Stop Import on First Error	Check the **Stop Import on First Error** check box if you want Cisco ISE to discontinue import when it encounters an error during import. Cisco ISE imports network devices until the time of an error. If this check box is not checked and an error is encountered, the error is reported and Cisco ISE continues to import the remaining devices.

Manage Network Device Groups

The following windows enable you to configure and manage network device groups.

Network Device Group Settings

The following table describes the fields in the **Network Device Groups** window that you use to create network device groups. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Device Groups** > **All Groups**.

You can also create network device groups in the **Work Centers** > **Device Administration** > **Network Resources** > **Network Device Groups** > **All Groups** window.

Table 190: Fields in the Network Device Group Window

Field Name	Usage Guidelines
Name	Enter a name for the root network device group. For all subsequent child network device groups added to this root network device group, enter the name of this newly created network device group. You can have a maximum of six nodes in a network device group hierarchy, including the root node. Each network device group name can have a maximum of 32 characters.
Description	Enter a description for the root or the child network device group.

Field Name	Usage Guidelines
No. of Network Devices	The number of network devices in the network group is displayed in this column.

Network Device Group Import Settings

The following table describes the fields in the **Import** dialog box in the **Network Device Group** window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Device Groups**.

Table 191: Fields in the Network Device Groups Import Window

Field Name	Usage Guidelines
Generate a Template	Click this link to download a CSV template file. Update the template with network device group information in the same format. Save the template locally to import the network device groups into any Cisco ISE deployment.
File	Click **Choose File** and navigate to the location of the CSV file that you want to upload. The file may be new or a file that was exported from another Cisco ISE deployment. You can import network device groups from one Cisco ISE deployment to another, with new and updated network device groups information.
Overwrite Existing Data with New Data	Check this check box if you want to replace the existing network device groups with the device groups in your import file. If you do not check this check box, only the new network device groups in the import file are added to the network device group repository. Duplicate entries are ignored.
Stop Import on First Error	Check this check box to discontinue import at the first instance of encountering an error during the import. If this check box is not checked and an error is encountered, Cisco ISE reports the error and continues importing the rest of the device groups.

Network Device Profiles Settings

The following table describes the fields on the Network Device Profiles window, which you can use to configure the default settings for a type of network device from a specific vendor, such as the device's support for protocols, redirect URLs, and CoA settings. You then use the profile to define specific network devices.

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **Network Device Profiles**.

Network Device Profile Settings

The following table describes the fields in the Network Device Profile section.

Table 192: Network Device Profile Settings

Field Name	Description
Name	Enter a name for the network device profile.
Description	Enter the description for the network device profile.
Icon	Select the icon to use for the network device profile. This icon will default to the icon for the vendor that you select. The icon you select must be a 16 x 16 PNG file.
Vendor	Select the vendor of the network device profile.
Supported Protocols	
RADIUS	Check this check box if this network device profile supports RADIUS.
TACACS+	Check this check box if this network device profile supports TACACS+.
TrustSec	Check this check box if this network device profile supports TrustSec.
RADIUS Dictionaries	Select one or more RADIUS dictionaries supported by this profile. Import any vendor-specific RADIUS dictionaries before you create the profile.

Authentication/Authorization Template Settings

The following table describes the fields in the Authentication/Authorization section.

Table 193: Authentication/Authorization Settings

Field Name	Description
Flow Type Conditions	Cisco ISE supports 802.1X, MAC authentication bypass (MAB), and browser-based Web authentication login for basic user authentication and access via both wired and wireless networks. Check the check boxes for the authentication logins that this type of network device supports. It could be one or more of the following: • Wired MAC authentication bypass (MAB) • Wireless MAB • Wired 802.1X • Wireless 802.1X • Wired Web Authentication • Wireless Web Authentication After you check the authentication logins that the network device profile supports, specify the conditions for the login.

Field Name	Description
Attribute Aliasing	Check the SSID check box to use the device's Service Set Identifier (SSID) as the friendly name in policy rules. This allows you to create a consistent name to use in policy rules.
Host Lookup (MAB)	
Process Host Lookup	Check this check box to define the protocols for host lookup used by the network device profile. Network devices from different vendors perform MAB authentication differently. Depending on the device type, check the **Check Password** or **Checking Calling-Station-Id equals MAC Address** check box, or both, for the protocol you are using.
Via PAP/ASCII	Check this check box to configure Cisco ISE to detect a PAP request from the network device profile as a Host Lookup request.
Via CHAP	Check this check box to configure Cisco ISE to detect this type of request from the network devices as a Host Lookup request. This option enables CHAP authentication. CHAP uses a challenge-response mechanism with password encryption. CHAP does not work with Microsoft Active Directory.
Via EAP-MD5	Check this check box to enable EAP-based MD5 hashed authentication for the network device profile.

Permissions

You can define the VLAN and ACL permissions that will be used for this network device profile. After the profile is saved, Cisco ISE automatically generates authorization profiles for each configured permission.

Table 194: Permissions

Field Name	Description
Set VLAN	Check this check box to set the VLAN permissions for this network device profile. Choose of the following options: • IETF 802.1X Attributes. This is a set of default RADIUS attributes defined by the Internet Engineering Task Force. • Unique Attributes. You can specify multiple RADIUS attribute-value pairs.
Set ACL	Check this check box to select the RADIUS attribute to set for the ACL on the network device profile.

Change of Authorization (CoA) Template Settings

This template defines how the CoA is sent to this type of network device. The following table describes the fields in the Change of Authorization (CoA) section.

Table 195: Change of Authorization (CoA) Settings

Field Name	Definition
CoA by	Select one of the following options: • RADIUS • SNMP • Not supported
CoA by RADIUS	
Default CoA Port	The port to send the RADIUS CoA. By default, this is port 1700 for Cisco devices and port 3799 for devices from a non-Cisco vendor. You can override this on the Network Device window.
Timeout Interval	The number of seconds that Cisco ISE waits for a response after sending the CoA.
Retry Count	The number of times Cisco ISE attempts to send the CoA after the first timeout.
Disconnect	Select how to send a disconnect request to these devices. • **RFC 5176**: Check this check box for a standard session termination and leave the port ready for a new session, as defined per RFC 5176. • **Port Bounce**: Check this check box to terminate the session and restart the port. • **Port Shutdown**: Check this check box to terminate the session and shutdown the port.
Re-authenticate	Select how to send a reauthentication request to the network devices. This is currently supported only by Cisco devices. • **Basic**: Check this check box for a standard session reauthentication. • **Rerun**: Check this check box to run through the authentication method from the beginning. • **Last**: Use the last successful authentication method for the session.
CoA Push	If the network devices do not support Cisco's TrustSec CoA feature, select this option to allow Cisco ISE to push a configuration change to the device.
CoA by SNMP	
Timeout Interval	The number of seconds that Cisco ISE waits for a response after sending the CoA.
Retry Count	The number of times that Cisco ISE attempts to send a CoA.
NAD Port Detection	Relevant RADIUS attribute is currently the only option.

Field Name	Definition
Relevant RADIUS Attribute	Select how to detect the NAD port: • Nas-Port • Nas-Port-ID
Disconnect	Select how to send a disconnect request to these devices: • **Reauthenticate**: Check this check box to terminate the session and restart the port. • **Port Bounce**: Check this check box to terminate the session and restart the port. • **Port Shutdown**: Check this check box to terminate the session and shutdown the port.

Redirect Template Settings

The network devices can redirect a client's HTTP requests if it's configured as part of the authorization profile. This template specifies whether this network device profile supports URL redirect. You will use the URL parameter names specific to the device type.

The following table describes the fields in the Redirect section.

Table 196: Redirect Settings

Field Name	Definition
Type	Select whether the network device profile supports a static or dynamic URL redirect. If your device supports neither, select **Not Supported** and set up a VLAN from **Settings** > **DHCP & DNS Services** .
Redirect URL Parameter Names	
Client IP Address	Enter the parameter name that the network devices use for a client's IP address.
Client MAC Address	Enter the parameter name that the network devices use for a client's MAC address.
Originating URL	Enter the parameter name that the network devices use for the originating URL.
Session ID	Enter the parameter name that the network devices use for the session ID.
SSID	Enter the parameter name that the network devices use for the Service Set Identifier (SSID).
Dynamic URL Parameters	
Parameter	When you select to use a Dynamic URL for redirection, you will need to specify how these network devices create the redirect URL. You can also specify whether the redirect URL uses the session ID or client MAC address.

Advanced Settings

You can use the Network Device Profile to generate a number of policy elements to make it easy to use a network device in policy rules. These elements include compound conditions, authorization profiles, and allowed protocols.

Click **Generate Policy Elements** to create these elements.

External RADIUS Server Settings

The following table describes the fields on the External RADIUS Server window, which you can use to configure a RADIUS server. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **External RADIUS Servers**.

Table 197: External RADIUS Server Settings

Field Name	Usage Guidelines
Name	Enter the name of the external RADIUS server.
Description	Enter a description of the external RADIUS server.
Host IP	Enter the IP address of the external RADIUS server. When entering an IPv4 address, you can use ranges and subnet masks. Ranges are not supported for IPv6.
Shared Secret	Enter the shared secret between Cisco ISE and the external RADIUS server that is used for authenticating the external RADIUS server. A shared secret is an expected string of text that a user must provide to enable the network device to authenticate a username and password. The connection is rejected until the user supplies the shared secret. The shared secret can be up to 128 characters in length.
Enable KeyWrap	Enable this option to increase the RADIUS protocol security via an AES KeyWrap algorithm, to help enable FIPS 140 compliance in Cisco ISE.
Key Encryption Key	(Only if you check the Enable Key Wrap check box) Enter a key to be used for session encryption (secrecy).
Message Authenticator Code Key	(Only if you check the Enable Key Wrap check box) Enter a key to be used for keyed HMAC calculation over RADIUS messages.
Key Input Format	Specify the format you want to use to enter the Cisco ISE encryption key, so that it matches the configuration that is available on the WLAN controller. The value you specify must be the correct (full) length for the key as defined below (shorter values are not permitted). • ASCII: The Key Encryption Key must be 16 characters (bytes) long, and the Message Authenticator Code Key must be 20 characters (bytes) long. • Hexadecimal: The Key Encryption Key must be 32 bytes long, and the Message Authenticator Code Key must be 40 bytes long.
Authentication Port	Enter the RADIUS authentication port number. The valid range is from 1 to 65535. The default is 1812.

Field Name	Usage Guidelines
Accounting Port	Enter the RADIUS accounting port number. The valid range is from 1 to 65535. The default is 1813.
Server Timeout	Enter the number of seconds that the Cisco ISE waits for a response from the external RADIUS server. The default is 5 seconds. Valid values are from 5 to 120.
Connection Attempts	Enter the number of times that the Cisco ISE attempts to connect to the external RADIUS server. The default is 3 attempts. Valid values are from 1 to 9.
RADIUS Proxy Failover Expiration	Enter the amount of time to elapse after the connection has failed and until a connection to this server is attempted again. Valid range is from 1 to 600. Configure this parameter to skip the server timeout and go straight to failover.

RADIUS Server Sequences

The following table describes the fields on the RADIUS Server Sequences window, which you can use to create a RADIUS server sequence. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **RADIUS Server Sequences > Add**.

Table 198: RADIUS Server Sequences

Field Name	Usage Guidelines
Name	Enter the name of the RADIUS server sequence.
Description	Enter an optional description.
Host IP	Enter the IP address of the external RADIUS server.
User Selected Service Type	Choose the external RADIUS servers that you want to use as policy servers from the Available list box and move them to the Selected list box.
Remote Accounting	Check this check box to enable accounting in the remote policy server.
Local Accounting	Check this check box to enable accounting in Cisco ISE.
Advanced Attribute Settings	
Strip Start of Subject Name up to the First Occurrence of the Separator	Check this check box to strip the username from the prefix. For example, if the subject name is acme\userA and the separator is \, the username becomes userA.

Field Name	Usage Guidelines
Strip End of Subject Name from the Last Occurrence of the Separator	Check this check box to strip the username from the suffix. For example, if the subject name is userA@abc.com and the separator is @, the username becomes userA. • You must enable the strip options to extract the username from NetBIOS or User Principle Name (UPN) format usernames (user@domain.com or /domain/user), because only usernames are passed to the RADIUS server for authenticating the user. • If you activate both the \ and @ stripping functions, and you are using AnyConnect, Cisco ISE does not accurately trim the first \ from the string. However, each stripping function that is used individually, works as it is designed with AnyConnect.
Modify Attributes in the Request to the External RADIUS Server	Check this check box to allow Cisco ISE to manipulate attributes that come from or go to the authenticated RADIUS server. The attribute manipulation operations include these: • **Add**: Add additional attributes to the overall RADIUS request/response. • **Update**: Change the attribute value (fixed or static) or substitute an attribute by another attribute value (dynamic). • **Remove**: Remove an attribute or an attribute-value pair. • **RemoveAny**: Remove any occurrences of the attribute.
Continue to Authorization Policy	Check this check box to divert the proxy flow to run the authorization policy for further decision making, based on identity store group and attribute retrieval. If you enable this option, attributes from the response of the external RADIUS server will be applicable for the authentication policy selection. Attributes that are already in the context will be updated with the appropriate value from the AAA server accept response attribute.
Modify Attributes before send an Access-Accept	Check this check box to modify the attribute just before sending a response back to the device.

NAC Manager Settings

The following table describes the fields on the New NAC Managers window, which you can use to add a NAC Manager. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **NAC Managers**.

Table 199: NAC Manager Settings

Fields	Usage Guidelines
Name	Enter the name of the Cisco Access Manager (CAM).

Fields	**Usage Guidelines**
Status	Click the Status check box to enable REST API communication from the Cisco ISE profiler that authenticates connectivity to the CAM.
Description	Enter the description of the CAM.
IP Address	Enter the IP address of the CAM. Once you have created and saved a CAM in Cisco ISE, the IP address of the CAM cannot be edited. You cannot use 0.0.0.0 and 255.255.255.255, as they are excluded when validating the IP addresses of the CAMs in Cisco ISE, and so, they are not valid IP addresses that you can use in the IP Address field for the CAM. **Note** You can use the virtual service IP address that a pair of CAMs share in a high-availability configuration. This allows a failover support of CAMs in a high-availability configuration.
Username	Enter the username of the CAM administrator that allows you to log on to the user interface of the CAM.
Password	Enter the password of the CAM administrator that allows you to log on to the user interface of the CAM.

Device Portal Management

Configure Device Portal Settings

Portal Identification Settings for Device Portals

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Managment** > **Blocked List Portal, Client Provisioning Portals, BYOD Portals, MDM Portals, or My Device Portals** > **Create, Edit or Duplicate** > **Portals Settings and Customization**.

- **Portal Name**: Enter a unique portal name to access this portal. Do not use this portal name for any other Sponsor, Guest, or nonguest portals, such as Blocked List, Bring Your Own Device (BYOD), Client Provisioning, Mobile Device Management (MDM), or My Devices portals.

  This name appears in the authorization profile portal selection for redirection choices. It is applied to the list of portals for easy identification among other portals.

- **Description**: Optional.

- **Portal Test URL**: A system-generated URL displays as a link after you click **Save**. Use it to test the portal.

  Click the link to open a new browser tab that displays the URL for this portal. Policy Services Node (PSN) with Policy Services must be turned on. If Policy Services are disabled, the PSN only displays the Admin portal.

Note The test portal does not support RADIUS sessions, so you won't see the entire portal flow for all portals. BYOD and Client Provisioning are examples of portals that depend on RADIUS sessions. For example, a redirect to an external URL will not work. If you have more than one PSN, Cisco ISE chooses the first active PSN.

- **Language File**: Each portal type supports 15 languages by default, which are available as individual properties files bundled together in a single zipped language file. Export or import the zipped language file to use with the portal. The zipped language file contains all the individual language files that you can use to display text for the portal.

  The language file contains the mapping to the particular browser locale setting along with all of the string settings for the entire portal in that language. A single language file contains all the supported languages, so that it can easily be used for translation and localization purposes.

  If you change the browser locale setting for one language, the change is applied to all the other end-user web portals. For example, if you change the French.properties browser locale from fr,fr-fr,fr-ca to fr,fr-fr in the Hotspot Guest portal, the changes also apply to the My Devices portal.

  An alert icon displays when you customize any of the text on the **Portal Page Customizations** tab. The alert message reminds you that any changes made to one language while customizing the portal must also be added to all the supported languages properties files. You can manually dismiss the alert icon using the drop-down list option; or it is automatically dismissed after you import the updated zipped language file.

Portal Settings for BYOD and MDM Portals

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **BYOD Portals or MDM Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Portal Settings**.

Configure these settings to define portal page operations.

- **HTTPS Port**: Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blocked List Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you modify this window. If you modify this window, update the port setting to comply with this restriction.

  If you assign ports used by a non-guest (such as My Devices) portal to a guest portal, an error message appears.

  For posture assessments and remediation only, the Client Provisioning portal also uses ports 8905 and 8909. Otherwise, it uses the same ports assigned to the Guest portal.

  Portals assigned to the same HTTPS port can use the same Gigabit Ethernet interface or another interface. If they use the same port and interface combination, they must use the same certificate group tag. For example:

  - Valid combinations include, using the Sponsor portal as an example:
    - Sponsor portal: Port **8443**, Interface **0**, Certificate tag **A** and My Devices portal: Port **8443**, Interface **0**, Certificate group **A**.

        - Sponsor portal: Port **8443**, Interface **0**, Certificate group **A** and My Devices portal: Port **8445**, Interface **0**, Certificate group **B**.
        - Sponsor portal: Port **8444**, Interface **1**, Certificate group **A** and Blocked List portal: Port **8444**, Interface **0**, Certificate group **B**.

    - Invalid combinations include:
        - Sponsor portal: Port **8443**, Interface **0**, Certificate group **A** and My Devices portal: **8443**, Interface **0**, Certificate group **B**.
        - Sponsor portal: Port **8444**, Interface **0**, Certificate tag **A** and Blocked List portal: Port **8444**, Interface **0**, Certificate group **A**.

> **Note** We recommend that you use interface 0 for Guest services for best performance. You can either configure only interface 0 in the **Portal Settings**, or you can use the CLI command **ip host** to map a hostname or FQDN to the IP address of interface 0.

- **Allowed Interfaces**: Select the PSN interfaces which a PAN can use to run a portal. When a request to open a portal is made on the PAN, the PAN looks for an available allowed port on the PSN. You must configure the Ethernet interfaces using IP addresses on different subnets.

  These interfaces must be available on all the PSNs, including VM-based ones, that have Policy Services turned on. This is a requirement because any of these PSNs can be used for the redirect at the start of the guest session.

    - The Ethernet interfaces must use IP addresses on different subnets.
    - The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
    - The portal certificate Subject Name or Alternate Subject Name must resolve to the interface IP address.
    - Configure **ip host x.x.x.x yyy.domain.com** in Cisco ISE CLI to map the secondary interface IP address to the FQDN, which is used to match the certificate Subject Name or Alternate Subject Name.
    - If only the bonded NIC is selected, when the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN logs an error and exits. The PSN will not try to start the portal on the physical interface.
    - NIC Teaming or bonding is a configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based in the **Portal Settings** configuration. If both physical NICs and the corresponding bonded NIC are configured, when the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.

- **Certificate Group tag**: Pick a certificate group tag that specifies the certificate to be used for the portal’s HTTPS traffic.
- **Endpoint Identity Group**: Choose an endpoint identity group to track guest devices. Cisco ISE provides the **GuestEndpoints** endpoint identity group to use as a default. You can also create more endpoint identity groups if you choose to not use the default.

  Choose an endpoint identity group to track employee devices. Cisco ISE provides the **RegisteredDevices** endpoint identity group to use as a default. You can also create more endpoint identity groups if you choose to not use the default.
- **Display Language**
  - **Use Browser Locale**: Use the language specified in the client browser's locale setting as the display language of the portal. If browser locale's language is not supported by Cisco ISE, then the **Fallback Language** is used as the language portal.
  - **Fallback Language**: Choose the language to use when the language cannot be obtained from the browser locale, or if the browser locale language is not supported by Cisco ISE.
  - **Always Use**: Choose the display language to use for the portal. This setting overrides the **User Browser Locale** option.

BYOD Settings for BYOD Portals

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **BYOD Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **BYOD Settings**.

Use these settings to enable Bring Your Own Device (BYOD) functionality for employees who want to use their personal devices to access your corporate network.

Field Name	Usage Guidelines
Include an AUP (on page/as link)	Display your company’s network-usage terms and conditions, either as text on the window currently being displayed for the user or as a link that opens a new tab or window with AUP text.
Require Acceptance	Require users to accept an AUP before their account is fully enabled. The **Login** button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not obtain network access.
Require scrolling to end of AUP	This option displays only if **Include an AUP on page** is enabled. Ensure that the user has read the AUP completely. The **Accept** button is enabled only after the user has scrolled to the end of the AUP.
Display Device ID Field During Registration	Display the device ID to the user during the registration process, even though the device ID is pre-configured and cannot be changed while using the BYOD portal.

Field Name	**Usage Guidelines**
Originating URL	After successfully authenticating to the network, redirect the user’s browser to the original website that the user is trying to access, if available. If not available, the Authentication Success window appears. Make sure that the redirect URL is allowed to work on port 8443 of the PSN by the access-control list on the NAD and by authorization profiles configured in Cisco ISE for that NAD. For Windows, MAC, and Android devices, control is given to the Self-Provisioning Wizard app, which does provisioning. Therefore, these devices are not redirected to the originating URL. However, iOS (dot1X) and unsupported devices (that are allowed network access) are redirected to this URL.
Success page	Display a page indicating that the device registration was successful.
URL	After successfully authenticating to the network, redirect the user's browser to the specified URL, such as your company’s website.

Note If you redirect a Guest to an external URL after authentication, there may be a delay while the URL address is resolved and the session is redirected.

Portal Settings for Certificate Provisioning Portal

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Certificate Provisioning Portal** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Portal Settings**.

- **HTTPS Port**: Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blocked List Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you modify this window. If you modify this window, update the port setting to comply with this restriction.

  If you assign ports used by a non-guest (such as My Devices) portal to a guest portal, an error message appears.

  For posture assessments and remediation only, the Client Provisioning portal also uses ports 8905 and 8909. Otherwise, it uses the same ports assigned to the Guest portal.

  Portals assigned to the same HTTPS port can use the same Gigabit Ethernet interface or another interface. If they use the same port and interface combination, they must use the same certificate group tag. For example:

  - Valid combinations include, using the Sponsor portal as an example:
    - Sponsor portal: Port **8443**, Interface **0**, Certificate tag **A** and My Devices portal: Port **8443**, Interface **0**, Certificate group **A**.
    - Sponsor portal: Port **8443**, Interface **0**, Certificate group **A** and My Devices portal: Port **8445**, Interface **0**, Certificate group **B**.
    - Sponsor portal: Port **8444**, Interface **1**, Certificate group **A** and Blocked List portal: Port **8444**, Interface **0**, Certificate group **B**.

  - Invalid combinations include:
    - Sponsor portal: Port **8443**, Interface **0**, Certificate group **A** and My Devices portal: **8443**, Interface **0**, Certificate group **B**.
    - Sponsor portal: Port **8444**, Interface **0**, Certificate tag **A** and Blocked List portal: Port **8444**, Interface **0**, Certificate group **A**.

