Threat Containment

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
- 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 Apex 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/

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

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 5
Configure Cognitive Threat Analytics Adapter, on page 6
Configure Authorization Profiles for CTA Adapter, on page 6
Configure Authorization Policy using the Course of Action Attribute, on page 6
Threat Centric NAC Service, on page 1

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 4).
- 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

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 4).
- 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.

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 ChooseIn 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 4.

Step 2 To configure:

- Qualys adapter, see Configure Qualys Adapter, on page 9.
- Nexpose adapter, see Configure Nexpose Adapter, on page 11.
- Tenable adapter, see Configure Tenable Adapter, on page 13.

Step 3 Configure Authorization Profile, on page 16.

Step 4 Configure Exception Rule to Quarantine a Vulnerable Endpoint, on page 16.

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

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 5
Configure Cognitive Threat Analytics Adapter, on page 6
Configure Authorization Profiles for CTA Adapter, on page 6
Configure Authorization Policy using the Course of Action Attribute, on page 6
Threat Centric NAC Service, on page 1

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

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.
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.

Field Name	Description
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

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.

Field Name	Description
Settings for checking latest scan results	
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

Note 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.
- Cisco ISE communicates with Tenable SecurityCenter over HTTPS/SSL (port 443).

Step 1

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.
Tenable SecurityCenter Port	443

Field Name	Description
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.
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.

Field Name	Description
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

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. The navigation path for this page is **Administration** > **System** > **Certificates** > **Trusted Certificates**. Check the check box for the Trusted Certificate you want to edit, and click **Edit**.

Table 1: 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	

Field Name	Usage Guidelines
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.”
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.

Field Name	Usage Guidelines
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
Edit a Trusted Certificate

Maintenance Settings

These windows help you to manage data using the backup, restore, and data purge features.

Repository Settings

Table 2: 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.

Fields	Usage Guidelines
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 =.

Related Topics

Backup and Restore Repositories
Create Repositories

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. The navigation path for this window is **Administration** > **System** > **Backup & Restore**.

Table 3: 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-Demand and Scheduled Backups
Backup History
Backup Failures
Cisco ISE Restore Operation
Export Authentication and Authorization Policy Configuration
Synchronize Primary and Secondary Nodes in a Distributed Environment
Perform an On-Demand Backup

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. The navigation path for this window is **Administration** > **System** > **Backup and Restore**.

Table 4: 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-Demand and Scheduled Backups
Backup History
Backup Failures
Cisco ISE Restore Operation
Export Authentication and Authorization Policy Configuration
Synchronize Primary and Secondary Nodes in a Distributed Environment
Backup Using the CLI
Schedule a Backup

Schedule Policy Export Settings

The following table describes the fields on the **Schedule Policy Export** window. The navigation path for this window is **Administration** > **System** > **Backup and Restore** > **Policy Export**.

Table 5: Schedule Policy Export 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.

- **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**

Related Topics

TrustSec Architecture
TrustSec Components
Configure TrustSec Global Settings

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. The navigation path for this page is **Administration** > **Network Resources** > **Network Devices**, and click **Add**.

Network Device Settings

The following table describes the fields in the **New Network Devices** window.

Table 6: 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** text box. 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 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 7: 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	

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 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.
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 8: 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 9: 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 10: 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
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.
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.
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.

Field Name	Usage Guidelines
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.
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.
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 11: 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	
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	

Field Name	Usage Guidelines
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.
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.

Field Name	Usage Guidelines
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

Network Device Import Settings

Table 12: 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.

Manage Network Device Groups

The following windows enable you to configure and manage network device groups.

Network Device Group Settings

You can also create network device groups in the **Work Centers** > **Device Administration** > **Network Resources** > **Network Device Groups** > **All Groups** window.

Table 13: 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

Table 14: 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.

Field Name	Usage Guidelines
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.

Network Device Profile Settings

The following table describes the fields in the Network Device Profile section.

Table 15: 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 16: 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.
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 17: 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 18: 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.

Field Name	Definition
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.
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 19: 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** .

Field Name	Definition
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

Table 20: 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.

Field Name	Usage Guidelines
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.
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

Table 21: 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.

Field Name	Usage Guidelines
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.
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

Table 22: NAC Manager Settings

Fields	Usage Guidelines
Name	Enter the name of the Cisco Access Manager (CAM).
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

Global Settings for Device Portals

Choose **Work Centers** > **BYOD** > **Settings** > **Employee Registered Devices** or **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.

Portal Identification Settings for Device Portals

The navigation path for this window is: **Administration** > **Device Portal Managment** > **Blacklist 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 Blacklist, 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 the Blacklist Portal

The navigation path for this window is: **Administration** > **Device Portal Management** > **Blacklist Portal** > **Edit** > **Portal Behavior and Flow Settings** > **Portal Settings**.

Use these settings to specify values or define behavior that applies to the overall portal; not just to specific portal pages that display to the user (guests, sponsors, or employees as applicable).

- **HTTPS Port**: Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blacklist 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 Blacklist 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 Blacklist 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.

Portal Settings for BYOD and MDM Portals

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 Blacklist 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 Blacklist 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 Blacklist 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

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

- **HTTPS Port**: Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blacklist 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 Blacklist 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 Blacklist 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

Portal Settings

- **HTTPS Port**: Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the **Blacklist** 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

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

- **HTTPS Port**: Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blacklist 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 Blacklist 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 Blacklist 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

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.

Post-Login Banner Page Settings for My Devices Portals

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 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

Table 23: 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 Blacklist 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.

Field Name	Usage Guidelines
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 Blacklist endpoint identity group, and removes its certificate.
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

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

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.

Field Name	Usage Guidelines
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**.