Note We recommend that you use interface 0 for Guest services for best performance. You can either configure only interface 0 in the **Portal Settings**, or you can use the CLI command **ip host** to map a hostname or FQDN to the IP address of interface 0.

- **Allowed Interfaces**: Select the PSN interfaces which a PAN can use to run a portal. When a request to open a portal is made on the PAN, the PAN looks for an available allowed port on the PSN. You must configure the Ethernet interfaces using IP addresses on different subnets.

  These interfaces must be available on all the PSNs, including VM-based ones, that have Policy Services turned on. This is a requirement because any of these PSNs can be used for the redirect at the start of the guest session.

  - The Ethernet interfaces must use IP addresses on different subnets.
  - The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
  - The portal certificate Subject Name or Alternate Subject Name must resolve to the interface IP address.
  - Configure **ip host x.x.x.x yyy.domain.com** in Cisco ISE CLI to map the secondary interface IP address to the FQDN, which is used to match the certificate Subject Name or Alternate Subject Name.
  - If only the bonded NIC is selected, when the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN logs an error and exits. The PSN will not try to start the portal on the physical interface.
  - NIC Teaming or bonding is a configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based in the **Portal Settings** configuration. If both physical NICs and the corresponding bonded NIC are configured, when the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.

- **Certificate Group tag**: Pick a certificate group tag that specifies the certificate to be used for the portal's HTTPS traffic.

- **Authentication Method**: Choose which identity source sequence or Identity Provider (IdP) to use for user authentication. The identity source sequence is a list of identity stores that are searched in sequence to verify user credentials.

  Cisco ISE includes a default identity source sequence for sponsor portals, Sponsor_Portal_Sequence.

  To configure IdP, choose **Administration** > **Identity Management** > **External Identity Sources** > **SAML Id Providers**.

  To configure an identity source sequence, choose **Administration > Identity Management > Identity Source Sequences**.

- **Configure authorized groups**: Choose the user identity groups to which you want to grant permission to generate certificates and move them to the Chosen box.

- **Fully Qualified Domain Name (FQDN)**: Enter at least one unique FQDN or hostname for the Sponsor or MyDevices portal. For example, you can enter `sponsorportal.yourcompany.com,sponsor`, so that when the user enters either of those into a browser, the sponsor portal displays. Separate names with commas, but do not include spaces between entries.

  If you change the default FQDN, then also do the following:

  - Update your DNS so that the FQDN of the new URL resolves to a valid Policy Services Node (PSN) IP address. Optionally, this address could point to a load balancer virtual IP address that serves a pool of PSNs.

  - To avoid certificate warning messages due to name mismatches, include the FQDN of the customized URL, or a wildcard, in the subject alternative name (SAN) attribute of the local server certificate of the Cisco ISE PSN. If the **Allow Kerberos SSO** option is enabled for the sponsor portal, you must include the FQDN of the Cisco ISE PSN, or a wildcard, in the SAN attribute of the local server certificate used by the portal.

- **Idle Timeout**: Enter the time in minutes that you want Cisco ISE to wait before it logs out the user if there is no activity in the portal. The valid range is from 1 to 30 minutes.

Login Page Settings

- **Maximum Failed Login Attempts Before Rate Limiting**: Specify the number of failed login attempts from a single browser session before Cisco ISE starts to throttle that account. This does not cause an account lockout. The throttled rate is configured in **Time between login attempts when rate limiting**.

- **Include an AUP**: Add a acceptable use policy window to the flow. You can add the AUP to the window, or link to another window.

Acceptable Use Policy (AUP) Page Settings

- **Include an AUP Page**: Display your company's network-usage terms and conditions on a separate page to the user.

- **Use Different AUP for Employees**: Display a different AUP and network-usage terms and conditions for employees only. If you choose this option, you cannot also choose **Skip AUP for employees**.

- **Skip AUP for Employees**: Employees are not required to accept an AUP before accessing the network. If you choose this option, you cannot also choose **Use different AUP for employees**.

- **Require Acceptance**: Require users to accept an AUP before their account is fully enabled. The **Login** button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not obtain network access.
- **Require Scrolling to End of AUP**: This option displays only if **Include an AUP on page** is enabled.

  Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP. Configure when the AUP appears to the user.

  - **On First Login only**: Display an AUP the first time the user logs into the network or portal.
  - **On Every Login**: Display an AUP every time the user logs into the network or portal.
  - **Every __ Days (starting at first login)**: Display an AUP periodically after the user first logs into the network or portal.

Portal Settings for Client Provisioning Portals

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Client Provisioning Portals** > **Create, Edit, Duplicate, or Delete** > **Portal Behavior and Flow Settings**.

Portal Settings

- **HTTPS Port**: Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the **Blocked List** Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you make any change to this page. If you make any change to this page, you must update the port setting to comply with this restriction.
- **Allowed Interfaces**: Select the PSN interfaces which can run a portal. Only a PSN with an available allowed interface on a PSN can create a portal. You can configure any combination of physical and bonded interfaces. This is a PSN-wide configuration; all portals can only run on these interfaces, this interface configuration is pushed to all the PSNs.
  - You must configure the Ethernet interfaces using IP addresses on different subnets.
  - The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
  - The portal certificate Subject Name/Alternate Subject Name must resolve to the interface IP.
  - Configure ip host x.x.x.x yyy.domain.com in ISE CLI to map secondary interface IP to FQDN, which will be used to match Certificate Subject Name/Alternate Subject Name.
  - If only the bonded NIC is selected, when the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond set upon that PSN, then the PSN logs an error and exits. It will NOT attempt to start the portal on the physical interface.
  - **NIC Teaming** or bonding is an O/S configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based on the portal settings configuration:
    - If both physical NICs and the corresponding bonded NIC are configured - When the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not

successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.

- **Certificate Group Tag**: Select the group tag of the certificate group to use for the portal’s HTTPS traffic.
- **Authentication Method**: Choose which identity source sequence (ISS) or Identity Provider (IdP) to use for user authentication. The ISS is a list of Identity Stores that are searched in sequence to verify user credentials. Some examples include: Internal Guest Users, Internal Users, Active Directory, and LDAP.

  Cisco ISE includes a default client provisioning Identity Source Sequence for Client Provisioning Portals, Certificate_Request_Sequence.
- **Fully Qualified Domain Name (FQDN)**: Enter at least one unique FQDN and/or hostname for your Client Provisioning portal. For example, you can enter provisionportal.yourcompany.com, so that when the user enters either of those into a browser, they will reach the Client Provisioning Portal.
  - Update DNS to ensure that the FQDN of the new URL resolves to a valid Policy Services Node (PSN) IP address. Optionally, this address could point to a load balancer virtual IP address that serves a pool of PSNs.
  - To avoid certificate warning messages due to name mismatches, include the FQDN of the customized URL, or a wildcard, in the subject alternative name (SAN) attribute of the local server certificate of the Cisco ISE PSN.

Note For Client Provisioning without URL redirection, the portal name that is entered in the Fully Qualified Domain Name (FQDN) field must be configured in the DNS configuration. This URL must be communicated to the users to enable Client Provisioning without URL redirection.

- **Idle Timeout**: Enter the time in minutes that you want Cisco ISE to wait before it logs out the user if there is no activity in the portal. The valid range is from 1 to 30 minutes..

Note In the Client Provisioning Portal, you can define the port number and the certificate so that the host allows you to download the same certificate for Client Provisioning and Posture. If the portal certificate is signed by the officials certificate authority, you will not receive any security warning. If the certificate is self-signed, you will receive one security warning for both the portals and Cisco AnyConnect Posture component.

Login Page Settings

- Enable Login: Select this check box to enable the login step in the Client Provisioning Portal
- Maximum failed login attempts before rate limiting: Specify the number of failed login attempts from a single browser session before Cisco ISE starts to artificially slow down the rate at which login attempts can be made, preventing additional login attempts. The time between attempts after this number of failed logins is reached is specified in **Time between login attempts when rate limiting**.

- Time between login attempts when rate limiting: Set the length of time in minutes that a user must wait before attempting to log in again, after failing to log in the number of times defined in **Maximum failed login attempts before rate limiting**.
- Include an AUP (on page/as link): Display your company’s network-usage terms and conditions, either as text on the page currently being displayed for the user or as a link that opens a new tab or window with AUP text.
- Require acceptance: Require users to accept an AUP before they can access the portal. The **Login** button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not be able to access the portal.
- Require scrolling to end of AUP: This option displays only if **Include an AUP on page** is enabled. Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP.

Acceptable Use Policy (AUP) Page Settings

- Include an AUP: Display your company’s network-usage terms and conditions on a separate page to the user.
- Require scrolling to end of AUP: Ensure that the user has read the AUP completely. The Accept button activates only after the user has scrolled to the end of the AUP.
- On first login only: Display an AUP when the user logs into the network or portal for the first time only.
- On every login: Display an AUP each time the user logs into the network or portal.
- Every ______ days (starting at first login): Display an AUP periodically after the user first logs into the network or portal.

Post-Login Banner Page Settings

Include a Post-Login Banner page: Display additional information after the users successfully log in and before they are granted network access.

Change Password Settings

Allow internal users to change their own passwords: Allow employees to change their passwords after they log in to the Client Provisioning Portal. This only applies to employees whose accounts are stored in the Cisco ISE database and not to those stored in external databases, such as Active Directory or LDAP.

Employee Mobile Device Management Settings for MDM Portals

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **MDM Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Employee Mobile Device Management Settings**.

Use these settings to enable Mobile Device Management (MDM) functionality for employees using the MDM portals and define their AUP experience.

Field Name	Usage Guidelines
Include an AUP (on page/as link)	Display your company's network-usage terms and conditions, either as text on the window currently being displayed for the user or as a link that opens a new tab or window with AUP text.
Require Acceptance	Require users to accept an AUP before their account is fully enabled. The **Login** button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not obtain network access.
Require scrolling to end of AUP	This option displays only if **Include an AUP on page** is enabled. Ensure that the user has read the AUP completely. The **Accept** button is enabled only after the user has scrolled to the end of the AUP.

Portal Settings for My Devices Portals

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **My Devices Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Portal Settings**.

- **HTTPS Port**: Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blocked List Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you modify this window. If you modify this window, update the port setting to comply with this restriction.

  If you assign ports used by a non-guest (such as My Devices) portal to a guest portal, an error message appears.

  For posture assessments and remediation only, the Client Provisioning portal also uses ports 8905 and 8909. Otherwise, it uses the same ports assigned to the Guest portal.

  Portals assigned to the same HTTPS port can use the same Gigabit Ethernet interface or another interface. If they use the same port and interface combination, they must use the same certificate group tag. For example:

  - Valid combinations include, using the Sponsor portal as an example:
    - Sponsor portal: Port **8443**, Interface **0**, Certificate tag **A** and My Devices portal: Port **8443**, Interface **0**, Certificate group **A**.
    - Sponsor portal: Port **8443**, Interface **0**, Certificate group **A** and My Devices portal: Port **8445**, Interface **0**, Certificate group **B**.
    - Sponsor portal: Port **8444**, Interface **1**, Certificate group **A** and Blocked List portal: Port **8444**, Interface **0**, Certificate group **B**.
  - Invalid combinations include:
    - Sponsor portal: Port **8443**, Interface **0**, Certificate group **A** and My Devices portal: **8443**, Interface **0**, Certificate group **B**.
    - Sponsor portal: Port **8444**, Interface **0**, Certificate tag **A** and Blocked List portal: Port **8444**, Interface **0**, Certificate group **A**.

Note We recommend that you use interface 0 for Guest services for best performance. You can either configure only interface 0 in the **Portal Settings**, or you can use the CLI command **ip host** to map a hostname or FQDN to the IP address of interface 0.

- **Allowed Interfaces**: Select the PSN interfaces which a PAN can use to run a portal. When a request to open a portal is made on the PAN, the PAN looks for an available allowed port on the PSN. You must configure the Ethernet interfaces using IP addresses on different subnets.

  These interfaces must be available on all the PSNs, including VM-based ones, that have Policy Services turned on. This is a requirement because any of these PSNs can be used for the redirect at the start of the guest session.

  - The Ethernet interfaces must use IP addresses on different subnets.
  - The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
  - The portal certificate Subject Name or Alternate Subject Name must resolve to the interface IP address.
  - Configure **ip host x.x.x.x yyy.domain.com** in Cisco ISE CLI to map the secondary interface IP address to the FQDN, which is used to match the certificate Subject Name or Alternate Subject Name.
  - If only the bonded NIC is selected, when the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN logs an error and exits. The PSN will not try to start the portal on the physical interface.
  - NIC Teaming or bonding is a configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based in the **Portal Settings** configuration. If both physical NICs and the corresponding bonded NIC are configured, when the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.

- **Certificate Group tag**: Pick a certificate group tag that specifies the certificate to be used for the portal's HTTPS traffic.

- **Fully Qualified Domain Name (FQDN)**: Enter at least one unique FQDN or hostname for the Sponsor or MyDevices portal. For example, you can enter **`sponsorportal.yourcompany.com,sponsor`**, so that when the user enters either of those into a browser, the sponsor portal displays. Separate names with commas, but do not include spaces between entries.

  If you change the default FQDN, then also do the following:

  - Update your DNS so that the FQDN of the new URL resolves to a valid Policy Services Node (PSN) IP address. Optionally, this address could point to a load balancer virtual IP address that serves a pool of PSNs.

  - To avoid certificate warning messages due to name mismatches, include the FQDN of the customized URL, or a wildcard, in the subject alternative name (SAN) attribute of the local server certificate of the Cisco ISE PSN. If the **Allow Kerberos SSO** option is enabled for the sponsor portal, you must include the FQDN of the Cisco ISE PSN, or a wildcard, in the SAN attribute of the local server certificate used by the portal.

- **Authentication Method**: Choose which identity source sequence or Identity Provider (IdP) to use for user authentication. The identity source sequence is a list of identity stores that are searched in sequence to verify user credentials.

  Cisco ISE includes a default identity source sequence for sponsor portals, Sponsor_Portal_Sequence.

  To configure IdP, choose **Administration** > **Identity Management** > **External Identity Sources** > **SAML Id Providers**.

  To configure an identity source sequence, choose **Administration > Identity Management > Identity Source Sequences**.

- **Endpoint Identity Group**: Choose an endpoint identity group to track guest devices. Cisco ISE provides the **GuestEndpoints** endpoint identity group to use as a default. You can also create more endpoint identity groups if you choose to not use the default.

  Choose an endpoint identity group to track employee devices. Cisco ISE provides the **RegisteredDevices** endpoint identity group to use as a default. You can also create more endpoint identity groups if you choose to not use the default.

- **Purge Endpoints in this Identity Group when they Reach __ Days**: Specify the number of days after which the device is purged from the Cisco ISE database. Purging is done on a daily basis and the purge activity is synchronized with the overall purge timing. The change is applied globally for this endpoint identity group.

  If changes are made to the Endpoint Purge Policy based on other policy conditions, this setting is no longer available for use.

- **Idle Timeout**: Enter the time in minutes that you want Cisco ISE to wait before it logs out the user if there is no activity in the portal. The valid range is from 1 to 30 minutes.

- **Display Language**

  - **Use Browser Locale**: Use the language specified in the client browser's locale setting as the display language of the portal. If browser locale's language is not supported by Cisco ISE, then the **Fallback Language** is used as the language portal.

  - **Fallback Language**: Choose the language to use when the language cannot be obtained from the browser locale, or if the browser locale language is not supported by Cisco ISE.

  - **Always Use**: Choose the display language to use for the portal. This setting overrides the **User Browser Locale** option.

Login Page Settings for My Devices Portals

- **Maximum Failed Login Attempts Before Rate Limiting**: Specify the number of failed login attempts from a single browser session before Cisco ISE starts to throttle that account. This does not cause an account lockout. The throttled rate is configured in **Time between login attempts when rate limiting**.

- **Maximum Failed Login Attempts Before Rate Limiting**: Specify the number of failed login attempts from a single browser session before Cisco ISE starts to throttle that account. This does not cause an account lockout. The throttled rate is configured in **Time between login attempts when rate limiting**.
- **Include an AUP**: Add a acceptable use policy window to the flow. You can add the AUP to the window, or link to another window.

Acceptable Use Policy Page Settings for My Devices Portals

To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Administration** > **Device Portal Management** > **My Devices Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Acceptable Use Policy (AUP) Page Settings**.

Use these settings to define the AUP experience for the users (guests, sponsors or employees as applicable).

Field	Usage Guidelines
Include an AUP Page	Display your company’s network-usage terms and conditions on a separate page to the user.
Require scrolling to end of AUP	Ensure that the user has read the AUP completely. The **Accept** button is enabled only after the user has scrolled to the end of the AUP.
On First Login only	Display an AUP when the user logs into the network or portal for the first time only.
On Every Login	Display an AUP each time the user logs into the network or portal.
Every __ Days (starting at first login)	Display an AUP periodically after the user first logs into the network or portal.

Post-Login Banner Page Settings for My Devices Portals

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **My Devices Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Post-Login Banner Page Settings**.

Use this setting to notify users (guests, sponsors or employees as applicable) of additional information after they log in successfully.

Field Name	Usage Guidelines
Include a Post-Login Banner page	Display additional information after the users successfully log in and before they are granted network access.

Employee Change Password Settings for My Devices Portals

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **My Devices Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Employee Change Password Settings**. Use these settings to define the password requirements for employees using the My Devices portal.

To set the employee password policy, choose **Administration** > **Identity Management** > **Settings** > **Username Password Policy**.

Field Name	Usage Guidelines
Allow internal users to change password	Allow employees to change their passwords after they log into the My Devices portal. This only applies to employees whose accounts are stored in the Cisco ISE database and not to those stored in external databases, such as Active Directory or LDAP.

Manage Device Settings for My Devices Portal

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **My Devices Portals** > **Create, Edit or Duplicate** > **Portal Page Customization** > **Manage Devices**.

Under **Page Customizations**, you can customize the messages, titles, content, instructions, and field and button labels that appear on the **Manage Accounts** tab of the My Devices portal.

Under **Settings**, you can specify the actions that employees using this portal can perform on their registered personal devices.

Table 200: Manage Device Settings for My Devices Portals

Field Name	Usage Guidelines
Lost	Enable employees to indicate that their device is lost. This action updates the device status in the My Devices portal to Lost and adds the device to the Blocked List endpoint identity group.
Reinstate	This action reinstates a block listed, lost or stolen device and resets it status to its last known value. This action resets the status of a stolen device to Not Registered, since it has to undergo additional provisioning before it can connect to the network. If you want to prevent employees reinstating devices that you have block listed, do not enable this option in the My Devices portal.
Delete	Enable employees to delete a registered device from the My Devices portal or to delete unused and add new devices, when the maximum number of registered devices is reached. This action removes the device from the list of devices displayed in the My Devices portal, but the device remains in the Cisco ISE database and continues to be listed in the Endpoints list. To define the maximum number of personal devices that employees can register using either the BYOD or My Devices portals, choose **Administration** > **Device Portal Management** > **Settings** > **Employee Registered Devices**. To permanently delete the device from the Cisco ISE database, choose **Work Centers** > **Network Access** > **Identities** > **Endpoints**.
Stolen	Enable employees to indicate that their device is stolen. This action updates the device status in the My Devices portal to Stolen, adds the device to the Blocked List endpoint identity group, and removes its certificate.

Field Name	Usage Guidelines
Device lock	For MDM enrolled devices only. Enable employees to immediately lock their device remotely from the My Devices portal, in the event it is lost or stolen. This action prevents unauthorized use of the device. However, the PIN cannot be set in the My Devices portal and should have already been configured by the employee on their mobile device in advance.
Unenroll	For MDM enrolled devices only. Enable employees to choose this option if they no longer need to use their device at work. This action removes only those applications and settings installed by your company, while retaining other apps and data on the employee's mobile device.
Full wipe	For MDM enrolled devices only. Enable employees to choose this option if they have lost their device or are replacing it with a new one. This action resets the employee's mobile device to its default factory settings, removing installed apps and data.

Add, Edit, and Locate Device Customization for My Devices Portals

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **My Devices Portals** > **Create, Edit or Duplicate** > **Portal Page Customization** > **Add Devices, Edit Devices or Locate Devices**.

Under **Page Customizations**, you can customize the messages, titles, content, instructions, and field and button labels that appear on the Add, Edit and Locate tabs of the My Devices portal.

Support Information Page Settings for Device Portals

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **BYOD Portals, Client Provisioning Portals, MDM Portals, or My Devices Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Support Information Page Settings**.

Use these settings to display the information that your Help Desk can use to troubleshoot access issues experienced by users (guests, sponsors or employees as applicable).

Field Name	Usage Guidelines
Include a Support Information Page	Display a link to an information window, such as **Contact Us**, on all enabled windows for the portal.
MAC Address	Include the MAC address of the device on the **Support Information** window.
IP Address	Include the IP address of the device on the **Support Information** window.
Browser User Agent	Include the browser details such as the product name and version, layout engine, and version of the user agent originating the request on the **Support Information** window.
Policy Server	Include the IP address of the ISE Policy Service Node (PSN) that is serving this portal on the **Support Information** window.

Field Name	Usage Guidelines
Failure Code	If available, include the corresponding number from the log message catalog. To view the message catalog, choose **Administration** > **System** > **Logging** > **Message Catalog**.
Hide Field	Do not display any field labels on the **Support Information** window if the information that they would contain is non-existent. For example, if the failure code is unknown, and therefore blank, do not display **Failure Code**, even if it is selected.
Display Label with no Value	Display all selected field labels on the **Support Information** window, even if the information that they would contain is non-existent. For example, if the failure code is unknown, display **Failure Code**, even if it is blank.
Display Label with Default Value	Display this text in any selected field on the **Support Information** window, if the information that they would contain is non-existent. For example, if you enter Not Available in this field, and the failure code is unknown, the **Failure Code** field displays **Not Available**.

CHAPTER 15

Cisco pxGrid

- Cisco pxGrid and ISE, on page 1321

Cisco pxGrid and ISE

Note From Cisco ISE Release 3.1, all pxGrid connections must be based on pxGrid 2.0. pxGrid 1.0-based (XMPP-based) integrations will cease to work on Cisco ISE from Release 3.1 onwards.

pxGrid Version 2.0, which is based on WebSockets, was introduced in Cisco ISE Release 2.4. We recommend that you plan and upgrade your other systems to pxGrid 2.0-compliant versions in order to prevent potential disruptions, if any, to integrations.

Cisco Platform Exchange Grid (pxGrid) is an open and scalable Security Product Integration Framework that allows for bi-directional any-to-any partner platform integrations.

pxGrid 2.0 uses REST and WebSocket interfaces. A client uses REST for control messages, queries and application data, and WebSockets for pushing events. For more information about pxGrid 2.0, see Welcome to Learning Cisco Platform Exchange Grid (pxGrid).

pxGrid can:

- Share context-sensitive information from the Cisco ISE session directory with other network systems, such as Cisco ISE ecosystem partner systems and other Cisco platforms.
- Enable third-party systems to invoke adaptive network control actions to quarantine users and devices in response to a network or security event. TrustSec information, such as tag definition, value, and description, pass from Cisco ISE via a TrustSec topic to other networks.
- Send endpoint profiles with Fully Qualified Names (FQNs) from Cisco ISE to other networks through an endpoint profile meta topic.
- Bulk download of tags and endpoint profiles.
- Publish and subscribe to SXP bindings (IP-SGT mappings) through pxGrid. For more information about SXP bindings, see the *Security Group Tag Exchange Protocol* section in the Segmentation chapter of the Cisco ISE Administrators Guide.

- Cisco pxGrid Context-in enables ecosystem partners to publish topic information into Cisco ISE. This enables Cisco ISE to take action based on the identified asset in the ecosystem. For more information about Cisco pxGrid Context-in, see pxGrid Context-In.

pxGrid Overview

pxGrid has the following components:

- Controller: Handles Discovery, Authentication, and Authorization.
- Provider: Returns query results or publishes.
- Pubsub: Provides pxGrid services to providers and consumers.
- Subscriber: Once authorized, subscribers get the contextual information and alerts from topics that they subscribe to.

pxGrid provides the following functions:

- Discovery: Discovers service properties based on service name. The flow starts when a provider asks to “Register Service” with the pxGrid Controller. After registration, the consumer uses “Lookup Service” to discover the locations of the providers.
- Authentication: The pxGrid Controller authenticates the pxGrid client for access to services. Credentials are either username and password, or certificates (preferred).
- Authorization: When pxGrid gets an operation request, it consults with pxGrid Controller to authorize the request. pxGrid assigns the client to a pre-defined group.

High Availability for pxGrid 2.0

pxGrid 2.0 nodes operate in an Active/Active configuration. For high availability, there should be at least two pxGrid nodes in the deployment. Large deployments can have up to four nodes for increased scale and redundancy. We recommend that you configure IP addresses for all nodes, so that if one node goes down, that node's clients connect to working node. When the PAN goes down, pxGrid server stops handling the activations. Manually promote the PAN to activate the pxGrid server. For more information about pxGrid deployments, see **ISE Performance & Scale**.

All pxGrid service provider clients periodically reregister themselves with the pxGrid controller within a span of 7.5 minutes. If the client does not reregister, the PAN node assumes it’s inactive, and deletes that client. If the PAN node goes down for more than 7.5 minutes, when it comes back up, it deletes all the clients with timestamp values older than 7.5 minutes. All those clients must then register again with the pxGrid controller.

pxGrid 2.0 clients use WebSocket and REST-based APIs for pub/sub and query. These APIs are served by the ISE application server on port 8910. The pxGrid processes shown by `show logging application pxgrid` don’t apply to pxGrid 2.0.

Note All the references to pxGrid 1.0 processes in the GUI and the CLI have been removed.

Loss Detection

In Cisco ISE 3.0, we added sequence IDs to pxGrid topics. If there is a break in transmission, the subscriber can recognize that by checking the gap in sequence of IDs. The subscriber notices the change in topic sequence

ID, and asks for data based on the date of last sequence number. If the Publisher goes down, when it comes back up, topic sequence starts at 0. When the Subscriber sees sequence 0, they must clear the cache and start bulk download. If subscriber goes down, the publisher keeps assigning sequential IDs. When the subscriber reconnects, and sees a gap in sequence IDs, the subscriber asks for data from time of the last sequence number. Loss detection works with Session Directory, and TrustSec Configuration. With Session Directory, when the client detects a loss, they must clear the cache and start bulk download.

If you have an existing application that doesn't use sequence IDs, you don't have to use them. But using them provides benefits of loss detection and recovery from loss.

Session Directory sessions are batched and published by MnT asynchronously for every notify interval to `/topic/com.cisco.ise.session`.

Changes to TrustSec Security Groups are published to `/topic/com.cisco.ise.config.trustsec.security.group`.

Loss Detection is only supported for pxGrid 2.0, and is on by default.

To see code examples of using Loss Detection, see https://github.com/cisco-pxgrid/pxgrid-rest-ws/tree/master/java/src/main/java/com/cisco/pxgrid/samples/ise.

Monitoring and Debugging

The following logs are available for pxGrid:

- pxgrid-server.log: pxGrid 2.0 activities and errors

The **Log** page displays all the pxGrid 2.0 management events. Event info includes the client and capability names along with the event type and timestamp. Choose **Administration** > **pxGrid Services** > **Diagnostics** > **Log** to view the list of events. You can also clear the logs and resynchronize or refresh the list.

pxGrid Failover and Recovery

The time taken for pxGrid recovery in different failover scenarios in a multi-pxGrid node deployment with atleast one primary and secondary pxGrid node each, varies depending on the node that goes down or comes back up and certain other variables, some of which are described in detail below.

Following are four different pxGrid failover and recovery scenarios and the workflows triggered internally in each of these cases:

- **Primary pxGrid node goes down**

  Secondary pxGrid node MnT continues to be the sessions data publisher. If the Firewall Management Center (FMC) is connected to the primary node, after a few unsuccessful retry attempts, it connects and subscribes to the secondary node. Since there has been a disruption, FMC will do a bulk download.

  If the FMC is already subscribed to the secondary pxGrid node, the recovery will be even smoother. Since there is no disruption, the FMC does not need to do a bulk download. Hence, the recovery is much faster. In this scenario, the recovery time can be as less as 2 minutes.

- **Primary pxGrid node comes back up**

  The FMC is still connected to the secondary pxGrid node and disruption will be less as the secondary node continues to publish sessions data. Bulk download is unncessary in this case, hence recovery is fast as in the case of the previous scenario.

  The FMC will be able to re-establish connection with pxGrid and connect to the primary pxGrid node only after all the fanouts are re-established and database sync is complete.

- **Secondary pxGrid node goes down**

  If the FMC is connected to the primary node pxGrid, it will continue to be connected there. But there will be a disruption because the secondary MnT node would have been the publisher of session topic data so far. Primary MnT node takes some time to realize that the secondary MnT node is down and when it realizes, it starts to publish session topic data from the primary node.

  If the FMC is connected to pxGrid on the secondary node, it retries connection, and on failure, connects to the primary PxGrid node for subscription. This happens in parallel to the previous step. On a successful reconnection with the secondary pxGrid node, FMC does a bulk download.

- **Secondary pxGrid node comes back up**

  This is the scenario in which recovery takes the longest time. If there were any pxGrid related database changes during the time that the secondary node had been down, there is a possibility that pxGrid will not be functional until the database sync operation completes. The time taken for database sync depends on the size of configuration database.

  The secondary pxGrid node goes back to being the sessions data publisher.

  A refresh deployment notification is sent to all modules and when pxgrid module receives this, it re-establishes all the fanouts that are used for internal distribution of data. Until this is completed, pxGrid will not be completely functional.

  If the FMC has to reconnect, after the reconnection succeeds, FMC will do a bulk download.

pxGrid Summary Page

The pxGrid Summary page displays statistics of the current pxGrid 2.0 environment.

- Current Connections: Lists the connections to the controller
- Control Messages: Authentication, Authorization, and service Discovery
- REST APIs: Number of clients who connected using WebSockets or XMPP
- Pubsub Throughput: Amount of data published to clients
- Clients: Clients connected by REST or WebSocket
- Errors: Number of transmission errors, which caused client to ask for data transfer restart

pxGrid Client Management

Clients must register and receive account approval to use pxGrid services in Cisco ISE. Clients use the pxGrid Client library through the pxGrid SDK to register. Cisco ISE supports both auto and manual registrations.

- **Clients**: Choose **Administration** > **pxGrid Services** > **Client Management** > **Clients** to view this window. Lists external client accounts for pxGrid 2.0.
- **pxGrid Policy**: Choose **Administration** > **pxGrid Services** > **Client Management** > **pxGrid Policy** to view this window. Lists the available services that clients can subscribe to. You can edit a policy to change which groups can access to that policy. You can also create a new policy for a service that doesn’t already have a policy.

- **Groups**: Choose **Administration > pxGrid Services > Client Management > Groups** to view this window. ANC is a predefined group. You can add more groups, and use them to limit access to services.

  A pxGrid client can register itself with the pxGrid controller by sending the username via REST API. The pxGrid controller generates a password for the pxGrid client during client registration. The administrator can approve or deny the connection request.

- **Certificates**: Choose **Administration > pxGrid Services > Client Management > Certificates** to view this window. You can generate a new certificate to use the Cisco ISE internal Certificate Authority.

  For information about creating certificates for pxGrid, see:

  - Deploying Certificates with Cisco pxGrid - Using Self-Signed Certificates Updates to Cisco ISE 2.0/2.1/2.2
  - Deploying Certificates with Cisco pxGrid - Using External CA with updates to Cisco ISE 2.0/2.1/2.2

Control pxGrid Policies

You can create pxGrid authorization policies to control access to the services that pxGrid clients can access. These policies control which services are available to the pxGrid clients.

You can create different types of groups and map the available services to the pxGrid clients to these groups. Use the **Manage Groups** option in the **Client Management > Groups** window to add new groups. You can view the example authorization rules in the **Client Management** > **Policies** window.

To create an authorization policies for pxGrid clients:

Step 1 Choose **Administration > pxGrid Services > Client Management > Policy**, and then click **Add**.

Step 2 From the **Service** drop-down list, choose one of the following options:

- com.cisco.ise.radius
- come.cisco.ise.sxp
- com.cisco.ise.trustsec
- com.cisco.ise.session
- com.cisco.ise.system
- com.cisco.ise.mdm
- com.cisco.ise.config.trustsec
- com.cisco.ise.config.profiler
- com.cisco.ise.pxgrid.admin
- com.cisco.ise.config.deployment.node
- com.cisco.ise.endpoint
- com.cisco.ise.config.anc
- com.cisco.ise.dnac
- com.cisco.ise.config.upn

- com.cisco.ise.pubsub

Step 3 From the **Operation** drop-down list, choose one of the following options:

- <ANY>
- publish
- publish /topic/com.cisco.ise.session
- publish /topic/com.cisco.ise.session.group
- publish /topic/com.cisco.ise.anc
- <CUSTOM>—You can specify a custom operation if you select this option.

Step 4 From the **Groups** drop-down list, choose the groups that you want to map to this service.

Predefined groups (such as EPS and ANC) and groups that you manually added are listed in this drop-down list.

Note Only the clients that are part of the groups included in the policy can subscribe to the service specified in that policy.

Step 5 Click **Submit**.

Enable pxGrid Service

Before you begin

- Enable the pxGrid persona on at least one node to view the requests from the Cisco pxGrid clients.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **pxGrid Services**.

Step 2 Check the checkbox next to the client and click **Approve**.

Step 3 Click **Refresh** to view the latest status.

Step 4 Select the capability you want to enable and click **Enable**.

Step 5 Click **Refresh** to view the latest status.

pxGrid Diagnostics

- **Websocket**: The **Administration > pxGrid Services > Diagnostics > Websocket** window lists pxGrid 2.0 clients (external and internal). It also lists the available pxGrid 2.0 topics, and the clients that publish or subscribe to each one.
- **Logs**: The **Administration > pxGrid Services > Diagnostics > Live Logs** window lists management events.

- **Tests**: Choose **Administration > pxGrid Services > Diagnostics > Tests > Health Monitoring test** and click **Start Test** to verify whether a client can access the Session Directory service. When the test is complete, you can view the log of the test activities.

pxGrid Settings

Choose one of the following options in the **Administration > pxGrid Services > Settings** window:

- **Automatically approve new certificate-based accounts**: This option is disabled by default. It gives you control over connections to the pxGrid server. Enable this option only when you trust all clients in your environment.
- **Allow password based account creation**: Check this check box to enable username/password based authentication for pxGrid clients. If you enable this option, the pxGrid clients are not automatically approved.

Generate Cisco pxGrid Certificate

Before you begin

- You must not use the same certificate for Cisco ISE pxGrid server and pxGrid clients. You must use client certificates for the pxGrid clients. To generate client certificates, choose **Administration > System > Certificates**.
- Some versions of Cisco ISE have a certificate for Cisco pxGrid that uses NetscapeCertType. We recommend that you generate a new certificate.
- To perform the following task, you must be a Super Admin or System Admin.
- A Cisco pxGrid certificate must be generated from the primary PAN.
- If the Cisco pxGrid certificate uses the subject alternative name (SAN) extension, be sure to include the FQDN of the subject identity as a DNS name entry.
- Create a certificate template with digital signature usage and use that to generate a new Cisco pxGrid certificate.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **pxGrid Services** > **Client Management** > **Certificates**.

Step 2 From the **I want to** drop-down list, choose one of the following options:

- **Generate a single certificate (without a certificate signing request)**: You must enter the Common Name (CN) if you select this option.
- **Generate a single certificate (with a certificate signing request)**: You must enter the Certificate Signing Request details if you select this option.

Step 3 (Optional) Enter a description for this certificate.

Step 4 Click the **pxGrid_Certificate_Template** link to download and edit the certificate template based on your requirements.

Step 5 Enter the **Subject Alternative Name (SAN)**. You can add multiple SANs. The following options are available:

- **IP address**: Enter the IP address of the Cisco pxGrid client to be associated with the certificate.
- **FQDN**: Enter the FQDN of the pxGrid client.

Step 6 From the **Certificate Download Format** drop-down list, choose one of the following options:

- **Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)**: The root certificate, the intermediate CA certificates, and the end entity certificate are represented in the PEM format. PEM-formatted certificates are BASE64-encoded ASCII files. Each certificate starts with the `"--------BEGIN CERTIFICATE-----"` tag and ends with the `"-------END CERTIFICATE----"` tag. The end entity's private key is stored using PKCS* PEM. It starts with the `"-----BEGIN ENCRYPTED PRIVATE KEY----"` tag and ends with the `"-----END ENCRYPTED PRIVATE KEY----"` tag.
- **PKCS12 format (including certificate chain; one file for both the certificate chain and key)**: A binary format to store the root CA certificate, the intermediate CA certificate, and the end entity's certificate and private key in one encrypted file.

Step 7 Enter the password for the certificate.

Step 8 Click **Create**.

You can view the certificate that you created in the **Issued Certificates** window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Certificate Authority** > **Issued Certificates**.

Note From Cisco ISE 2.4 patch 13 onwards, the certificate requirements have become stricter for the pxGrid service. If you are using the Cisco ISE default self-signed certificate as the pxGrid certificate, Cisco ISE might reject that certificate after applying Cisco ISE 2.4 patch 13 or later. This is because the earlier versions of that certificate have the **Netscape Cert Type** extension specified as **SSL Server**, which now fails (a client certificate is also required now).

Any client with a noncompliant certificate fails to integrate with Cisco ISE. Use a certificate issued by the internal CA, or generate a new certificate with proper usage extensions:

- The **Key Usage** extension in the certificate must contain the **Digital Signature** and **Key Encipherment** fields.
- The **Extended Key Usage** extension in the certificate must contain the **Client Authentication** and **Server Authentication** fields.
- The **Netscape Certificate Type** extension is not required. If you want to include that extension, add both **SSL Client** and **SSL Server** in the extension.
- If you are using a self-signed certificate, the **Basic Constraints CA** field must be set to **True**, and the **Key Usage** extension must contain the **Key Cert Sign** field.

Known Limitations in pxGrid Certificate Generation

pxGrid certificate generation in Cisco ISE follows the tabulated logic explained below:

Serial number	System Certificate (EAP)	Issuer Certificate	pxGrid Format	Support
1	Multiple Common Name	Single Common Name	PKCS8 , PKCS12	Yes, supported

Serial number	System Certificate (EAP)	Issuer Certificate	pxGrid Format	Support
2	Multiple Common Name	Multiple Common Name	PKCS12	Yes, supported
3	Multiple Common Name	Multiple Common Name	PKCS8	Not supported

CHAPTER 16

Integration

The following sections describe the configuration required on switches and Wireless Controllers to support Cisco ISE functions.

- Enable Your Switch to Support Standard Web Authentication, on page 1331
- Define Local Username and Password for Synthetic RADIUS Transactions, on page 1332
- Configure NTP Server for Accurate Log and Accounting Timestamps, on page 1332
- Command to Enable AAA Functions, on page 1332
- RADIUS Server Configuration on the Switch, on page 1333
- Enable Switch to Handle RADIUS Change of Authorization (CoA), on page 1333
- Enable Device Tracking and DHCP Snooping on Switch Ports, on page 1334
- Enable 802.1X Port-Based Authentication for Switch Ports, on page 1334
- Enable EAP for Critical Authentications, on page 1334
- Throttle AAA Requests Using Recovery Delay, on page 1334
- VLAN Definitions Based on Enforcement States, on page 1335
- Local (Default) Access List (ACL) Definitions on the Switch, on page 1335
- Enable Switch Ports for 802.1X and MAB, on page 1336
- Command to Enable 802.1X based on Identity-Based Networking Services, on page 1338
- Enable EPM Logging, on page 1340
- Enable Switch to Receive SNMP Traps, on page 1340
- Enable SNMP v3 Query for Profiling on Switch, on page 1340
- Enable MAC Notification Traps for Profiler to Collect, on page 1340
- Configure RADIUS Idle-Timeout on the Switch, on page 1340
- Wireless Controller Configuration for iOS Supplicant Provisioning, on page 1341
- Configure ACLs on Wireless Controllers for MDM Interoperability, on page 1341

Enable Your Switch to Support Standard Web Authentication

Ensure that you include the following commands in your switch configuration to enable standard web authentication functions for Cisco ISE, including provisions for URL redirection upon authentication:

```
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 10.1.2.3
ip http server

! Must enable HTTP/HTTPS for URL-redirection on port 80/443

ip http secure-server
```

Define Local Username and Password for Synthetic RADIUS Transactions

Enter the following command to enable the switch to talk to the Cisco ISE node as though it is the RADIUS server for this network segment:

```
username test-radius password 0 abcde123
```

Configure NTP Server for Accurate Log and Accounting Timestamps

Ensure that you specify the same NTP server on the switch as you have set in Cisco ISE by entering the following command:

```
ntp server <IP_address>|<domain_name>
```

Command to Enable AAA Functions

Enter the following commands on the switch to enable the various AAA functions between the switch and Cisco ISE, including 802.1X and MAB authentication functions:

```
aaa new-model

! Creates an 802.1X port-based authentication method list

aaa authentication dot1x default group radius

! Required for VLAN/ACL assignment

aaa authorization network default group radius

! Authentication & authorization for webauth transactions

aaa authorization auth-proxy default group radius

! Enables accounting for 802.1X and MAB authentications

aaa accounting dot1x default start-stop group radius

!

aaa session-id common
```

```
!

aaa accounting update periodic 1440

! Update AAA accounting information periodically every 1440 minutes

aaa accounting system default start-stop group radius

!
```

RADIUS Server Configuration on the Switch

Configure the switch to interact with Cisco ISE as the RADIUS source server by entering the following commands:

```
!
radius-server <ISE Name>

! ISE Name is the name of the ISE PSN

address ipv4 <ip address> auth-port 1812 acct-port 1813

! IP address is the address of the PSN. This example uses the standard RADIUS ports.

key <passwd>

! passwd is the secret password confiugured in Cisco ISE

exit
```

Note We recommend that you configure a dead-criteria time of 30 seconds with 3 retries to provide longer response times for RADIUS requests that use Active Directory for authentication.

Enable Switch to Handle RADIUS Change of Authorization (CoA)

Specify the settings to ensure the switch can appropriately handle RADIUS CoA behavior and related posture functions on Cisco ISE by entering the following commands:

```
aaa server radius dynamic-author client <ISE-IP> server-key 0 abcde123
```

Note

- Cisco ISE uses port 1700 (Cisco IOS software default) versus RFC default port 3799 for CoA. Existing Cisco Secure ACS 5.x customers may already have this set to port 3799 if they use CoA as part of an existing ACS implementation.
- secret key should be the same as the one configured on Cisco ISE while adding a network device and the IP address should be a PSN IP address.

Enable Device Tracking and DHCP Snooping on Switch Ports

To help provide optional security-oriented functions from Cisco ISE, enable device tracking and DHCP snooping for IP substitution in dynamic ACLs on switch ports by entering the following commands:

```
! Optional
 ip dhcp snooping

! Required!

! Configure Device Tracking Policy!device-tracking policy <DT_POLICY_NAME>no protocol
 ndp tracking enable

! Bind it to interface!interface <interface_id>device-tracking
attach-policy<DT_POLICY_NAME>
```

In RADIUS accounting, the DHCP attributes are not sent by the IOS sensor to Cisco ISE even when DHCP snooping is enabled. In such cases, DHCP snooping should be enabled on the VLAN to make the DHCP active.

Use the following commands to enable DHCP snooping on VLAN:

```
ip dhcp snooping

ip dhcp snooping vlan 1-100
```

Enable 802.1X Port-Based Authentication for Switch Ports

Enter the following commands to turn on 802.1X authentication for switch ports, globally:

```
dot1x system-auth-control
```

Enable EAP for Critical Authentications

To support supplicant authentication requests over the LAN, enable EAP for critical authentications (Inaccessible Authentication Bypass) by entering the following command:

```
dot1x critical eapol
```

Throttle AAA Requests Using Recovery Delay

In the case of a critical authentication recovery, configure the switch to automatically introduce an authentication delay (in milliseconds) to ensure Cisco ISE can launch services again after recovery. Use the following command:

```
authentication critical recovery delay 1000
```

VLAN Definitions Based on Enforcement States

Enter the following commands to define the VLAN names, numbers, and Switch Virtual Interfaces (SVIs) based on known enforcement states in your network. Create the respective VLAN interfaces to enable routing between networks. This can be especially helpful to handle multiple sources of traffic passing over the same network segments from both the endpoints (such as PC, laptop) and the IP phone through which the endpoint is connected to the network, for example:

```
vlan <VLAN_number>
name ACCESS!
vlan <VLAN_number>
name VOICE

!
interface <VLAN_number>
description ACCESS
ip address 10.1.2.3 255.255.255.0
ip helper-address <DHCP_Server_IP_address>
ip helper-address <Cisco_ISE_IP_address>

!
interface <VLAN_number>
description VOICE
ip address 10.2.3.4 255.255.255.0
ip helper-address <DHCP_Server_IP_address>
```

Local (Default) Access List (ACL) Definitions on the Switch

Enable these functions on older switches (with Cisco IOS software releases earlier than 12.2(55)SE) to ensure Cisco ISE is able to perform the dynamic ACL updates required for authentication and authorization by entering the following commands:

```
ip access-list extended ACL-ALLOW

 permit ip any any

!

ip access-list extended ACL-DEFAULT

  remark DHCP

  permit udp any eq bootpc any eq bootps

  remark DNS

  permit udp any any eq domain
 remark Ping

 permit icmp any any

 remark Ping

 permit icmp any any

 remark PXE / TFTP

 permit udp any any eq tftp

 remark Allow HTTP/S to ISE and WebAuth portal
permit tcp any host <Cisco_ISE_IP_address> eq www

permit tcp any host <Cisco_ISE_IP_address> eq 443

permit tcp any host <Cisco_ISE_IP_address> eq 8443

permit tcp any host <Cisco_ISE_IP_address> eq 8905

permit udp any host <Cisco_ISE_IP_address> eq 8905

permit udp any host <Cisco_ISE_IP_address> eq 8906

permit tcp any host <Cisco_ISE_IP_address> eq 8080

permit udp any host <Cisco_ISE_IP_address> eq 9996

remark Drop all the rest

 deny ip any any log

!

! The ACL to allow URL-redirection for WebAuth
ip access-list extended ACL-WEBAUTH-REDIRECT

permit tcp any any eq www

permit tcp any any eq 443
```

Note This configuration on the Wireless Controller may increase CPU utilization and raises the risk of system instability. This is an IOS issue and does not adversely affect Cisco ISE.

Enable Switch Ports for 802.1X and MAB

To enable switch ports for 802.1X and MAB:

Step 1 Enter the interface configuration mode for all of the access switch ports:

interface range FastEthernet0/1-8

Step 2 Enable the switch ports for access mode (instead of trunk mode):

switchport mode access

Step 3 Statically configure the access VLAN. This provides local provisioning for the access VLANs and is required for open-mode authentication:

switchport access vlan <*VLAN_number*>

Step 4 Statically configure the voice VLAN:

switchport voice vlan <*VLAN_number*>

Step 5 Enable open-mode authentication. Open mode allows traffic to be bridged onto the data and voice VLANs before authentication is completed. We strongly recommend using a port-based ACL in a production environment to prevent unauthorized access.

Enabling open-mode authentication also allows pre-authentication access before the AAA server response, subject to the port ACL.

authentication open

Step 6 Apply a port-based ACL to determine which traffic should be bridged by default from unauthenticated endpoints onto the access VLAN. Because you should allow all access first and enforce policy later, you should apply ACL-ALLOW to permit all traffic through the switch port. You have already created a default Cisco ISE authorization to allow all traffic for now because we want complete visibility and do not want to impact the existing end-user experience yet.

An ACL must be configured to prepend dynamic ACLs from the AAA server.

ip access-group ACL-ALLOW in

Note Before Cisco IOS software Release 12.2(55)SE on DSBU switches, a port ACL is required for dynamic ACLs from a RADIUS AAA server to be applied. Failure to have a default ACL will result in assigned dynamic ACLs being ignored by the switch. With Cisco IOS software Release 12.2(55)SE, a default ACL will be automatically generated and applied.

Note We are using ACL-ALLOW at this point in the lab because we want to enable 802.1X port-based authentication, but without any impact on the existing network. In a later exercise, we will apply a different ACL-DEFAULT, which blocks undesired traffic for a production environment.

Step 7 Enable Multi-Auth host mode. Multi-Auth is essentially a superset of Multi-Domain Authentication (MDA). MDA only allows a single endpoint in the data domain. When multi-auth is configured, a single authenticated phone is allowed in the voice domain (as with MDA) but an unlimited number of data devices can be authenticated in the data domain.

Allow voice and multiple endpoints on the same physical access port

authentication host-mode multi-auth

Note Multiple data devices (whether virtualized devices or physical devices connected to a hub) behind an IP phone can exacerbate the access ports' physical link-state awareness.

Step 8 Enable various authentication method options with the following commands:

Enable re-authentication:

authentication periodic

Enable re-authentication via RADIUS Session-Timeout:

authentication timer reauthenticate server

authentication event fail action next-method

Configure critical authentication vlan method in case of dead server:

authentication event server dead action reinitialize vlan *<VLAN_number>*

authentication event server alive action reinitialize

Configure IOS Flex-Auth authentication for 802.1X and MAB:

authentication order dot1x mab

authentication priority dot1x mab

Step 9 Enable 802.1X port control on the switchport:

authentication port-control auto

authentication violation restrict

Step 10 Enable MAC Authentication Bypass (MAB):

mab

Step 11 Enable 802.1X on the switchport:

dot1x pae authenticator

Step 12 Set the retransmit period to 10 seconds:

dot1x timeout tx-period *10*

Note The 802.1X tx-period timeout should be set to 10 seconds. Do not change this unless you understand the implications.

Step 13 Enable the portfast feature:

spanning-tree portfast

Command to Enable 802.1X based on Identity-Based Networking Services

The following example shows a control policy that is configured to allow sequential authentication methods using 802.1X, MAB, and web authentication.

```
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all MAB
 match method mab
!
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
!
!


policy-map type control subscriber DOT1XMAB
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event authentication-failure match-first
  10 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  20 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
   30 authorize
  40 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
!
```

The following example shows a control policy that is configured to allow sequential authentication methods using MAB, 802.1X, and web authentication.

```
policy-map type control subscriber MABDOT1X
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using mab priority 20
   20 authenticate using dot1x priority 10
 event authentication-failure match-first
  10 class ALL_FAILED do-until-failure
   10 authentication-restart 60
 event authentication-success match-all
  10 class DOT1X do-until-failure
   10 terminate mab
 event agent-found match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
```

Applying the service policy on the interface:

```
interface GigabitEthernet1/0/4
 switchport mode access
 device-tracking attach-policy pol1
 ip access-group sample in
 authentication timer reauthenticate server
 access-session port-control auto
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 dot1x timeout auth-period 10
 spanning-tree portfast
 service-policy type control subscriber DOT1XMAB
```

Enable EPM Logging

Set up standard logging functions on the switch to support possible troubleshooting and recording for Cisco ISE functions:

```
epm logging
```

Enable Switch to Receive SNMP Traps

Ensure the switch can receive SNMP trap transmissions from Cisco ISE over the appropriate VLAN in this network segment:

```
snmp-server community public RO
snmp-server trap-source <VLAN_number>
```

Enable SNMP v3 Query for Profiling on Switch

Configure the switch to ensure SNMP v3 polling takes place as intended to support Cisco ISE profiling services using the following commands. Before that configure the SNMP settings in the Cisco ISE GUI in the **SNMP Settings** window. To view this window, click the **Menu** icon (☰) and choose**Administration** > **Network Resources** > **Network Devices** > **Add | Edit** > **SNMP Settings**.

```
Snmp-server user <name> <group> v3 auth md5 <string> priv des <string>
snmp-server group  <group> v3 priv
snmp-server group <group> v3 priv contextvlan-1
```

Note The **snmp-server group** *<group>* **v3 priv context** *vlan-1* command must be configured for each context. The **snmp show context** command lists all the context information.

If the SNMP request times out and there is no connectivity issue, then you can increase the timeout value.

Enable MAC Notification Traps for Profiler to Collect

Configure your switch to transmit the appropriate MAC notification traps so that the Cisco ISE profiler function can collect information on network endpoints:

```
mac address-table notification change
mac address-table notification mac-move
snmp trap mac-notification change added
snmp trap mac-notification change removed
```

Configure RADIUS Idle-Timeout on the Switch

To configure the RADIUS idle-timeout on a switch, use the following command:

```
Switch(config-if)# authentication timer inactivity
```

where *inactivity* is the interval of inactivity in seconds, after which the client activity is considered unauthorized.

In Cisco ISE, you can enable this option for any authorization policies to which such a session inactivity timer should apply. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.

Wireless Controller Configuration for iOS Supplicant Provisioning

For Single SSID

To support Apple iOS-based devices (iPhone or iPad) switching from one SSID to another on the same wireless access point, configure the Wireless Controller to enable the **FAST SSID change** function. This function helps ensure iOS-based devices can switch between SSIDs quickly.

For Dual SSID BYOD

Fast SSID must be enabled to support dual SSID BYOD. When fast SSID changing is enabled, the Wireless Controller allows clients to move faster between SSIDs. When fast SSID is enabled, the client entry is not cleared and the delay is not enforced. For more information about configuring fast SSID on a Cisco Wireless Controller, see the Cisco Wireless Controller Configuration Guide.

Example Wireless Controller Configuration

```
WLC (config)# FAST SSID change
```

You might see the following error message while trying to connect to a wireless network for some of the Apple iOS-based devices:

```
Could not scan for Wireless Networks.
```

You can ignore this error message because this does not affect the authentication of the device.

Configure ACLs on Wireless Controllers for MDM Interoperability

Configure ACLs on the Wireless Controller for use in an authorization policy to redirect nonregistered devices and certificate provisioning. Your ACLs must be in the following sequence.

Step 1 Allow all outbound traffic from the server to the client.

Step 2 (Optional) Allow ICMP inbound traffic from the client to the server for troubleshooting.

Step 3 Allow access to the MDM server for unregistered and noncompliant devices to download the MDM agent and proceed with compliance checks.

Step 4 Allow all inbound traffic from the client to the server to Cisco ISE for the web portal and supplicant, and certificate provisioning flows.

Step 5 Allow inbound Domain Name System (DNS) traffic from the client to the server for name resolution.

Step 6 Allow inbound DHCP traffic from the client to the server for IP addresses.

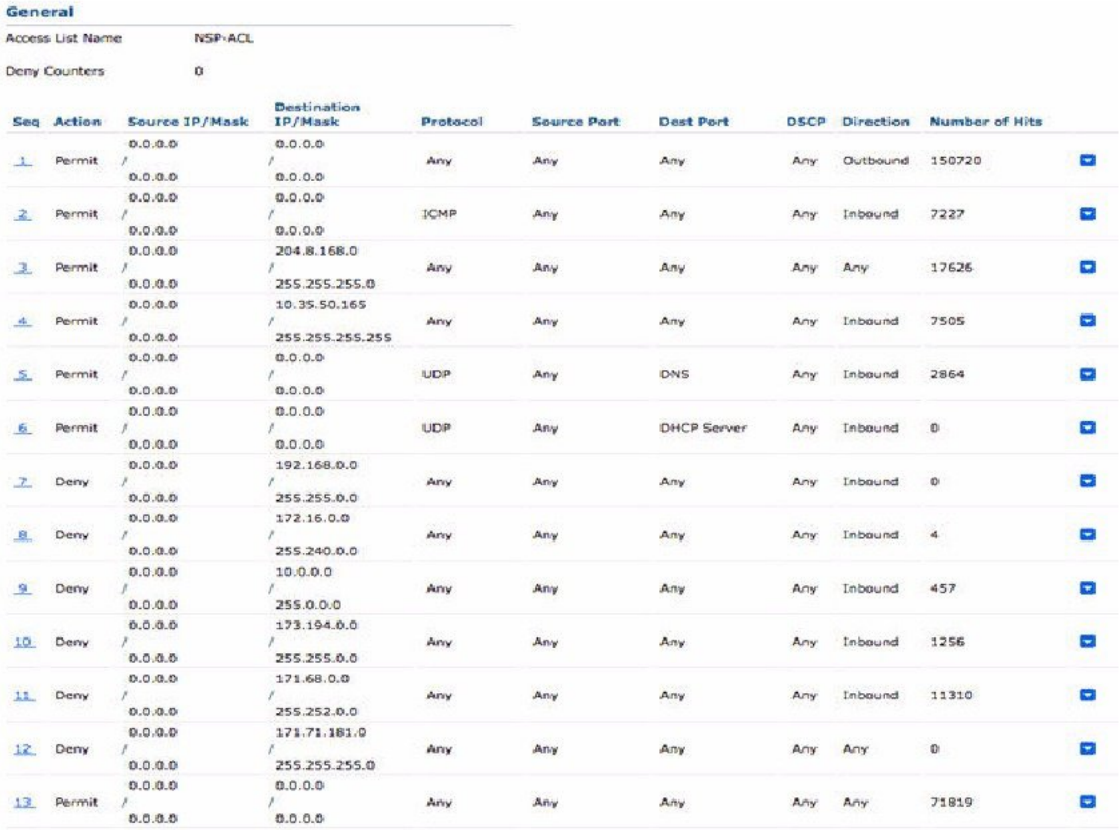
Step 7 Deny all inbound traffic from the client to the server to corporate resources for redirection to Cisco ISE (as per your company policy).

Step 8 (Optional) Permit the rest of the traffic.

Example

The following example shows the ACLs for redirecting a nonregistered device to the BYOD flow. In this example, the Cisco ISE IP address is 10.35.50.165, the internal corporate network IP addresses are 192.168.0.0 and 172.16.0.0 (to redirect), and the MDM server subnet is 204.8.168.0.

Figure 65: ACLs for Redirecting Nonregistered Device



General

Access List Name: NSP-ACL

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819

CHAPTER 17

Troubleshoot

- Monitoring and Troubleshooting Service in Cisco ISE, on page 1343
- Cisco ISE Telemetry, on page 1349
- Information that Telemetry Gathers, on page 1350
- SNMP Traps to Monitor Cisco ISE, on page 1352
- Cisco ISE Alarms, on page 1355
- Log Collection, on page 1374
- RADIUS Live Logs, on page 1375
- TACACS Live Logs, on page 1377
- Live Authentications, on page 1378
- RADIUS Live Sessions, on page 1380
- Export Summary, on page 1384
- Authentication Summary Report, on page 1385
- Cisco Support Diagnostics for Deployment and Support Information, on page 1386
- Obtain Configuration Backup Using Cisco Support Diagnostics Connector , on page 1387
- Diagnostic Troubleshooting Tools, on page 1388
- Session Trace Test Cases, on page 1391
- TCP Dump Utility to Validate Incoming Traffic, on page 1392
- Obtaining Additional Troubleshooting Information, on page 1396

Monitoring and Troubleshooting Service in Cisco ISE

The Monitoring and Troubleshooting (MnT) service is a comprehensive identity solution for all Cisco ISE run-time services. The **Operations** menu contains the following components, and can be viewed only from the primary Policy Administration Node (PAN). Note that the **Operations** menu does not appear in the primary Monitoring node.

- Monitoring: Provides real-time presentation of meaningful data representing the state of access activities on a network. This insight allows you to easily interpret and monitor operational conditions.

- Troubleshooting: Provides contextual guidance for resolving access issues on networks. You can then address user concerns and provide resolution in a timely manner.

- Reporting: Provides a catalog of standard reports that you can use to analyze trends and monitor system performance and network activities. You can customize reports in various ways and save them for future use. You can search records using wild cards and multiple values in all the reports for the **Identity**, **Endpoint ID**, and **ISE Node** (except the **Health Summary** report) fields.

ISE Community Resource

For a complete list of troubleshooting TechNotes, see ISE Troubleshooting TechNotes.

Open TAC Support Cases in Cisco ISE

You can now open TAC support cases in Cisco ISE to request support for both deployment issues with Cisco ISE and issues with other Cisco products and services such as Webex, Software Licensing, and so on. Using the TAC Support Case feature in the Cisco ISE portal, you can easily raise a support case for specific nodes that you face issues with. Along with the information you provide through the form that is provided, information like the serial number of your node and the Cisco ISE version in use are also sent to Cisco TAC. When opening TAC cases for other Cisco products, you can choose relevant categories and provide additional information such as Sales Order, Serial Number, and Contract Number to enable quicker case resolution by Cisco TAC.

In the **TAC Support Cases** window, you can also add a case to your favorites by clicking the star in the **Actions** column. Your favorite cases are then listed in the **Favourites** tab. You can filter your cases by checking the respective check boxes for **Open Cases, Draft Cases, Closed Cases, Created Cases, Updated Cases**, and their time of creation. You can also filter your cases by **Status** and **Severity** in the **Advanced Filters** area.

Note

- From Cisco ISE, Release 3.1, Patch 2, you can open TAC support cases in the Cisco ISE portal to request support for Cisco ISE and other Cisco products and services, Webex, and software licensing products.
- To disable the creation of TAC support cases, choose **Administration** > **System** > **Settings** > **Enable TAC Support Cases** and uncheck the check box.
- The Support Case Manager (SCM) feature does not function when Cisco ISE is deployed in an air-gapped environment. We therefore, recommend that you disable the SCM feature if you deploy Cisco ISE in this environment.
- Procedures outlined here describe only some of the fields in the Cisco ISE GUI because whenever changes are made to the Support Case Manager (SCM) interface, the same changes will be reflected in the Cisco ISE GUI.

Step 1 In the Cisco ISE portal home page, click the question mark icon at the top-right corner.

Step 2 In the **Interactive Help** menu that is displayed, from the **Resources** drop-down list, choose **TAC Support Cases**.

Note **Interactive Help** can be disabled by a Cisco ISE admin. If disabled, **TAC Support Cases** can be found as the last option under the question mark icon at the top-right corner.

Step 3 In the **SSO Authentication** window, log in using your cisco.com credentials. If you see an error message indicating failure in accessing the feature, consult Cisco customer support to review the terms of your Cisco ISE contract. After you log in, the **TAC Support Cases** window is displayed. All the cases that are associated with your Cisco account are displayed in this window.

Step 4 Click **Open A Case**.

Step 5 The **Open New Case** dialog box is displayed. Click the **Cisco ISE Case** radio button to raise a case for your Cisco ISE deployment or click the **Other Case** radio button to open a TAC case for other Cisco products and services.

- If you click the **Cisco ISE Case** radio button to open a TAC case for a Cisco ISE issue, perform these tasks:

a. From the **Nodes List** drop-down, choose up to four nodes for which to open a case. The Primary PAN and MnT nodes are chosen by default.

b. Click **Next**

c. In the **Check Entitlement** window that is displayed, choose your request type by clicking the appropriate radio button:

- **Diagnose and Fix**: Raise a case to diagnose and fix a problem in your Cisco ISE deployment.
- **RMA**: Raise a case to initiate a Return Material Authorization (RMA) request.
- **Ask a Question**: Raise a case to ask Cisco Technical Assistance Center (TAC) representatives questions about your Cisco ISE deployment.

d. You can find the details of your product using the **Serial Number** of your Cisco ISE device or by choosing a **Service Agreement.**

e. Click **Next** after finding your product details.

f. Fill in the necessary details in the **Problem Description** window. Severity level 3 is assigned to the case by default.

g. Fill in your contact information and preferred mode of communication. Review your case information and click **Submit** to submit your case.

- If you click the **Other Case** radio button to open a TAC case for Cisco products (other than Cisco ISE) and services, perform these tasks:

Note We recommend that you use the procedure of opening TAC support cases in Support Case Manager (SCM) to open cases for other Cisco products and services through Cisco ISE.

a. Click the **Other Case** radio button to create a case for an issue that is not related to your Cisco ISE deployment. A dialog box is displayed that contains information of other Cisco Products and Services.

b. Click the product or service that you want to raise a case for and select the category of your issue by clicking the corresponding options.

c. Click **Open Case**. The **Problem Description** window of **Support Case Manager** (SCM) is displayed.

d. Enter the details of your issue in the **Title** and **Description** fields.

e. Fill in your contact information in the corresponding fields.

f. Review your case information and click **Submit** to submit your case.

Cisco TAC receives the details of your issue and contacts you to further investigate the problem and troubleshoot.

Note We recommend that you contact Cisco TAC to open higher severity cases (1 and 2).

You can update or modify your contact information after opening a case by clicking the **Support Cases Preferences** icon in the **TAC Support Cases** window, updating the required fields, and saving your contact preferences.

You can also download your list of cases as a Microsoft Excel file by clicking the **Export as Microsoft Excel** option.

Click the **Ask the bot** option next to a case to get assistance from the Cisco bot for a particular case. You can view the summary of a case by the clicking the summary link. The **Summary** tab in the **Case Summary** window that is displayed contains an overview of the case. Some fields can be edited to update information about the case. In the **Notes** tab, you can view a list of notes, including updates from TAC on this case.

Click **Add Notes** to add a note of your own to the case, **Add Files** to upload files such as debug logs or support bundles to support your case. Use **Save as PDF** to download your case summary as a PDF file.

Health Check

Cisco ISE has an on-demand health check option to diagnose all the nodes in your Cisco ISE deployment. Running a health check on all the nodes before any operation helps to reduce the downtime and improve the overall functionality of Cisco ISE system by identifying critical issues, if any. Health Check provides the working status of a component and displays troubleshooting recommendations regarding issues, if any, in your deployment.

Table 201: Health Check Deployment

Deployment Type	Description
Platform Support Check	Checks the supported platforms in the deployment. A platform that does not meet the recommended requirement specification may cause performance issues. Checks the 34xx and other unsupported platform details and checks if the system has a minimum of 12 core CPU, 300-GB hard disk, 16-GB memory.
Deployment Validation	Checks if the state-of-the-deployment node is in sync or in progres.
DNS Resolvability	Checks for the forward and reverse lookup of host name and IP address. Both forward and reverse DNS resolutions are recommended for deployment Health Check to function properly.
Trust Store Certificate Validation	Checks if your Trust Store certificate is valid or has expired. Delete or renew unused or expired certificates to ensure optimum Cisco ISE functionality.
System Certificate Validation	Checks the system certificate validation for each node. Delete or renew unused or expired certificates to ensure optimum Cisco ISE functionality.
Disk Space Check	Checks the hard disk located in the Platform Support Check, and the free space available in the disk for further upgrade procedures. We recommend that you run a Disk Space Check before you begin the upgrade operation to avoid performance issues.

Deployment Type	Description
NTP Reachability and Time Source Check	Checks the NTP configured in the system and whether the time source is the NTP server. NTP synchronization is essential for Cisco ISE services such as AD operations, upgrade workflows, and so on.
Load Average Check	Checks system load at specified intervals. The valid interval configurations are 1, 5, and 15 minutes. Load Average Check failures could lead to performance issues in Cisco ISE.
MDM Validation	Checks for connectivity between the configured MDM servers and Cisco ISE PSN servers. To use the MDM-supported features in Cisco ISE, the MDM Validation Check must be successful.
License Validation	Checks if Smart Licensing is configured and valid. If your smart licences are not configured or are valid, a warning is displayed in the Cisco ISE GUI asking you to configure and validate your licenses. Cisco ISE Release 3.0 and later releases support only Smart Licensing. Convert your traditional licenses to smart licenses before you upgrade to Cisco ISE Release 3.0 and later releases.
Services or Process Failures	Checks if the status of a service or application is in Running or Failed state.
I/O Bandwidth Performance Check	Checks for the disk read and write speeds to avoid any Cisco ISE performance issues.

Note The numbers adjacent to the deployment indicates the number of nodes and their health check details. For example, if a deployment has 0/2, 0 indicates the number of nodes that are in Failed, In progress, and Completed and 2 indicates the number of nodes in the deployment. During the health check, if any node does not send back response for 15 minutes, health check for that specific node gets timed out.

Run Health Check

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Health Checks**.

Step 2 Click **Start health checks**.

An information pop-up window displays the following message:

```
Health Checks triggered.
```

Step 3 Click **Ok** to view the status.

Step 4 In the **Health Checks** window, you will be able to view the health status of each component. The following colors indicate the health status of a corresponding Cisco ISE component:

Color	Health Status	Action
Red	Not Good	Click the drop-down option to view the troubleshooting recommendations. We recommend that you resolve these issues because you cannot proceed with operations such as the Upgrade workflow until these issues are resolved.
Orange	Good	Click the drop-down option to view the troubleshooting recommendations that are available in the box. When the health status of a component is good to perform an operation and you can proceed with the upgrade workflow, we recommend that you resolve the issues indicated in orange before you proceed because these issues too might impact Cisco ISE functionalities.
Green	Good	No action is required.
Blue	Good	Click the information icon to view the critical information about the functionality.

Step 5 Click **Download report**.

A HealthChecksReport.json file is saved on your local system with detailed health status information of your Cisco ISE deployment.

After the health check is triggered, the status is retained in the **Health Check** window for next three hours. You will not be able to run health check until the **Health Checks** window is refreshed or has expired.

Network Privilege Framework Event Flow Process

The Network Privilege Framework (NPF) authentication and authorization event flow uses the process described in the following table:

Process Stage	Description
1	Network Access Device (NAD) performs either a normal authorization or a flex authorization.
2	An unknown agentless identity is profiled with web authorization.
3	A RADIUS server authenticates and authorizes the identity.
4	Authorization is provisioned for the identity at the port.
5	Unauthorized endpoint traffic is dropped.

User Roles and Permissions for Monitoring and Troubleshooting Capabilities

Monitoring and troubleshooting capabilities are associated with default user roles. The tasks you are allowed to perform are directly related to your assigned user role.

See Cisco ISE Administrator Groups, on page 17 for information on the permissions and restrictions set for each user role.

Note Accessing Cisco ISE using the root shell without Cisco TAC supervision is not supported, and Cisco is not responsible for any service disruption that might be caused as a result.

Data Stored in the Monitoring Database

The Cisco ISE monitoring service collects and stores data in a specialized monitoring database. The rate and amount of data utilized to monitor network functions may require a node dedicated solely to monitoring. If your Cisco ISE network collects logging data at a high rate from policy service nodes or network devices, we recommend a Cisco ISE node dedicated to monitoring.

To manage the information stored in the monitoring database, perform full and incremental backups of the database. This includes purging unwanted data and then restoring the database.

Cisco ISE Telemetry

Telemetry monitors your system and the devices in your network to provide feedback to Cisco on how you use the product. Cisco uses this information to improve the product.

Cisco ISE telemetry data communication occurs as HTTPS traffic through Port 443 with https://connectdna.cisco.com/.

Telemetry is enabled by default. To disable this feature:

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Network Success Diagnostics** > **Telemetry**
2. Uncheck the **Enable Telemetry** check box to disable telemetry.

   - **Cisco Account**: Enter your Cisco account credentials so that you can get emails from Telemetry. We may also use this ID to contact you if Telemetry finds any serious issues that may affect your Cisco ISE deployment..
   - **Transport Gateway**: You can use a proxy between your Cisco ISE and the Cisco external telemetry servers for extra security. To do this, check this check box and enter the FQDN of your proxy server. Telemetry does not require a proxy.

     Cisco provides software for Transport Gateway. You can download from cisco.com. This software runs on a Linux server. See the Smart Call Home Deployment Guide for information on how to deploy the Transport Gateway software on an *RHEL server*. If you are using this Cisco software, the URL value is **<FQDN of proxyserver>/Transportgateway/services/DeviceRequestHandler**.

     You can use this gateway to connect to the Smart Licensing server, too. From Version 3.5 of the Transport Gateway, you cannot change the port, but you can enter IP address instead of the FQDN.

Information that Telemetry Gathers

Telemetry sends the following information to Cisco.

Nodes:

For each Policy Administration Node (PAN)

- Current number of postured endpoints
- Current number of PxGrid clients
- Current number of endpoints managed by MDM
- Current number of Guest users
- Start and end date of this telemetry record
- FIPS status

For each Policy Service Node (PSN)

- Number of profiler probes
- Node service type
- Passive ID used

For All nodes

- Total and Active NADs
- Number of CPU cores
- VM available disk space
- VM memory and CPU settings
- System name
- Serial number
- VID and PID
- Uptime
- Last CLI login

MnT node count

pxGrid node count

Licenses

- Have any licenses expired?
- Number of Cisco ISE Essentials licenses available, maximum ever used
- Number of Cisco ISE Advantage licenses available, maximum ever used

- Number of Cisco ISE Premier licenses available, maximum ever used
- Is an evaluation license in use?
- Name of the smart account
- Number of TACACS devices
- Expiration date, remaining days, license term
- Service types, primary and secondary UDI

Posture

- Number of inactive policies
- Last posture feed update
- Number of active policies
- Posture feed updates

Guest Users

- Maximum number of authenticated guests for the day
- Maximum number of active guests for the day
- Maximum number of BYOD users for the day
- External ID information for authenticated guests

Network Access Devices (NAD)

- Authorization: Activated ACLs, VLANS, Policy size
- NDG map and NAD hierarchy
- Authentication:
  - Number of RADIUS, RSA ID, LDAP, ODBC, and Active Directory ID stores
  - Number of local (nonadmin) users
  - NDG map and NAD map
  - Number of policy lines

For authorizations, active VLANs, policy count, number of activated ACLs:

- Status, VID, PT
- Average load, memory usage
- Number of PAP, MnT, pxGrid, and PIC nodes
- Name, profile name, profile ID

NAD Profile

For each NAD profile:

- Name and ID
- Cisco device
- TACACS support
- RADIUS support
- Trustsec support
- Default profile

Profiler

- Date of last feed update
- Are automatic updates enabled?
- Endpoints profiled, endpoint type, unknown endpoints, percentage unknown, and total endpoint count
- Number of custom profiles
- Serial number, scope, endpoint types, custom profiles

Mobile Device Management (MDM)

- List of MDM nodes
- For a date range, current MDM endpoint count, current guest user count, current postured users count
- pxGrid client count
- Node count

Patch and Hot Patch

- Node FQDN
- Cisco ISE version
- Names and installation status of patches and hot patches

SNMP Traps to Monitor Cisco ISE

SNMP traps help you to monitor the status of Cisco ISE. If you want to monitor Cisco ISE without accessing the Cisco ISE server, you can configure a MIB browser as an SNMP host in Cisco ISE. You can then monitor the status of Cisco ISE from the MIB browser.

See the Cisco Identity Services Engine CLI Reference Guide for information on the **snmp-server host** and **snmp-server trap** commands.

Cisco ISE supports SNMPv1, SNMPv2c, and SNMPv3.

Cisco ISE sends the following generic system traps if you configure the SNMP host from the CLI:

- Cold start: When the device reboots.
- Linkup: When Ethernet interface is up.

- Linkdown: When Ethernet interface is down.
- Authentication failure: When the community strings do not match.

The following table lists the generic SNMP traps that are generated by default in Cisco ISE.

OID	**Description**	**Trap Example**
.1.3.6.1.4.1.8072.4.0.3 \n NET-SNMP-AGENT-MIB::nsNotifyRestart	Indicates that the agent has been restarted.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (478) 0:00:04.78 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyRestart SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpNotificationPrefix
.1.3.6.1.4.1.8072.4.0.2 \n NET-SNMP-AGENT-MIB::nsNotifyShutdown	Indicates that the agent is in the process of being shut down.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyShutdown SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpNotificationPrefix
.1.3.6.1.6.3.1.1.5.4 \n IF-MIB::linkUp	Signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the Down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (478) 0:00:04.78 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkUp IF-MIB::ifIndex.12 = INTEGER: 12 IF-MIB::ifAdminStatus.12 = INTEGER: up(1) IF-MIB::ifOperStatus.12 = INTEGER: up(1) SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
.1.3.6.1.6.3.1.1.5.3 \n IF-MIB::linkDown	Signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the Down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkDown IF-MIB::ifIndex.5 = INTEGER: 5 IF-MIB::ifAdminStatus.5 = INTEGER: up(1) IF-MIB::ifOperStatus.5 = INTEGER: down(2) SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10

OID	Description	Trap Example
.1.3.6.1.6.3.1.1.5.1 \n SNMPv2-MIB::coldStart	Signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8) 0:00:00.08 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-MIB::coldStart SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10

Process-Monitoring SNMP Traps in Cisco ISE

Cisco ISE allows you to send hrSWRunName traps for Cisco ISE process statuses to the SNMP manager if you configure an SNMP host from the Cisco ISE CLI. Cisco ISE uses a cron job to trigger these traps. The cron job retrieves the Cisco ISE process status from Monit. After you configure the **SNMP-Server Host** command from the CLI, a cron job runs every five minutes and monitors Cisco ISE.

Note When an ISE process is manually stopped by an admin, Monit for the process also stops and no traps are sent to the SNMP manager. A process-stop SNMP trap is sent to the SNMP manager only when a process accidentally shuts down and is not automatically revived.

The following is a list of process-monitoring SNMP traps in Cisco ISE.

OID	Description	Trap Example
.1.3.6.1.2.1.25.4.2.1.2 \n HOST-RESOURCES-MIB::hrSWRunName	A textual description of this running piece of software, including the manufacturer, revision, and the name by which it is commonly known. If this software was installed locally, this must be the same string as that used in the corresponding hrSWInstalledName. The services considered are app-server, rsyslog, redis-server, ad-connector, mnt-collector, mnt-processor, ca-server est-server, and elasticsearch.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (63692139) 7 days, 8:55:21.39 SNMPv2-MIB::snmpTrapOID.0 = OID: HOSTRESOURCES- MIB::hrSWRunName HOSTRESOURCES- MIB::hrSWRunName = STRING: "redis-server:Running"

Cisco ISE sends traps for the following statuses to the configured SNMP server:

- Process Start (monitored state)
- Process Stop (not monitored state)
- Execution Failed: When the process state changes from Monitored to Execution Failed, a trap is sent.
- Does Not Exist: When the process state changes from Monitored to Does Not Exist, a trap is sent.

A unique object ID (OID) is generated for every object in the SNMP server and a value is assigned to the OID. You can find the object with its OID value in the SNMP server. The OID value for a running trap is *running*, and the OID value for the Not monitored, Does not exist, and Execution failed traps is *stopped*.

Cisco ISE sends traps using the OID of hrSWRunName that belongs to the HOST-RESOURCES MIB, and sets the OID value as < *PROCESS NAME* > - < *PROCESS STATUS* >, for example, runtime - running.

To stop Cisco ISE from sending SNMP traps to the SNMP server, remove the SNMP configuration from the Cisco ISE CLI. This operation stops sending SNMP traps and polling from the SNMP manager.

Disk Utilization SNMP Traps in Cisco ISE

When a Cisco ISE partition reaches its threshold disk utilization limit and the configured amount of free space is reached, the disk utilization trap is sent.

The following is a list of disk utilization SNMP traps that can be configured in Cisco ISE:

OID	Description	Trap Example
.1.3.6.1.4.1.2021.9.1.9 \n UCD-SNMP-MIB::dskPercent	Percentage of space used in the disk.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (118198297) 13 days, 16:19:42.97 SNMPv2-MIB::snmpTrapOID.0 = OID: UCD-SNMP-MIB::dskPercent UCD-SNMP-MIB::dskPercent = INTEGER: 13
.1.3.6.1.4.1.2021.9.1.2 \n UCD-SNMP-MIB::dskPath	Path where the disk is mounted. dskPath can send traps for all the mount points in the output of the ISE admin command **show disks**.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (118198304) 13 days, 16:19:43.04 SNMPv2-MIB::snmpTrapOID.0 = OID: UCD-SNMP-MIB::dskPath UCD-SNMP-MIB::dskPath = STRING: /opt

Cisco ISE Alarms

Alarms notify you of critical conditions on a network and are displayed in the Alarms dashlet. They also provide information on system activities, such as data purge events. You can either configure how you want to be notified about system activities, or disable them entirely. You can also configure the threshold for certain alarms.

Most alarms do not have an associated schedule and are sent immediately after an event occurs. At any given point in time, only the latest 15,000 alarms are retained.

If the event recurs, the same alarms are suppressed for about an hour. During the time that the event recurs, depending on the trigger, it may take about an hour for the alarms to reappear.

You can filter the alarms you want to view based on alarm name, category, severity, or status. As you select filters, the effects are additive, also referred to as cascading filter, which allows you to drill down to find the particular data you are looking for.

The **Quick Filter** allows you to enter a value for any of the field attributes displayed in the listing page, refreshes the page, and lists only those records that match your filter criteria.

The **Advanced Filter** allows you to filter information based on specified conditions, such as, *Alarm Name contains TrustSec*. You can specify more than one condition.

You can create and save user-specific custom filters that are accessible only to you.

Click **Clear All Filters** to remove all the applied filters.

The following table lists all the Cisco ISE alarms, descriptions, and resolutions.

Table 202: Cisco ISE Alarms

Alarm Name	Alarm Description	Alarm Resolution
Administrative and Operational Audit Management		
Deployment Upgrade Failure	An upgrade has failed on an ISE node.	Check ADE.log on the failed node for upgrade failure reason and corrective actions.
Upgrade Bundle Download failure	An upgrade bundle download has failed on an ISE node.	Check ADE.log on the failed node for upgrade failure reason and corrective actions.
SXP Connection Failure	SXP connection has failed.	Verify that the SXP service is running. Check the peer for compatibility.
Cisco profile applied to all devices	Network device profiles define the capabilities of network access devices, such as MAB, Dot1X, CoA, and Web Redirect.	Consider editing the configuration of non-Cisco network devices to assign the appropriate profile.
Secure LDAP connection reconnect due to CRL found revoked certificate	CRL check result indicates that the certificate used for LDAP connection is revoked.	Check the CRL configuration and verify that it is valid. Check that the LDAP server certificate and its issuer certificates are not revoked. If revoked, issue a new certificate and install it on the LDAP server.
Secure LDAP connection reconnect due to OCSP found revoked certificate	OCSP check result indicates that the certificate used for LDAP connection is revoked.	Check the OCSP configuration and verify that it is valid. Check that the LDAP server certificate and its issuer certificates are not revoked. If revoked, issue a new certificate and install it on the LDAP server.
Secure syslog connection reconnect due to CRL found revoked certificate	CRL check result indicates that the certificate used for syslog connection is revoked.	Check the CRL configuration and verify that it is valid. Check that the syslog server certificate and its issuer certificates are not revoked. If revoked, issue a new certificate and install it on the syslog server.

Alarm Name	Alarm Description	Alarm Resolution
Secure syslog connection reconnect due to OCSP found revoked certificate	OCSP check result indicates that the certificate used for syslog connection is revoked.	Check the OCSP configuration and verify that it is valid. Check that the syslog server certificate and its issuer certificates are not revoked. If revoked, issue a new certificate and install it on the syslog server.
Administrator account Locked/Disabled	Administrator account is locked or disabled because of password expiration or incorrect login attempts. For more details, refer to the administrator password policy.	Administrator password can be reset by another administrator using the GUI or CLI.
ERS identified deprecated URL	ERS-identified deprecated URL	The request URL is deprecated and we recommend that you avoid using it.
ERS identified out-dated URL	ERS-identified outdated URL	The requested URL is outdated and we recommend that you use a newer one. The outdated URL will not be removed in future releases.
ERS request content-type header is outdated	ERS request content-type header is outdated.	The request resource version stated in the request content-type header is outdated. This means that the resource schema has been modified. One or more attributes may have been added or removed. To overcome that with the outdated schema, the ERS engine will use default values.
ERS XML input is a suspect for XSS or Injection attack	ERS XML input is a suspect for XSS or injection attack.	Review your XML input.
Backup Failed	The ISE backup operation failed.	Check the network connectivity between Cisco ISE and the repository. Ensure that: • The credentials used for the repository are correct. • There is sufficient disk space in the repository. • The repository user has write privileges.
CA Server is down	CA server is down.	Check to make sure that the CA services are up and running on the CA server.
CA Server is Up	CA server is up.	A notification is issued to inform the administrator that the CA server is up.
Certificate Expiration	This certificate will expire soon. When it expires, Cisco ISE may fail to establish secure communication with clients.	Replace the certificate. For a trust certificate, contact the issuing Certificate Authority (CA). For a CA-signed local certificate, generate a CSR and have the CA create a new certificate. For a self-signed local certificate, use Cisco ISE to extend the expiration date. You can delete the certificate if it is no longer used.

Alarm Name	Alarm Description	Alarm Resolution
Certificate Revoked	Administrator has revoked the certificate issued to an endpoint by the internal CA.	Go through the BYOD flow again from the start to be provisioned with a new certificate.
Certificate Provisioning Initialization Error	Certificate provisioning initialization failed.	More than one certificate found with the same value of CN (CommonName) attribute in the subject. Cannot build certificate chain. Check all the certificates in the system, including those from the SCEP (Simple Certificate Enrollment Protocol) server.
Certificate Replication Failed	Certificate replication to secondary node failed.	The certificate is not valid on the secondary node, or there is some other permanent error condition. Check the secondary node for a pre-existing, conflicting certificate. If found, delete the pre-existing certificate on the secondary node, and export the new certificate on the primary node, delete it, and import it in order to reattempt replication.
Certificate Replication Temporarily Failed	Certificate replication to secondary node temporarily failed.	The certificate was not replicated to a secondary node because of a temporary condition such as a network outage. The replication is retried until it succeeds.
Certificate Expired	This certificate has expired. Cisco ISE may fail to establish secure communication with clients. Node-to-node communication may also be affected.	Replace the certificate. For a trust certificate, contact the issuing Certificate Authority (CA). For a CA-signed local certificate, generate a CSR and have the CA create a new certificate. For a self-signed local certificate, use Cisco ISE to extend the expiration date. You can delete the certificate if it is no longer used.
Certificate Request Forwarding Failed	Certificate request forwarding failed.	Make sure that the certificate request that is coming in matches the attributes from the sender.
Configuration Changed	Cisco ISE configuration is updated. This alarm is not triggered for any configuration change in users and endpoints.	Check if the configuration change is expected.
CRL Retrieval Failed	Unable to retrieve CRL from the server. This occurs if the specified CRL is unavailable.	Ensure that the download URL is correct and is available for the service.
DNS Resolution Failure	DNS resolution failed on the node.	Check if the DNS server configured by the **ip name-server** command is reachable. If you get the alarm as **DNS Resolution failed for CNAME <hostname of the node>**, ensure that you create CNAME RR along with the A record for each Cisco ISE node.

Alarm Name	Alarm Description	Alarm Resolution
Firmware Update Required	A firmware update is required on this host.	Contact Cisco TAC to obtain firmware update.
Insufficient Virtual Machine Resources	Virtual Machine (VM) resources such as CPU, RAM, disk space, or IOPS (Input/output operations per second) are insufficient on this host.	Ensure that the minimum requirements for the VM host, as specified in the *Cisco ISE Hardware Installation Guide*.
NTP Service Failure	The NTP service is down on this node.	This could be because there is a large time difference between the NTP server and a Cisco ISE node (more than 1000 seconds). Ensure that your NTP server is working properly and use the **ntp server** <*servername*> CLI command to restart the NTP service and fix the time gap.
NTP Sync Failure	All the NTP servers configured on this node are unreachable.	Run the **show ntp** command from the CLI for troubleshooting. Ensure that the NTP servers are reachable from Cisco ISE. If NTP authentication is configured, ensure that the key ID and value matches with that of the server.
No Configuration Backup Scheduled	No Cisco ISE configuration backup is scheduled.	Create a schedule for configuration backup.
Operations DB Purge Failed	Unable to purge older data from the operations database. This occurs if the MnT nodes are busy.	Check the Data Purging Audit report and ensure that the used space is lesser than the threshold space. Log in to the MnT nodes using the CLI and perform the purge operation manually.
Profiler SNMP Request Failure	Either the SNMP request timed out, or the SNMP community or user authentication data is incorrect.	Ensure that SNMP is running on the NAD and verify that SNMP configuration on Cisco ISE matches with NAD.
Restore Failed	Cisco ISE restore operation failed.	Ensure network connectivity between Cisco ISE and the repository. Ensure that the credentials used for the repository is correct. Also ensure that the backup file is not corrupted. Execute the **reset-config** command from the CLI and restore the last-known good backup.
Patch Failure	A patch process has failed on the server.	Reinstall the patch process on the server.
Patch Success	A patch process has succeeded on the server.	—
External MDM Server API Version Mismatch	External MDM server API version does not match with what is configured in Cisco ISE.	Ensure that the MDM server API version is the same as what is configured in Cisco ISE. Update the Cisco ISE MDM server configuration, if needed.

Alarm Name	Alarm Description	Alarm Resolution
External MDM Server Connection Failure	Connection to the external MDM server failed.	Ensure that the MDM server is up and the Cisco ISE-MDM API service is running on the MDM server.
External MDM Server Response Error	External MDM server response error.	Ensure that the Cisco ISE-MDM API service is running properly on the MDM server.
MDM Compliance Polling Disabled	Periodic compliance polling received huge non-compliance device information.	Keep the number of non-compliant device requests reaching the MDM server below 20000.
Endpoint certificates expired	Endpoint certificates were marked expired by daily the scheduled job.	Re-enroll the endpoint device to get a new endpoint certificate.
Endpoint certificates purged	Expired endpoint certificates were purged by the daily scheduled job.	No action is needed. This is an administrator-initiated clean-up operation.
Endpoints Purge Activities	Purge the activities on endpoints for the past 24 hours. This alarm is triggered at midnight.	Review the purge activities by choosing **Operations** > **Reports** > **Endpoints and Users** > **Endpoint Purge Activities**.
PAN Auto Failover - Failover Failed	Promotion request to the Secondary Administration Node failed.	See the alarm details for further action.
PAN Auto Failover - Failover Triggered	Successfully triggered the failover of the Secondary Administration Node to Primary role.	Wait for the promotion of secondary PAN to complete, and bring up the old primary PAN.
PAN Auto Failover - Health Check Inactivity	PAN did not receive the health check monitoring request from the designated monitoring node.	Verify if the reported monitoring node is down or out-of-sync, and trigger a manual synchronization, if needed.
PAN Auto Failover - Invalid Health Check	Invalid health check monitoring request received for auto failover.	Verify if the health check monitoring node is out-of-sync, and trigger a manual synchronization if needed.
PAN Auto Failover - Primary Administration Node Down	PAN is down or is not reachable from the monitoring node.	Bring up the PAN, or wait for failover to happen.
PAN Auto Failover - Rejected Failover Attempt	Secondary administration node rejected the promotion request made by the health check monitor node.	See the alarm details for further action.
EST Service is down	EST service is down.	Make sure that the CA and EST services are up and running, and that the certificate services endpoint sub CA certificate chain is complete.
EST Service is up	EST service is up.	A notification is sent to inform the administrator that the EST service is up.
Smart Call Home Communication Failure	Smart Call Home messages were not sent successfully.	Ensure that there is network connectivity between Cisco ISE and Cisco Systems.

Alarm Name	Alarm Description	Alarm Resolution
Telemetry Communication Failure	Telemetry messages were not sent successfully.	Ensure that there is network connectivity between Cisco ISE and Cisco Systems.
Adapter not reachable	Cisco ISE cannot connect to the adapter.	Check the adapter logs for more details about the failure.
Adapter Error	Adapter has encountered an error.	Check the description of the alarm.
Adapter Connection Failed	The adapter cannot connect to the source server.	Ensure that the source server is reachable.
Adapter Stopped Due to Error	The adapter has encountered an error and is not in the desired state.	Ensure that the adapter configuration is correct and the source server is reachable. See the adapter logs for more details about the error.
Service Component Error	The service component has encountered an error.	Check the description of the alarm.
Service Component Info	The service component has sent a notification.	None.
ISE Services		
Excessive TACACS Authentication Attempts	The ISE Policy Service nodes are experiencing higher than expected rate of TACACS authentications.	• Check the re-auth timer in the network devices. • Check the network connectivity of the ISE infrastructure.
Excessive TACACS Authentication Failed Attempts	The ISE Policy Service nodes are experiencing higher than expected rate of failed TACACS authentications.	• Check the authentication steps to identify the root cause. • Check the ISE or NAD configuration for Identity and Secret mismatch.
MSE Location Server accessible again	MSE Location Server is accessible again.	None.
MSE Location Server not accessible.	MSE Location Server is not accessible, or is down.	Check if the MSE Location Server is up and running and is accessible from the ISE nodes.
AD Connector had to be restarted	AD Connector stopped unexpectedly and had to be restarted.	If this issue persists, contact Cisco TAC for assistance.
Active Directory Forest is unavailable	Active Directory forest Global Catalog is unavailable, and cannot be used for authentication, authorization, and group and attribute retrieval.	Check DNS configuration, Kerberos configuration, error conditions, and network connectivity.
Authentication domain is unavailable	Authentication domain is unavailable, and cannot be used for authentication, authorization and group and attribute retrieval.	Check DNS configuration, Kerberos configuration, error conditions, and network connectivity.

Alarm Name	Alarm Description	Alarm Resolution
Authorization Result	Monitor authorization results and active sessions. See Configure Authorization Result Alarm, on page 1371.	Check your network or Cisco ISE configuration changes for any discrepancies.
ISE Authentication Inactivity	Cisco ISE policy service nodes are not receiving authentication requests from the network devices.	• Check the Cisco ISE and NAD configuration. • Check the network connectivity of the Cisco ISE and NAD infrastructure.
ID Map. Authentication Inactivity	No user authentication events were collected by the Identity Mapping Service in the last 15 minutes.	If user authentications are expected during this time, for example, during work hours, check the connection to the Active Directory domain controllers.
CoA Failed	Network device has denied the Change of Authorization (CoA) request issued by the Cisco ISE policy service nodes.	Ensure that the network device is configured to accept CoA from Cisco ISE. Check if CoA is issued on a valid session.
Configured nameserver is down	Configured nameserver is down or unavailable.	Check DNS configuration and network connectivity.
Supplicant Stopped Responding	Cisco ISE sent last message to the client 120 seconds ago, but there is no response from the client.	• Verify that the supplicant is configured properly to conduct a full EAP conversation with Cisco ISE. • Verify that NAS is configured properly to transfer EAP messages to and from the supplicant. • Verify that the supplicant or NAS does not have a short timeout for EAP conversation.
Excessive Authentication Attempts	Cisco ISE policy service nodes are experiencing higher than expected rate of authentications.	Check the reauthorization timer in the network devices. Check the network connectivity of the Cisco ISE infrastructure. After the threshold is met, the Excessive Authentication Attempts and Excessive Failed Attempts alarms are triggered. The numbers displayed next to the **Description** column are the total number of authentications that have succeeded or failed against Cisco ISE in the last 15 minutes.

Alarm Name	Alarm Description	Alarm Resolution
Excessive Failed Attempts	Cisco ISE policy service nodes are experiencing higher than expected rate of failed authentications.	Check the authentication steps to identify the root cause. Check the Cisco ISE or NAD configuration for identity and secret mismatch. After the threshold is met, the Excessive Authentication Attempts and Excessive Failed Attempts alarms are triggered. The numbers displayed next to the **Description** column are the total number of authentications that have succeeded or failed against Cisco ISE in the last 15 minutes.
AD: Machine TGT refresh failed	ISE server Ticket Granting Ticket (TGT) refresh has failed. The TGT is used for Active Directory connectivity and services.	Check that the ISE machine account exists and is valid. Also check for possible clock skew, replication, Kerberos configuration, or network errors, or all of them.
AD: ISE account password update failed	ISE server has failed to update it's AD machine account password.	Check that the ISE machine account password is not changed and that the machine account is not disabled or restricted. Check the connectivity to KDC.
Joined domain is unavailable	Joined domain is unavailable, and cannot be used for authentication, authorization, and group and attribute retrieval.	Check DNS configuration, Kerberos configuration, error conditions, and network connectivity.
Identity Store Unavailable	Cisco ISE policy service nodes are unable to reach the configured identity stores.	Check the network connectivity between Cisco ISE and the identity stores.
Misconfigured Network Device Detected	Cisco ISE has detected too many RADIUS accounting information from NAS. This alarm is disabled by default. To enable this alarm, see Enable and Configure Alarms.	Too much duplicate RADIUS accounting information has been sent to ISE from NAS. Configure NAS with accurate accounting frequency.
Misconfigured Supplicant Detected	Cisco ISE has detected misconfigured supplicant on the network. This alarm is disabled by default. To enable this alarm, see Enable and Configure Alarms.	Ensure that the configuration on the supplicant is correct.
No Accounting Start	Cisco ISE policy service nodes have authorized a session, but did not receive accounting start from the network device.	Ensure that RADIUS accounting is configured on the network device. Check the network device configuration for local authorization.

Alarm Name	Alarm Description	Alarm Resolution
Unknown NAD	Cisco ISE policy service nodes are receiving authentication requests from a network device that is not configured in Cisco ISE.	Check if the network device is a genuine request and add it to the configuration. Ensure that the secret matches.
SGACL Drops	Secure Group Access (SGACL) drops occurred. This occurs if a Trustsec-capable device drops packets because of SGACL policy violations.	Run the RBACL drop summary report and review the source causing the SGACL drops. Issue a CoA to the offending source to reauthorize or disconnect the session.
RADIUS Request Dropped	The authentication and accounting request from a NAD is silently discarded. This may occur because of unknown NAD, mismatched shared secrets, or invalid packet content per RFC. This alarm is disabled by default. To enable this alarm, see Enable and Configure Alarms.	Check that the NAD/AAA client has a valid configuration in Cisco ISE. Check whether the shared secrets on the NAD/AAA client and Cisco ISE match each other. Ensure that the AAA client and the network device, have no hardware problems or problems with RADIUS compatibility. Also, ensure that the network that connects the device to Cisco ISE has no hardware problems.
EAP Session Allocation Failed	A RADIUS request was dropped because EAP sessions limit is reached. This condition can be caused by too many parallel EAP authentication requests.	Wait for a few seconds before invoking another RADIUS request with a new EAP session. If system overload continues to occur, try restarting the ISE server.
RADIUS Context Allocation Failed	A RADIUS request was dropped due to system overload. This condition can be caused by too many parallel authentication requests.	Wait for a few seconds before invoking a new RADIUS request. If system overload continues to occur, try restarting the ISE server.
AD: ISE machine account does not have the required privileges to fetch groups	Cisco ISE machine account does not have the required privileges to fetch groups.	Check if the Cisco ISE machine account has rights to fetch user groups in the Active Directory.
Posture Configuration Detection	The posture state synchronization port is not blocked for compliant authorization profiles.	Configure an ACL to block the posture state synchronization probe from reaching Cisco ISE if the client posture status is compliant.
Posture Query to MnT Lookup is High	Posture query for MnT session lookup is high per hour.	Check the network configuration and ensure that the PSNs cannot be reached from any client that is outside the ISE network.
Node Replication		
Slow Replication Info	Slow or stuck replication is detected when the pending message count is greater than 10000 or the time taken to replicate messages exceeds an hour.	Verify that the node is reachable, is a part of the deployment, and validate if it is under high load.

Alarm Name	Alarm Description	Alarm Resolution
Slow Replication Warning	Slow or stuck replication is detected when the pending message count is greater than 20000 or the time taken to replicate messages exceeds three hours.	Verify that the node is reachable, is a part of the deployment, and validate if it is under high load.
Slow Replication Error	Slow or stuck replication is detected when the pending message count is greater than 40000 or the time taken to replicate messages exceeds five hours.	Verify that the node is reachable, is a part of the deployment, and validate if it is under high load.
Replication Failed	The secondary node failed to consume the replicated message.	Log in to the Cisco ISE GUI and perform a manual synchronization from the **Deployment** window or deregister and register the affected Cisco ISE node.
Replication Stopped	The Cisco ISE node could not replicate configuration data from the PAN.	Log in to the Cisco ISE GUI to perform a manual synchronization from the **Deployment** window or deregister and register the affected Cisco ISE node with the required field.
System Health		
High Disk I/O Utilization	Cisco ISE system is experiencing high disk I/O utilization.	Check if the system has sufficient resources. Check the actual amount of work on the system, for example, number of authentications, profiler activity, and so on. Add an additional server to distribute the load.
High Disk Space Utilization	Cisco ISE system is experiencing high disk space utilization.	Check if the system has sufficient resources. Check the actual amount of work on the system, for example, number of authentications, profiler activity, and so on. Add an additional server to distribute the load.

Alarm Name	Alarm Description	Alarm Resolution
High Load Average	Cisco ISE system is experiencing high load average.	Check if the system has sufficient resources. Check the actual amount of work on the system, for example, number of authentications, profiler activity, and so on. Add an additional server to distribute the load. Do not use third-party tools to check the load average on a single CPU core because this metric would not reflect the overall system load. We recommend that you use the **tech top** command in the Cisco ISE CLI for a cumulative view of the system load. If the High Load Average alarm is seen against 2:00 a.m. time stamps for Primary and Secondary MnT nodes, note that CPU usage might be high due to DBMS statistics being run at that hour. CPU usage will be back to normal after the DBMS stats is complete. A High Load Average alarm is triggered at 1:00 a.m. every Sunday by a weekly maintenance task. This maintenance task rebuilds all the indexes that occupy more than 1 GB space. This alarm can be ignored.
High Memory Utilization	Cisco ISE system is experiencing high memory utilization. This alarm is triggered when memory utilization has reached its threshold. The default threshold value is 90% (MEMORY_UTILIZATION=90). Though this can be configured, we recommend that you do not change the default threshold value.	Check if the system has sufficient resources. Check the actual amount of work on the system, for example, number of authentications, profiler activity, and so on. Add an additional server to distribute the load. We recommend that you use the **show memory** command in the Cisco ISE CLI to check memory utilization. In a Cisco ISE node, its operating system manages memory utilization. You must check for the available memory (instead of free memory) metric for a more reliable measure of memory utilization. Note that an operating system segments most of the memory in buffer or cache. If less than 90% of the total memory is displayed as used, and there is no substantial increase in swap memory, Cisco ISE memory utilization can be considered stable.
High Operations DB Usage	Cisco ISE monitoring nodes are experiencing higher volume of syslog data than expected.	Check and reduce the purge configuration window for the operations data.

Alarm Name	Alarm Description	Alarm Resolution
High Authentication Latency	Cisco ISE system is experiencing high authentication latency.	Check if the system has sufficient resources. Check the actual amount of work on the system, for example, number of authentications, profiler activity, and so on. Add an additional server to distribute the load.
Health Status Unavailable	The monitoring node has not received the health status from the Cisco ISE node.	Ensure that Cisco ISE nodes are up and running, and are able to communicate with the monitoring nodes.
Process Down	One of the Cisco ISE processes is not running.	Restart the Cisco ISE application.
Profiler Queue Size Limit Reached	The ISE Profiler Queue Size Limit has been reached. Events received after reaching the queue size limit will be dropped.	Check if the system has sufficient resources, and ensure that the EndPoint attribute filter is enabled.
OCSP Transaction Threshold Reached	The OCSP transaction threshold has been reached. This alarm is triggered when the internal OCSP service transaction has reached its threshold.	Check if the system has sufficient resources.
Licensing		
License About to Expire	License installed on the Cisco ISE nodes are about to expire.	See the **Licencing** window in Cisco ISE to view the license usage.
License Expired	License installed on the Cisco ISE nodes has expired.	Contact the Cisco Accounts team to purchase new licenses.
License Violation	Cisco ISE nodes have detected that you are exceeding or are about to exceed the allowed license count.	Contact the Cisco Accounts team to purchase additional licenses.
Smart Licensing Authorization Expired	Authorization for Smart Licensing has expired.	See the **Cisco ISE License Administration** window to manually renew registration for Smart Licensing or check your network connectivity with Cisco Smart Software Manager. Contact your Cisco partner if the issue persists.
Smart Licensing Authorization Renewal Failure	Renewal of authorization with Cisco Smart Software Manager has failed.	See the **Cisco ISE License Administration** window to manually renew authorization with Cisco Smart Software Manager using the **Refresh** button in the **Licenses** table. Contact your Cisco partner if issue persists.
Smart Licensing Authorization Renewal Success	Renewal of authorization with Cisco Smart Software Manager was successful.	Send notification to inform that authorization renewal of Cisco ISE with Cisco Smart Software Manager was successful.

Alarm Name	Alarm Description	Alarm Resolution
Smart Licensing Communication Failure	Communication of Cisco ISE with Cisco Smart Software Manager has failed.	Check your network connectivity with Cisco Smart Software Manager. Log in to Cisco Smart Software Manager or contact your Cisco partner if issue persists.
Smart Licensing Communication Restored	Communication of Cisco ISE with Cisco Smart Software Manager was restored.	Send notification to inform that your network connectivity with Cisco Smart Software Manager has been restored.
Smart Licensing De-Registration Failure	Deregistration of Cisco ISE with Cisco Smart Software Manager has failed.	See the **Cisco ISE License Administration** window for additional details. Log in to Cisco Smart Software Manager or contact your Cisco partner if issue persists.
Smart Licensing De-Registration Success	Deregistration of Cisco ISE with Cisco Smart Software Manager was successful.	Send notification to inform that deregistration of Cisco ISE with Cisco Smart Software Manager was successful.
Smart Licensing Disabled	Smart Licensing is disabled on Cisco ISE, and traditional licensing is in use.	See the **License Administration** window to enable Smart Licensing again. See the Cisco ISE Admin Guide or contact your Cisco partner to learn about using Smart Licensing on Cisco ISE.
Smart Licensing Evaluation Period Expired	Evaluation period of Smart Licensing has expired.	See the **Cisco ISE License Administration** window to register Cisco ISE with Cisco Smart Software Manager.
Smart Licensing HA Role changed	High-availability role change has occurred while using Smart Licensing.	Send notification to inform that the HA role of Cisco ISE has changed.
Smart Licensing Id Certificate Expired	Smart Licensing certificate has expired.	See the **Cisco ISE License Administration** window to manually renew registration for Smart Licensing. Contact your Cisco partner if the issue persists.
Smart Licensing Id Certificate Renewal Failure	Registration renewal for Smart Licensing with Cisco Smart Software Manager has failed.	See the **Cisco ISE License Administration** window to manually renew registration for Smart Licensing. Contact your Cisco partner if the issue persists.
Smart Licensing Id Certificate Renewal Success	Registration renewal for Smart Licensing with Cisco Smart Software Manager was successful.	Send notification to inform that registration renewal with Cisco Smart Software Manager was successful.
Smart Licensing Invalid Request	Invalid request was made to Cisco Smart Software Manager.	See the **Cisco ISE License Administration** window for additional details. Log in to Cisco Smart Software Manager or contact your Cisco partner if issue persists.
Smart Licensing Out of Compliance	Cisco ISE licenses are out of compliance.	See the **ISE License Administration** window for additional details. Contact your partner or Cisco account team to purchase new licenses.

Alarm Name	Alarm Description	Alarm Resolution
Smart Licensing Registration Failure	Registration of Cisco ISE with Cisco Smart Software Manager has failed.	See the **ISE License Administration** winsow for additional details. Log in to Cisco Smart Software Manager or contact your Cisco partner if issue persists.
Smart Licensing Registration Successful	Registration of Cisco ISE with Cisco Smart Software Manager was successful.	Send notification to inform that registration of Cisco ISE with Cisco Smart Software Manager was successful.
System Error		
Log Collection Error	The Cisco ISE monitoring collector process is unable to continue with the audit logs generated from the policy service nodes.	This will not impact the actual functionality of the Policy Service nodes. Contact Cisco TAC for further resolution.
Scheduled Report Export Failure	Unable to copy the exported report (CSV file) to the configured repository.	Verify the configured repository. If it has been deleted, add it back. If it is not available or is not reachable, reconfigure the repository to a valid one.
TrustSec		
Unknown SGT was provisioned	Unknown SGT was provisioned.	ISE provisioned an Unknown SGT as part of the authorization flow. Unknown SGT should not be assigned as part of a known flow.
Some TrustSec network devices do not have the latest ISE IP-SGT mapping configuration	Some TrustSec network devices do not have the latest ISE IP-SGT mapping configuration.	ISE identified some network devices that have a different IP-SGT mapping sets. Use the **IP-SGT Mapping Deploy** option to update the devices.
TrustSec SSH connection failed	TrustSec SSH connection failed.	ISE failed to establish SSH connection to a network device. Verify if the network device's SSH credentials in the **Network Device** window are similar to the credentials configured on the network device. Check the network device-enabled SSH connections from ISE (IP address).
TrustSec identified ISE was set to work with TLS versions other than 1.0	TrustSec-identified ISE was set to work with TLS versions other than 1.0.	TrustSec supports only TLS Version 1.0.
Trustsec PAC validation failed	Trustsec PAC validation failed.	ISE could not validate a PAC that was sent by the network device. Check the Trustsec device credentials in the **Network Device** window and in the device CLI. Make sure the device uses a valid PAC that was provisioned by the ISE server.

Alarm Name	Alarm Description	Alarm Resolution
Trustsec environment data download failed	Trustsec environment data download has failed.	Cisco ISE has received illegal Environment Data request. Verify the following: • PAC exists in the request, and is valid. • All the attributes exist in the request.
TrustSec CoA message ignored	TrustSec CoA message was ignored.	Cisco ISE sent a TrustSec CoA message and did not receive a response. Verify if the network device is CoA capable. Check the network device configuration.
TrustSec default egress policy was modified	TrustSec default egress policy was modified.	Make sure it is aligned with your security policy.

Note Alarms are not triggered when you add users or endpoints to Cisco ISE.

Alarm Settings

The following table describes the fields in the **Alarm Settings** window(In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Alarm Settings** > **Alarm Configuration** > **Add**)

Field Name	Description
Alarm Type	Alarm type.
Alarm Name	Name of the alarm.
Description	Description for the alarm.
Suggested Actions	Action to be performed when the alarm is triggered.
Status	Enable or disable the alarm rule.
Severity	Select the severity level for your alarm. Valid options are: • Critical: Indicates a critical error condition. • Warning: Indicates a normal but significant condition. This is the default condition. • Info: Indicates an informational message.
Send Syslog Message	Send a syslog message for each system alarm that Cisco ISE generates.

Field Name	Description
Enter multiple e-mails separated with comma	List of e-mail addresses or ISE administrator names or both.
Notes in Email (0 to 4000 characters)	Custom text messages that you want associated with your system alarm.

Configure Authorization Result Alarm

You can configure alarms based on the results of authorization policies. This allows you to monitor the impact of any networking, infrastructure, or application changes on endpoint authorizations. You can define the scope of your alarms by choosing specific Network Device Groups (NDG). For each NDG you choose, a new Authorization Result alarm is created.

You can filter the authorization logs that you want monitored for this alarm by choosing specific authorization profiles and Security Group Tags (SGT). Only endpoints that have met authorization policy sets with the specified authorization profiles and SGTs are monitored by the alarm.

You can define one of the following thresholds for this alarm:

- The total number of current active sessions.
- The percentage of active sessions with selected Authorization Profiles, SGTs, or both, compared to the total number of active sessions.
- The number of endpoint authorizations with selected Authorization Profiles, SGTs, or both, that have occurred in a defined time period.
- The percentage of endpoint authorizations with selected Authorization Profiles, SGTs, or both, compared to the total number of authorization logs that were generated in a defined time period.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Alarm Settings**.

Step 2 From the list of alarms, click the radio button next to **Authorization Result**, and click **Edit**.

Step 3 In the new window displayed, in the **Alarm Configuration** tab, configure the following fields in the **Thresholds** area:

a) **Threshold On**: Choose **Active Sessions** or **Authorizations in Configured Time Period** from the drop-down list.

   Active Sessions: Define an alarm based on the active sessions.

   Authorizations in Configured Time Period: Define an alarm based on the endpoint authorizations in a defined time period.

b) **Threshold Type**: Choose **Number** or **Percentage** from the drop-down list.

c) **Threshold Operator**: Choose **Greater Than** or **Less Than** from the drop-down list.

d) **Threshold Value**: Enter a threshold value in the text field. The valid range is from 0 to 999999 when the **Threshold Type** is **Number**, and from 0 to 100 when the **Threshold Type** is **Percentage**.

e) **Include Data of Last (Minutes):** This field is displayed only if you choose **Authorizations in Configured Time Period** from the **Threshold On** drop-down list. Choose the required value from the drop-down list.

f) **Run Every**: From the drop-down list, choose the polling interval, in minutes, for the alarms.

Step 4 Define filters for the authorization logs polled for this alarm, in the **Filters** area. Choose the required options from the **Authorization Profile** and **SGT** drop-down lists.

You must choose at least one option in the **Filters** area, an authorization profile or an SGT, to successfully configure this alarm. You can choose multiple options for each filter.

Step 5 Define the scope of the alarms in the **Scope** area. Choose specific NDGs from the corresponding drop-down list to poll only the endpoint authorization logs related to specific NDGs. For each NDG chosen, an individual alarm is created. You can view and acknowledge the logs of each NDG separately. If you do not choose any option from the drop-down list, all the NDGs in your Cisco ISE are included in the scope of this alarm.

Step 6 To receive syslog messages related to this alarm's activity, check the **Send Syslog Message** check box.

Enter the email addresses to which the syslogs must be sent, in the **Enter multiple e-mails separated with comma** field. To include a specific message in the syslog emails, enter the message in the **Notes in Email** field.

Step 7 Click **Submit** to save the configurations.

Step 8 In the **Alarm Notification** tab, enter the email addresses to which alarm notifications must be sent. Enter the email addresses of recipients in the **Enter multiple e-mails separated with comma** field. Enter the email address of the sender in the **Enter sender e-mail** field.

Step 9 Click **Save**.

Authorization Result alarms are displayed in the **Alarms** dashlet on your Cisco ISE **Dashboard**. The details of this alarm include the hit counts for each authorization policy that contains an Authorization Profile or SGT chosen as a filter. You can then check specific authorization policies to determine the network, infrastructure, or application changes that are impacting endpoint authorization.

Add Custom Alarms

Cisco ISE contains 12 default alarm types, such as High Memory Utilization and Configuration Changes. Cisco-defined system alarms are listed in the **Alarms Settings** window (In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Alarm Settings**). You can only edit the system alarms.

In addition to existing system alarms, you can add, edit, or delete custom alarms under the existing alarm types.

For each alarm type, you can create a maximum of five alarms. The total number of alarms is limited to 200.

In the **Alarm Configuration** tab of the **Alarm Settings** window, the **Conditions** column displays details for four alarms: High Authentication Latency, High Disk I/O Utilization, High Disk Space Utilization, and High Memory Utilization. Each of these alarms has a configurable threshold value. However, the **Conditions** column may not display details even after the threshold values are configured. In such a scenario, re-edit the relevant threshold field for the alarm to view the details in the **Conditions** column.

Perform this procedure to add an alarm.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Alarm Settings**

Step 2 In the **Alarm Configuration** tab, click **Add**.

Step 3 Enter the required details. See the Alarm Settings section for more information.

Based on the alarm type (High Memory Utilization, Excessive RADIUS Authentication Attempts, Excessive TACACS Authentication Attempts, and so on), additional attributes are displayed in the **Alarm Configuration** window. For example, **Object Name**, **Object Type**, and **Admin Name** fields are displayed for Configuration Change alarms. You can add multiple instances of the same alarm with different criteria.

Step 4 Click **Submit**.

Cisco ISE Alarm Notifications and Thresholds

You can enable or disable Cisco ISE alarms and configure alarm notification behavior to notify you of critical conditions. For certain alarms, you can configure thresholds such as maximum failed attempts for the Excessive Failed Attempts alarm or maximum disk utilization for the High Disk Utilization alarm.

You can configure the notification settings on a per-alarm basis, and enter the email IDs of the users who have to be notified for each alarm (both system-defined and user-defined alarms).

Note The recipient email address specified at the alarm rule level overrides the global recipient email address setting.

Enable and Configure Alarms

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Alarm Settings**.

Step 2 Select an alarm from the list of default alarms y clicking on the radio button and click **Edit**.

Step 3 Select **Enable** or **Disable**. from the **Status** drop-down list.

Step 4 Configure alarm threshold, if applicable.

Step 5 Click **Submit**.

Cisco ISE Alarms for Monitoring

Cisco ISE provides system alarms that notify you whenever any critical system condition occurs. Alarms that are generated by Cisco ISE are displayed in the Alarm dashlet. These notifications automatically appear in the Alarm dashlet.

The Alarm dashlet displays a list of recent alarms. From this list, you can choose which alarm's details you want to view. You can also receive notifications of alarms through e-mail and syslog messages.

View Monitoring Alarms

Step 1 Go to the Cisco ISE **Dashboard**.

Step 2 Click on an alarm in the **Alarms** dashlet. A dialog box opens with the alarm details and a suggested action.

Step 3 Click **Refresh** to refresh the alarms.

Step 4 Acknowledge alarms to reduce the alarm counters (number of times an alarm is raised) by marking them as read. Select alarms for acknowledgement by checking the check boxes next to the timestamps.

Choose **Acknowledge Selected** from the **Acknowledge** drop-down list to mark as read all the alarms currently displayed in the window. By default, 100 rows are displayed in the window. You can choose a different number of rows to be displayed, by choosing a value from the **Rows/Page** drop-down list.

Choose **Acknowledge All** from the **Acknowledge** drop-down list to mark as read all the alarms in the list, whether or not they are currently displayed in the window.

Note When you check the check box next to the **Time Stamp** in the title row, all the alarms displayed in the window are selected. However, if you then uncheck a check box for one or more of the selected alarms, the select all function lapses. You will see that the check box next to the **Time Stamp** is unchecked at this point.

Step 5 Click the **Details** link corresponding to the alarm that you select. A dialog box opens with the details corresponding to the selected alarm.

Note The **Details** link corresponding to the alarms that were generated prior to persona change shows no data.

Log Collection

Monitoring services collect log and configuration data, store the data, and then process it to generate reports and alarms. You can view the details of the logs that are collected from any of the servers in your deployment.

Alarm Syslog Collection Location

If you configure monitoring functions to send alarm notifications as syslog messages, you need a syslog target to receive the notification. Alarm syslog targets are the destinations where alarm syslog messages are sent.

Note Cisco ISE monitoring requires that the logging-source interface configuration use the network access server (NAS) IP address. You must configure a switch for Cisco ISE monitoring.

You must also have a system that is configured as a syslog server to be able to receive syslog messages. You can create, edit, and delete alarm syslog targets.

To configure a remote logging target as an alarm target, perform this procedure.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Remote Logging Targets**.

Step 2 Click **Add**.

Step 3 In the **New Logging Target** window, submit the required details for the logging target, and check the **Include Alarms for this Target** check box.

RADIUS Live Logs

The following table describes the fields in the Live logs window that displays the recent RADIUS authentications. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **RADIUS** > **Live Logs**. Note that you can view the RADIUS live logs only in the Primary PAN.

Table 203: RADIUS Live Logs

Field Name	Description
Time	Shows the time at which the log was received by the monitoring and troubleshooting collection agent. This column is required and cannot be deselected.
Status	Shows if the authentication succeeded or failed. This column is mandatory and cannot be deselected. Green is used to represent passed authentications. Red is used to represent failed authentications.
Details	Clicking the icon under the **Details** column opens the **Accounting Detail** report if an accounting event is processed for that session. If the session is in authenticated state, **Authentication Detail** report is displayed when you click the icon under the **Details** column. The **Response Time** in the **Authentication Detail** report is the total time taken by Cisco ISE to process the authentication flow. For example, if authentication consists of three roundtrip messages that took 300 ms for the initial message, 150 ms for the next message, and 100 ms for the last, **Response Time** is 300 + 150 + 100 = 550 ms. **Note** You cannot view the details for endpoints that are active for more than 7 days. You will see a window with the following message when you click the **Details** icon for endpoints that are active for more than 7 days: `No Data available for this record. Either the data is purged or authentication for this session record happened a week ago. Or if this is an 'PassiveID' or 'PassiveID Visibility' session, it will not have authentication details on ISE but only the session.`
Repeat Count	Shows the number of time the authentication requests were repeated in the last 24 hours, without any change in the context of identity, network devices, and authorization.
Identity	Shows the logged in username that is associated with the authentication. If the username is not present in any ID Store, it is displayed as `INVALID`. If the authentication fails due to any other reason, it is displayed as `USERNAME`. **Note** This is applicable only for users. This is not applicable for MAC addresses. To aid debugging, you can force Cisco ISE to display the invalid usernames. To do this, check the **Disclose Invalid Usernames** check box under **Administration** > **System** > **Settings** > **Security Settings**. You can also configure the **Disclose Invalid Usernames** option to time out, so that you do not have to manually turn it off.
Endpoint ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.

Field Name	Description
Endpoint Profile	Shows the type of endpoint that is profiled, for example, profiled to be an iPhone, Android, MacBook, Xbox, and so on.
Authentication Policy	Shows the name of the policy selected for specific authentication.
Authorization Policy	Shows the name of the policy selected for specific authorization.
Authorization Profiles	Shows the authorization profile that was used for authentication.
IP Address	Shows the IP address of the endpoint device.
Network Device	Shows the IP address of the Network Access Device.
Device Port	Shows the port number at which the endpoint is connected.
Identity Group	Shows the identity group that is assigned to the user or endpoint, for which the log was generated.
Posture Status	Shows the status of posture validation and details on the authentication.
Server	Indicates the policy service from which the log was generated.
MDM Server Name	Shows the name of the MDM server.
Event	Shows the event status.
Failure Reason	Shows the detailed reason for failure, if the authentication failed.
Auth Method	Shows the authentication method that is used by the RADIUS protocol, such as Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2), IEE 802.1x or dot1x, and so on.
Authentication Protocol	Shows the authentication protocol used, such as Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol (EAP), and so on.
Security Group	Shows the group that is identified by the authentication log.
Session ID	Shows the session ID.

Note In the **RADIUS Live Logs** and **TACACS+ Live Logs** window, a Queried PIP entry appears for the first attribute of each policy authorization rule. If all the attributes within the authorization rule are related to a dictionary that was already queried for previous rules, no additional Queried PIP entry appears.

You can do the following in the RADIUS **Live Logs** window:

- Export the data in CSV or PDF format.

- Show or hide the columns based on your requirements.
- Filter the data using the quick or custom filter. You can also save your filters for later use.
- Rearrange the columns and adjust the width of the columns.
- Sort the column values.

Note All the user customizations are stored as user preferences.

TACACS Live Logs

The following table describes the fields in the TACACS Live Logs window that displays the TACACS+ AAA details. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **TACACS** > **Live Logs**. You can view the TACACS live logs only in the Primary PAN.

Table 204: TACACS Live Logs

Field Name	Usage Guidelines
Generated Time	Shows the syslog generation time based on when a particular event was triggered.
Logged Time	Shows the time when the syslog was processed and stored by the Monitoring node. This column is mandatory and cannot be deselected.
Status	Shows if the authentication succeeded or failed. This column is required and cannot be deselected. Green is used to represent passed authentications. Red is used to represent failed authentications.
Details	Brings up a report when you click the magnifying glass icon, allowing you to drill down and view more detailed information about the selected authentication scenario. This column is required and cannot be deselected.
Session Key	Shows the session keys (found in the EAP success or EAP failure messages) returned by ISE to the network device.
Username	Shows the user name of the device administrator. This column is required and cannot be deselected.
Type	Consists of two Types—Authentication and Authorization. Shows names of users who have passed or failed authentication, authorization, or both. This column is mandatory and cannot be deselected.
Authentication Policy	Shows the name of the policy selected for specific authentication.
Authorization Policy	Shows the name of the policy selected for specific authorization.
ISE Node	Shows the name of the ISE node through which the access request is processed.

Field Name	Usage Guidelines
Network Device Name	Shows the names of network devices.
Network Device IP	Shows the IP addresses of network devices whose access requests are processed.
Network Device Groups	Shows the name of corresponding network device groups to which a network device belongs.
Device Type	Shows the device type policy that is used to process access requests from different network devices.
Location	Shows the location-based policy that is used to process access requests from network devices.
Device Port	Shows the device port number through which the access request is made.
Failure Reason	Shows the reason for rejecting an access request that is made by a network device.
Remote Address	Shows the IP address, MAC address, or any other string that uniquely identifies the end station.
Matched Command Set	Shows the MatchedCommandSet attribute value if it is present, or an empty value if the MatchedCommandSet attribute value is empty or the attribute itself does not exist in the syslog.
Shell Profile	Shows the privileges that were granted to a device administrator for executing commands on the network device.

You can do the following in the **TACACS Live Logs** window:

- Export the data in CSV or PDF format.
- Show or hide the columns based on your requirements.
- Filter the data using the quick or custom filter. You can also save your filters for later use.
- Rearrange the columns and adjust the width of the columns.
- Sort the column values.

Note All the user customizations are stored as user preferences.

Live Authentications

You can monitor recent RADIUS authentications as they occur, from the **Live Authentications** window. The window displays the top ten RADIUS authentications in the last 24 hours. This section explains the functions of the **Live Authentications** window.

The **Live Authentications** window shows the live authentication entries corresponding to the authentication events as they happen. In addition to authentication entries, this window also shows the live session entries corresponding to the events. You can also drill-down a session to view a detailed report corresponding to that session.

The **Live Authentications** window provides a tabular account of recent RADIUS authentications, in the order in which they occur. The last update shown at the bottom of the **Live Authentications** window shows the date of the server, time, and timezone.

Note If the password attribute in an Access-Request packet is empty, an error message is triggered and the access request fails.

When a single endpoint is authenticated successfully, two entries appear in the **Live Authentications** window—one corresponding to the authentication record and another corresponding to the session record (pulled from the session live view). Subsequently, when the device performs another successful authentication, the repeat counter corresponding to the session record is incremented. The Repeat Counter that appears in the **Live Authentications** window shows the number of duplicate RADIUS authentication success messages that are suppressed.

See the Live Authentication data categories that are shown by default. These are described in the Recent RADIUS Authentications section.

You can choose to view all the columns, or only selected data columns. After selecting the columns that you want to be displayed, you can save your selections.

Monitor Live Authentications

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **RADIUS** > **Live logs**

Step 2 From the **Refresh** drop-down list, choose a time interval to change the data refresh rate.

Step 3 Click the **Refresh** icon to manually update the data.

Step 4 From the **Show** drop-down list, choose an option to change the number of records that appear.

Step 5 From the **Within** drop-down list, choose an option to specify a time interval.

Step 6 Click **Add or Remove Columns** and choose the options from the drop-down list to change the columns that are displayed.

Step 7 Click **Save** at the bottom of the window to save your modifications.

Step 8 Click **Show Live Sessions** to view the live RADIUS sessions.

You can use the dynamic Change of Authorization (CoA) feature for the live sessions that allows you to dynamically control active RADIUS sessions. You can send reauthenticate or disconnect requests to a Network Access Device (NAD).

Filter Data in the Live Authentications Page

Using the filters in the **Live Authentications** window, you can filter the information that you need, and troubleshoot network authentication issues quickly. You can filter records in the Authentication **Live Logs** window and view only those records that you are interested in. The authentication logs contain many details, and filtering the authentications by a particular user or location helps you scan the data quickly. You can use several operators that are available in the **Live Authentications** window to filter out records based on your search criteria.:

- 'abc' : Contains 'abc'
- '!abc' : Does not contain 'abc'
- '{}' : Is empty
- '!{}' : Is not empty
- 'abc*' : Starts with 'abc'
- '*abc' : Ends with 'abc'
- '\!', '*', '\{', '\\' : Escape

The Escape option allows you to filter text with special characters (including the special characters used as filters). You must prefix the special character with a backward slash (\). For example, if you want to view the authentication records of users with identity "Employee!," enter "Employee\!" in the **Identity Filter** field. In this example, Cisco ISE considers the exclamation mark (!) as a literal character and not as a special character.

In addition, the **Status** field allows you to filter only passed authentication records, failed authentications, live sessions, and so on. The green check mark filters all the passed authentications that occurred in the past. The red cross mark filters all failed authentications. The blue i icon filters all the live sessions. You can also choose to view a combination of these options.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **RADIUS** > **Live Logs**

Step 2 Filter data based on any of the fields in the **Show Live Authentications** window.

You can filter the results based on passed or failed authentications, or live sessions.

RADIUS Live Sessions

The following table describes the fields in the RADIUS **Live Sessions** window, which displays live authentications. To view this window, click the **Menu** icon (☰) and chooseYou can view the RADIUS live sessions only in the Primary PAN.

Table 205: RADIUS Live Sessions

Field Name	Description
Initiated	Shows the timestamp when the session was initiated.
Updated	Shows the timestamp when the session was last updated because of a change.
Account Session Time	Shows the time span (in seconds) of a user's session.
Session Status	Shows the current status of an endpoint device.

Field Name	Description
Action	Click the **Actions** icon to reauthenticate an active RADIUS session or disconnect an active RADIUS session.
Repeat Count	Shows the number of times a user or endpoint is reauthenticated.
Endpoint ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.
Identity	Shows the username of an endpoint device.
IP Address	Shows the IP address of an endpoint device.
Audit Session ID	Shows a unique session identifier.
Account Session ID	Shows a unique ID provided by a network device.
Endpoint Profile	Shows the endpoint profile for a device.
Posture Status	Shows the status of posture validation and details of the authentication.
Security Group	Shows the group that is identified by the authentication log.
Server	Indicates the Policy Service node from which the log was generated.
Auth Method	Shows the authentication method that is used by the RADIUS protocol, such as Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), IEE 802.1x or dot1x, and so on.
Authentication Protocol	Shows the authentication protocol used, such as Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol (EAP), and so on.
Authentication Policy	Shows the name of the policy selected for specific authentication.
Authorization Policy	Shows the name of the policy selected for specific authorization.
Authorization Profiles	Shows an authorization profile that was used for authentication.
NAS IP Address	Shows the IP address of a network device.
Device Port	Shows the connected port to a network device.
PRA Action	Shows the periodic reassessment action taken on a client after it is successfully postured for compliance on your network.
ANC Status	Adaptive Network Control status of a device as **Quarantine, Unquarantine**, or **Shutdown**.

Field Name	Description
WLC Roam	Shows the boolean (Y/N) used to track if an endpoint has been handed off during roaming, from one Wireless Lan Controller (WLC) to another. It has the value of cisco-av-pair=nas-update =Y or N. **Note** Cisco ISE relies on the nas-update=true attribute from WLC to identify whether the session is in roaming state. When the original WLC sends an accounting stop attribute with nas-update=true, the session is not deleted in ISE to avoid reauthentication. If roaming fails, ISE clears the session after five days of inactivity.
Packets In	Shows the number of packets received.
Packets Out	Shows the number of packets sent.
Bytes In	Shows the number of bytes received.
Bytes Out	Shows the number of bytes sent.
Session Source	Indicates whether it is a RADIUS session or a Passive ID session.
User Domain Name	Shows the registered DNS name of a user.
Host Domain Name	Shows the registered DNS name of a host.
User NetBIOS Name	Shows the NetBIOS name of a user.
Host NetBIOS Name	Shows the NetBIOS name of a host.
License Type	Shows the type of license used.
License Details	Shows the license details.

Field Name	Description
Provider	Endpoint events are learned from different syslog sources. These syslog sources are referred to as providers. • Windows Management Instrumentation (WMI): WMI is a Windows service that provides a common interface and object model to access management information about operating system, devices, applications, and services. • Agent: A program that runs on a client on behalf of the client or another program. • Syslog: A logging server to which a client sends event messages. • REST: A client is authenticated through a terminal server. The TS Agent ID, Source Port Start, Source Port End, and Source First Port values are displayed for this syslog source. • Span: Network information is discovered using span probes. • DHCP: DHCP event. • Endpoint **Note** When two events from different providers are learned or obtained from an endpoint session, the providers are displayed as comma-separated values in the **Live Sessions** window.
MAC Address	Shows the MAC address of a client.
Endpoint Check Time	Shows the time at which an endpoint was last checked by the endpoint probe.
Endpoint Check Result	Shows the result of an endpoint probe. The possible values are: • Unreachable • User Logout • Active User
Source Port Start	(Values are displayed only for the REST provider) Shows the first port number in a port range.
Source Port End	(Values are displayed only for the REST provider) Shows the last port number in a port range.
Source First Port	(Values are displayed only for the REST provider) Shows the first port allocated by the Terminal Server Agent. A Terminal Server refers to a server or network device that allows multiple endpoints to connect to it without a modem or network interface and facilities the connection of the multiple endpoints to a LAN network. The multiple endpoints appear to have the same IP address, and therefore, it is difficult to identify the IP address of a specific user. Consequently, to identify a specific user, a Terminal Server Agent is installed in the server, which allocates a port range to each user. This helps create an IP address-port user mapping.

Field Name	Description
TS Agent ID	(Values are displayed only for the REST provider) Shows the unique identity of the Terminal Server Agent that is installed on an endpoint.
AD User Resolved Identities	(Values are displayed only for AD user) Shows the potential accounts that matched.
AD User Resolved DNs	(Values are displayed only for AD user) Shows the Distinguished Name of AD user, for example, CN=chris,CN=Users,DC=R1,DC=com

Export Summary

You can view the details of the reports exported by all the users in the last seven days, along with the status. The export summary includes both the manual and scheduled reports. The **Export Summary** window is automatically refreshed every two minutes. Click the **Refresh** icon to refresh the **Export Summary** window manually.

The super admin can cancel the export that is **In-Progess** or in **Queued** state. Other users are allowed only to cancel the export process that they have initiated.

By default, only three manual export of reports can run at a given point of time; the remaining triggered manual export of reports are queued. There are no such limits for the scheduled export of reports.

Note All the reports in the queued state are scheduled again and the reports in the **In-Progress** or **Cancellation-in-progress** state are marked as failed when the Cisco ISE server is restarted. If the primary MnT node is down, the scheduled report export job runs on secondary MnT node.

The following table describes the fields in the **Export Summary** window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Export Summary**.

Table 206: Export Summary

Field Name	Description
Report Exported	Displays the name of the report.
Exported By	Shows the role of the user who initiated the export process.
Scheduled	Shows whether the report export is a scheduled one.
Triggered On	Shows the time at which the export process has been triggered in the system.
Repository	Displays the name of the repository where the exported data will be stored.
Filter Parameters	Shows the filter parameters selected while exporting the report.

Field Name	Description
Status	Shows the status of the exported reports. It can be one of the following: • Queued • In-progress • Completed • Cancellation-in-progress • Cancelled • Failed • Skipped **Note** Failed status indicates the reason for failure. Skipped status indicates that the scheduled export of reports is skipped because the primary MnT node is down.

You can do the following in the **Export Summary** window:

- Show or hide the columns based on your requirements.
- Filter the data using quick or custom filter. You can also save your filters for later use.
- Rearrange the columns and adjust the width of the columns.

Authentication Summary Report

You can troubleshoot network access for a specific user, device, or search criteria based on the attributes that are related to the authentication requests. You can do this by running an Authentication Summary report.

Note You can generate the Authentication Summary report only for the last 30 days.

Troubleshoot Network Access Issues

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Reports** > **Device Administration** > **Authentication Summary Report**.

Step 2 Filter the report for the **Failure Reasons**.

Step 3 Review the data in the **Authentication by Failure Reasons** section of the report to troubleshoot your network access problem.

Note Because the Authentication Summary report collects and displays the latest data corresponding to failed or passed authentications, the contents of the report appear after a delay of a few minutes.

Cisco Support Diagnostics for Deployment and Support Information

Overview

The Cisco Support Diagnostics Connector is a new feature that helps Cisco Technical Assistance Center (TAC) and Cisco support engineers obtain deployment information from the Primary Administration Node. TAC can get support information of any particular node in your deployment through the connector. This data enables quicker and better-informed troubleshooting.

You can enable the Cisco Support Diagnostics Connector through the Cisco ISE administration portal. The feature allows a two-way connection between the Primary Policy Administration Node in your deployment and Cisco Support Diagnostics, leveraging the Security Services Exchange (SSE) cloud portal.

Pre-requisites

- You must have Super Admin or System Admin role to enable or disable Cisco Support Diagnostics.

Configure Cisco Support Diagnostics Connector

To enable the Cisco Support Diagnostics feature:

- In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Network Success Diagnostics** > **Cisco Support Diagnostics** > **Cisco Support Diagnostics Setting**.
- This feature is disabled by default. If it is not, check the **Enable Cisco Support Diagnostics** check box to activate Cisco Support Diagnostics.

Verify Cisco Support Diagnostics BiDirectional Connection

To verify that Cisco ISE is successfully registered or enrolled with Cisco Support Diagnostics, and that a bi-directional connection has been established through the Security Services Exchange portal, perform this procedure:

- In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Reports** > **Audit** > **Change Configuration Audit**.
- Ensure the following:
    1. Cisco Support Diagnostics is enabled.
    2. The ISE server is registered to Cisco Support Diagnostics.
    3. The ISE SSE services are enrolled to Cisco Support Diagnostics.
    4. The Cisco Support Diagnostics bidirectional connectivity is enabled.
- You can also go to the Operations Audit window **(**In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Reports** > **Audit** > **Operations Audit**) for details of the services enabled, disabled, registered, unregistered, enrolled, or unenrolled as part of Cisco Support Diagnostics.

Troubleshooting Information

If the Cisco Support Diagnostics bidirectional connection appears as to be broken, check for the following:

- **Smart Licensing**: Disabling Smart Licensing disables Cisco Support Diagnostics automatically. Re-enable smart licensing to enable the connector.
- **Connectivity to Security Services Exchange cloud**: When Cisco Support Diagnostics is enabled, Cisco ISE continuously checks the persistent connectivity established with the Security Services Exchange portal. If this connection is found to be broken, the following critical alarm is triggered: Alarms: The Cisco Support Diagnostics bi-directional connectivity is broken. Re-enable the feature using the configuration steps provided earlier.

Related Information

An administrator can use ERS APIs to perform these specific tasks:

- Trigger support information on a specific node.
- Get the status of the triggered support bundle.
- Download the support bundle.
- Pull the deployment information.

See the ERS SDK page for usage and other information.

Obtain Configuration Backup Using Cisco Support Diagnostics Connector

This feature helps Cisco Technical Assistance Center (TAC) and Cisco support engineers to trigger configuration backup and upload the backup files to the Cisco Support Diagnostics folder. After uploading the backup files to the Cisco Support Diagnostics folder, the backup files can be deleted from the Cisco ISE local disk.

To use this feature, smart licensing and Cisco Support Diagnostics must be enabled in Cisco ISE. To enable Cisco Support Diagnostics:

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Network Success Diagnostics** > **Cisco Support Diagnostics** > **Cisco Support Diagnostics Setting**.
2. Check the **Enable Cisco Support Diagnostics** check box to activate Cisco Support Diagnostics.

The following method is used to trigger configuration backup and upload the backup files to the Cisco Support Diagnostics folder:

1. The REST API is used to get the organization ID for *ISE Integration* Company Name.
2. The Organization ID in the REST API is used to get the list of devices.
3. The REST API is used to get the Service ID.
4. The Service ID and the Organization ID are used to generate the JSON Web Token (JWT).
5. The REST API is used to check the services available for the device by using the Device ID as a path parameter.
6. The REST API is used to upload the backup files from Cisco ISE to the Cisco Support Diagnostics folder. The upload status of the backup files can be verified. If the files are not uploaded to the Cisco Support Diagnostics folder, a 404 error is displayed.

Diagnostic Troubleshooting Tools

Diagnostic tools help you diagnose and troubleshoot problems on a Cisco ISE network and provide detailed instructions on how to resolve problems. You can use these tools to troubleshoot authentications and evaluate the configuration of any network device on your network, including TrustSec devices.

The RADIUS Authentication Troubleshooting Tool

This tool allows you to search for and select a RADIUS authentication or an Active Directory-related RADIUS authentication for troubleshooting when there is an unexpected authentication result. Use this tool if you expected an authentication to pass, but it failed, or if you expected a user or machine to have a certain level of privileges, and the user or machine did not have those privileges.

- Searching RADIUS authentications based on Username, Endpoint ID, Network Access Service (NAS) IP address, and reasons for authentication failure for troubleshooting, Cisco ISE displays authentications only for the system (current) date.
- Searching RADIUS authentications based on NAS port for troubleshooting, Cisco ISE displays all the NAS port values since the beginning of the previous month to the current date.

Note When searching for RADIUS authentications based on NAS IP Address and Endpoint ID Fields, a search is first performed in the operational database, and then in the configuration database.

Troubleshoot Unexpected RADIUS Authentication Results

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **RADIUS Authentication Troubleshooting**.

Step 2 Specify the search criteria in the fields, as needed.

Step 3 Click **Search** to display the RADIUS authentications that match your search criteria.

If you are searching for Active Directory-related authentication, and an Active Directory server is not configured in your deployment, a message stating *AD not configured* is displayed.

Step 4 Select a RADIUS authentication record from the table, and click **Troubleshoot**.

To troubleshoot Active Directory-related authentication, access the Diagnostics Tool under **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory** > **AD node**.

Step 5 Click **User Input Required**, modify the fields, as needed, and then click **Submit**.

Step 6 Click **Done**.

Step 7 Click **Show Results Summary** after the troubleshooting is complete.

Step 8 (Optional) To view the diagnosis, the steps taken to resolve the problem, and the troubleshooting summary, click **Done**.

The Execute Network Device Command Diagnostic Tool

The Execute Network Device Command diagnostic tool allows you to run the **show** command on any network device.

The results that are displayed are the same as what you would see on a console. The tool enables you to identify problems, if any, in a device configuration.

Use this tool to validate the configuration of any network device, or if you are want to know how a network device is configured.

To access the Execute Network Device Command diagnostic tool, choose one of the following navigation paths:

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **Execute Network Device Command**.In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Profiler** > **Troubleshoot** > **Execute Network Device Command**.
2. In the **Execute Network Device Command** window that is displayed, enter the IP address of the network device and the **show** command that you want to run in the corresponding fields.
3. Click **Run**.

Execute Cisco IOS show Commands to Check Configuration

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **Execute Network Device Command**.

Step 2 Enter the information in the appropriate fields.

Step 3 Click **Run** to execute the command on the specified network device.

Step 4 Click **User Input Required**, and modify the fields, as necessary.

Step 5 Click **Submit** to run the command on the network device, and view the output.

The Evaluate Configuration Validator Tool

You can use this diagnostic tool to evaluate the configuration of a network device and identify configuration problems, if any. The **Expert Troubleshooter** compares the configuration of the device with the standard configuration.

Agentless Posture Troubleshooting

The Agentless Posture report is the main troubleshooting tool to use when agentless posture isn't working as expected. This report shows the stages of agentless flow, including events such as script upload completed, script upload failed, script execution completed, and so on, along with any known failure reasons, if any.

Note The agentless posture script cannot verify itself, but the script verifies the data received from Cisco ISE after it is executed.

You can access Agentless Posture Troubleshooting from two locations:

- In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations > Live Logs**, and click the vertical three dots in the **Posture Status** column adjacent to the client you want to troubleshoot.
- In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations > Troubleshoot > Diagnostics > General Tools > Agentless Posture Troubleshooting**.

The Agentless Posture Troubleshooting tool collects Agentless Posture activity for a specified client. **Agentless Posture Flow** initiates posture and displays all the interactions between a currently active client and Cisco ISE. **Only Download Client Logs** creates logs with up to 24 hours of posture flows from the client. The client can delete the logs at any time. After collection is completed, you can export a ZIP file of the logs.

Reports

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations > Reports > Reports > Endpoints and Users > Agentless Posture** to view all the endpoints that ran Agentless posture.

Troubleshoot Network Device Configuration Issues

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **Evaluate Configuration Validator**.

Step 2 Enter the IP address of the network device that you want to evaluate in the **Network Device IP** field.

Step 3 Check the check boxes and click the radio buttons next to the configuration options you want to compare against the recommended template.

Step 4 Click **Run**.

Step 5 In the **Progress Details...** area, click **Click Here to Enter Credentials**.

Step 6 In the **Credentials Window** dialog box, enter the connection parameters and credentials that are required to establish a connection with the network devices.

Step 7 Click **Submit**.

Step 8 (Optional) To cancel the workflow, click **Click Here to Cancel the Running Workflow** in the **Progress Details...** window.

Step 9 (Optional) Check the check boxes next to the interfaces that you want to analyze, and click **Submit**.

Step 10 (Optional) Click **Show Results Summary** for details of the configuration evaluation.

Troubleshoot Endpoint Posture Failure

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **Posture Troubleshooting**.

Step 2 Enter the information in the appropriate fields.

Step 3 Click **Search**.

Step 4 To find an explanation and determine a resolution for an event, select the event in the list and click **Troubleshoot**.

Session Trace Test Cases

This tool allows you to test policy flows in a predicable way to check and verify the way that the policy is configured, without needing to have real traffic originate from a real device.

You can configure the list of attributes and their values to be used in a test case. These details are used to perform interactions with the Policy system to simulate the run-time invocation of the policy.

The attributes can be configured by using dictionaries. All the dictionaries that are applicable to Simple RADIUS authentication are listed in the **Attributes** field.

Note You can configure test cases only for Simple RADIUS authentication.

Configure a Session Trace Test Case

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **Session Trace Test Cases**.

Step 2 Click **Add**.

Step 3 In the **Test Details** tab, enter a name and description for the test case.

Step 4 Select one of the predefined test cases or configure the required attributes and their values. The following predefined Test Cases are available:

- Basic Authenticated Access
- Profiled Cisco Phones
- Compliant Devices Access
- Wi-Fi Guest (Redirect)
- Wi-Fi Guest (Access)

After you select a predefined test case, Cisco ISE automatically populates the relevant attributes for the test case. You can use the default values of these attributes or select a value from the displayed options. You can also add additional custom attributes to the test case.

The attributes and the values that you add to the test case are listed in the **Text** field (below the **Custom Attributes** field). When you edit the content in the **Text** field, Cisco ISE checks the validity and syntax of the updated content.

You can view the summary of all the attributes at the bottom of the **Test Details** window.

Step 5 Click **Submit** .

Cisco ISE validates the attributes and their values and indicates errors, if any, before saving the test details.

Step 6 In the **Test Visualizer** tab, select the node on which you want to run this Test Case.

Note Only the nodes with Policy Service persona are displayed in the **ISE Node** drop-down list.

Click **User Groups/Attributes** to retrieve the groups and attributes for a user from an external identity store.

Step 7 Click **Execute**.

Cisco ISE executes the Test Case and displays the step-by-step results of the test case in a tabular format. It displays the policy stages, matching rules, and result objects. Click the green icon to view the details for each step.

Step 8 (Optional) Click the **Previous Test Executions** tab to view the results of previous test executions. You can also select and compare any two test cases. Cisco ISE displays the comparative view of the attributes for each test case in a tabular format.

Step 9 You can launch the Session Trace Test Case tool from the **RADIUS Live Logs** window. You can select an entry on the **Live Logs** window and click the **Actions** icon (in the **Details** column) to launch the **Session Trace Test Case** tool. Cisco ISE extracts the relevant attributes and their values from the corresponding log entry. You can modify these attributes and values, if required, and execute the test case.

TCP Dump Utility to Validate Incoming Traffic

The TCP Dump Utility sniffs packets that you can use to verify if the expected packet has reached a node. For example, when there is no incoming authentication or log indicated in the report, you may suspect that there is no incoming traffic, or that the incoming traffic cannot reach Cisco ISE. In such cases, you can run this tool to validate.

You can configure the TCP dump options and then collect data from the network traffic to help you troubleshoot a network issue.

Use TCP Dump to Monitor Network Traffic

The TCP Dump window lists TCP dump process files that you create. You can create different files for different purposes, run them as needed, and delete them when you don't need them.

You can control the data that is collected by specifying size, number of files, and how long the process runs. If the process finishes before the time limit, and the file is less than the maximum size, and you enabled more than one file, then the process continues and creates another dump file.

You can run TCP dump on more interfaces, including bonded interfaces.

Note Human-readable format is no longer an option; the dump file is always in raw format.

We support IPv6 connections to the repository.

Before you begin

The **Network Interface** drop-down list in the **TCP Dump** window displays only the network interface cards (NICs) that have an IPv4 or IPv6 address configured. By default in VMware, all the NICs are connected, which means that all the NICs have an IPv6 address and are displayed in the **Network Interface** drop-down list.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **TCP Dump**.

Step 2 From the **Host Name** drop-down list, choose the source for the TCP Dump utility.

Step 3 From the **Network Interface** drop-down list, choose an interface to monitor.

Step 4 In the **Filter** field, enter a boolean expression on which to filter.

The following are supported standard TCP dump filter expressions:

- ip host 10.77.122.123
- ip host ISE123
- ip host 10.77.122.123 and not 10.77.122.119

Step 5 Enter a **File Name** for this TCP dump process.

Step 6 From the **Repository** drop-down list, choose a repository to store TCP dump log files in.

Step 7 From the **File Size** drop-down list—Select a maximum file size.

If the dump exceeds this file size, a new file opens to continue the dump. The number of times the dump can continue to a new file is limited by the **Limit to** setting.

Step 8 The **Limit to** option can be used to limit the number of files that the dump can expand into.

Step 9 The **Time Limit** option can be used to configure how long a dump runs before ending.

Step 10 Set **Promiscuous Mode** by clicking **On** or **Off**. The default is **On**.

Promiscuous mode is the default packet sniffing mode in which the network interface passes all traffic to the system's CPU. We recommend that you leave it set to On.

Save a TCP Dump File

Before you begin

You should have successfully completed the task, as described in Using TCP Dump to Monitor network Traffic section.

Note You can also access TCP Dump through the Cisco ISE CLI. For more information, see the *Cisco Identity Services Engine CLI Reference Guide*.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **TCP Dump**.

Step 2 Click **Download**, corresponding to the desired location, and then click **Save**.

Step 3 (Optional) To get rid of the previous dump file without saving it, click **Delete**.

Compare Unexpected SGACL for an Endpoint or User

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **TrusSsec Tools** > **Egress (SGACL) Policy**.

Step 2 Enter the network device IP address of the TrustSec device whose SGACL policy you want to compare.

Step 3 Click **Run**.

Step 4 Click **User Input Required** and modify the fields, as necessary.

Step 5 Click **Submit**.

Step 6 Click **Show Results Summary** to view the diagnosis and suggested resolution steps.

Egress Policy Diagnostic Flow

The Egress Policy diagnostic tool uses the process described in the following table:

Process Stage	Description
1	Connects a the device with the IP address that you provided, and obtains the access control lists (ACLs) for each source and destination SGT pair.
2	Checks the egress policy that is configured in Cisco ISE and obtains the ACLs for each source and destination SGT pair.
3	Compares the SGACL policy that is obtained from the network device with the SGACL policy that is obtained from Cisco ISE.
4	Displays the source and destination SGT pair if there is a mismatch. Also, displays the matching entries as additional information.

Troubleshoot Connectivity Issues in a Trustsec-Enabled Network with SXP-IP Mappings

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **Trustsec Tools** > **SXP-IP Mappings** .

Step 2 Enter the IP address of the network device.

Step 3 Click **Select**.

Step 4 Click **Run**.

The Expert Troubleshooter retrieves TrustSec SXP connections from the network device and again prompts you to select the peer SXP devices.

Step 5 Click **User Input Required**, and enter the necessary information, in that field.

Step 6 Check the check box of the peer SXP devices for which you want to compare SXP mappings, and enter the common connection parameters.

Step 7 Click **Submit**.

Step 8 Click **Show Results Summary** to view the diagnosis and resolution steps.

Troubleshoot Connectivity Issues in a TrustSec-Enabled Network with IP-SGT Mappings

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **TrustSec Tools** > **IP User SGT**.

Step 2 Enter the information in the fields, as needed.

Step 3 Click **Run**.

You are prompted for additional input.

Step 4 Click **User Input Required** and modify the fields, as necessary.

Step 5 Click **Submit**.

Step 6 Click **Show Results Summary** to view the diagnosis and resolution steps.

Device SGT Tool

For devices that are enabled with the TrustSec solution, each network device is assigned an SGT value through RADIUS authentication. The Device SGT diagnostic tool connects to the network device (with the IP address that you provide) and obtains the network device SGT value. It then checks the RADIUS authentication records to determine the SGT value assigned most recently. Finally, it displays the Device-SGT pairs in a tabular format, and identifies whether the SGT values are the same or different.

Troubleshoot Connectivity Issues in a TrustSec-Enabled Network by Comparing Device SGT Mappings

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **Trustsec Tools** > **Device SGT**.

Step 2 Enter the information in the fields, as needed.

The default port number for Telnet is 23 and SSH is 22.

Step 3 Click **Run**.

Step 4 Click **Show Results Summary** to view the results of the device SGT comparison.

Obtaining Additional Troubleshooting Information

Cisco ISE allows you to download support and troubleshooting information from the Admin portal. You can use the support bundles to prepare diagnostic information for the Cisco Technical Assistance Center (TAC) to troubleshoot problems with Cisco ISE.

Note The support bundles and debug logs provide advanced troubleshooting information for TAC and are difficult to interpret. You can use the various reports and troubleshooting tools that Cisco ISE provides to diagnose and troubleshoot issues that you are facing in your network.

Cisco ISE Support Bundle

You can configure the logs that you want to be a part of your support bundle. For example, you can configure logs from a particular service to be a part of your debug logs. You can also filter the logs based on dates.

The logs that you can download are categorized as follows:

- Full configuration database: Contains the Cisco ISE configuration database in a human-readable XML format. When you troubleshoot issues, you can import this database configuration into another Cisco ISE node to re-create the scenario.
- Debug logs: Captures bootstrap, application configuration, run-time, deployment, public key infrastructure (PKI) information, and monitoring and reporting.

  Debug logs provide troubleshooting information for specific Cisco ISE components. To enable debug logs, see chapter 11 on *Logging*. If you do not enable the debug logs, all the informational messages (INFO) will be included in the support bundle. For more information, see Cisco ISE Debug Logs, on page 1398.
- Local logs: Contains syslog messages from the various processes that run on Cisco ISE.
- Core files: Contains critical information that helps identify the cause of a crash. These logs are created when the application crashes, and includes heap dumps.
- Monitoring and reporting logs: Contains information about alerts and reports.
- System logs: Contains Cisco Application Deployment Engine-related (ADE-related) information.
- Policy configuration: Contains policies configured in Cisco ISE in human-readable format.

You can download these logs from the Cisco ISE CLI by using the **backup-logs** command. For more information, see the *Cisco Identity Services Engine CLI Reference Guide*.

Note For Inline Posture node, you cannot download the support bundle from the Admin portal. You must use the **backup-logs** command from the Cisco ISE CLI.

If you choose to download these logs from the Admin portal, you can do the following:

- Download only a subset of logs based on the log type, such as debug logs or system logs.

- Download only the latest *n* number of files for the selected log type. This option allows you to control the size of the support bundle and the time taken for download.

Monitoring logs provide information about the monitoring, reporting, and troubleshooting features. For more information about downloading logs, see Download Cisco ISE Log Files, on page 1397.

Support Bundle

You can download the support bundle to your local computer as a simple tar.gpg file. The support bundle will be named with the date and time stamps in the format ise-support-bundle_ise-support-bundle-mm-dd-yyyy--hh-mm.tar..gpg. The browser prompts you to save the support bundle to an appropriate location. You can extract the content of the support bundle and view the README.TXT file, which describes the contents of the support bundle, as well as how to import the contents of the ISE database if it is included in the support bundle.

Download Cisco ISE Log Files

You can download the Cisco ISE log files to look for more information while troubleshooting issues in your network.

You can also download system logs that include ADE-OS and other log files to troubleshoot installation and upgrade issues.

While downloading a support bundle, instead of entering an encryption key manually, you can choose to use a public key for encryption. If you choose this option, Cisco PKI will be used for encryption and decryption of the support bundle. Cisco TAC maintains the public and private keys. Cisco ISE uses the public keys to encrypt the support bundle. Cisco TAC can decrypt the support bundle using the private keys. Use this option if you want to provide the support bundle to Cisco TAC for troubleshooting. Use the shared key encryption if you are going to troubleshoot the issues on premise.

Before you begin

- You must have Super Admin or System Admin privileges to perform the following task.
- You should have configured the debug logs and debug log levels.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Download Logs** > **Appliance Node List**.

Step 2 Click the node from which you want to download the support bundles.

Step 3 In the **Support Bundle** tab, choose the parameters that you want to be populated in your support bundle.

If you include all the logs, your support bundle will be excessively large and the download will take a long time. To optimize the download process, choose to download only the most recent *n* number of files.

Step 4 Enter the **From** and **To** dates for which you want to generate the support bundle.

Step 5 Choose one of the following:

- **Public Key Encryption**: Choose this option if you want to provide the support bundle to Cisco TAC for troubleshooting purposes.

- **Shared Key Encryption**: Choose this option if you want to troubleshoot the issues locally on premise. If you choose this option, you must enter the encryption key for the support bundle.

Step 6 Enter and re-enter the encryption key for the support bundle.

Step 7 Click **Create Support Bundle**.

Step 8 Click **Download** to download the newly-created support bundle.

The support bundle is a tar.gpg file that is downloaded to the client system that is running your application browser.

What to do next

Download debug logs for specific components.

Cisco ISE Debug Logs

Debug logs provide troubleshooting information for various Cisco ISE components. Debug logs contain critical and warning alarms generated over the last 30 days, and information alarms generated over the last seven days. While reporting problems, you might be asked to enable these debug logs and send them for diagnosis and resolution of your problems.

Note Enabling debug logs with heavy load (such as monitoring debug logs) will generate alarms about high load.

Obtain Debug Logs

Step 1 Configure the components for which you want to obtain debug logs. See Cisco ISE Components and Corresponding Debug Logs, on page 1398.

Step 2 Download Debug Logs.

Cisco ISE Components and Corresponding Debug Logs

Table 207: Components and Corresponding Debug Logs

Component	Debug Log
Active Directory	ad_agent.log
Cache Tracker	tracking.log
Entity Definition Framework (EDF)	edf.log
JMS	ise-psc.log
License	ise-psc.log
Notification Tracker	tracking.log
Replication-Deployment	replication.log

Component	Debug Log
Replication-JGroup	replication.log
Replication Tracker	tracking.log
RuleEngine-Attributes	ise-psc.log
RuleEngine-Policy-IDGroups	ise-psc.log
accessfilter	ise-psc.log
admin-infra	ise-psc.log
boot-strap wizard	ise-psc.log
cisco-mnt	ise-psc.log
client	ise-psc.log
cpm-clustering	ise-psc.log
cpm-mnt	ise-psc.log
epm-pdp	ise-psc.log
epm-pip	ise-psc.log
anc	ise-psc.log
anc	ise-psc.log
ers	ise-psc.log
guest	ise-psc.log
Guest Access Admin	guest.log
Guest Access	guest.log
MyDevices	guest.log
Portal	guest.log
Portal-Session-Manager	guest.log
Portal-web-action	guest.log
guestauth	ise-psc.log
guestportal	ise-psc.log
identitystore-AD	ise-psc.log
infrastructure	ise-psc.log
ipsec-api	api-service.log
ipsec-ui	ise-psc.log
mdm	ise-psc.log
mdm-pip	ise-psc.log

Component	Debug Log
mnt-report	reports.log
mydevices	ise-psc.log
nsf	ise-psc.log
nsf-session	ise-psc.log
org-apache	ise-psc.log
org-apache-cxf	ise-psc.log
org-apache-digester	ise-psc.log
posture	ise-psc.log
profiler	profiler.log
provisioning	ise-psc.log
policy-engine	ise-psc.log
prrt-JNI	prrt-management.log
runtime-AAA	prrt-management.log
runtime-config	prrt-management.log
runtime-logging	prrt-management.log
sponsorportal	ise-psc.log
swiss	ise-psc.log
telemetry	sch.log

Configure Debug Wizard by Function

The Debug wizard contains debug templates that you can use to troubleshoot issues on Cisco ISE nodes. You can configure debug profiles and the debug logs.

In the **Debug Profile Configuration** window, you can configure the debug log severity level for individual components inside the template.

In the **Debug Log Configuration** window, you can configure the severity levels for debug logs. Debug logs capture bootstrap, application configuration, runtime, deployment, monitoring, reporting, and public key infrastructure (PKI) information.

Note

- The per-node log levels take precedence over Debug wizard profiles.
- When enabling multiple profiles that edit the same component, the higher log level takes precedence, where trace has the highest priority.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Debug Wizard** > **Debug Profile Configuration** to configure a debug profile.

Step 2 To create a new profile, click **Add**.

Step 3 Enter the **Name** and **Description** of the new profile.

Step 4 Check the check boxes adjacent to the components that you want to include in the profile, and set the corresponding **Log Level** for each of the components.

Step 5 Click **Save**.

Step 6 To enable the ISE node immediately, click **Enable**. Otherwise click **Do it Later**.

Step 7 If you click **Enable**, check the check boxes adjacent to the ISE nodes for which you want to enable the profile.

Step 8 Click **Save**.

Step 9 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Debug Wizard** > **Debug Log Configuration** to configure a debug log.

Step 10 Click a radio button to choose a node.

Step 11 Click a radio button to choose a component.

Step 12 Click **Edit** to change the **Component Name**, **Log Level**, **Description** and **Log File Name** of a component.

Step 13 Click **Save**.

Download Debug Logs

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Download Logs** > **Appliance Node List**.

Step 2 From the Appliance node list, click the node for which you want to download the debug logs.

Step 3 Click the **Debug Logs** tab.

A list of debug log types and debug logs is displayed. This list is based on your debug log configuration.

Step 4 Click the log file that you want to download and save it to the system that is running your client browser.

You can repeat this process to download other log files as needed. The following are the additional debug logs that you can download from the **Debug Logs** window:

- isebootstrap.log: Provides bootstrapping log messages
- monit.log: Provides watchdog messages
- pki.log: Provides third-party crypto library logs
- iseLocalStore.log: Provides logs about the local store files
- ad_agent.log: Provides Microsoft Active Directory third-party library logs
- catalina.log: Provides third-party logs