Release Notes for Cisco Identity Services Engine, Release 3.0

First Published: 2020-09-18

Last Modified: 2024-05-23

Note Come to the Content Hub at content.cisco.com, where, using the Faceted Search feature, you can accurately zoom in on the content you want; create customized PDF books on the fly for ready reference; and can do so much more...

So, what are you waiting for? Click content.cisco.com now!

And, if you are already experiencing the Content Hub, we'd like to hear from you!

Click the **Feedback** icon on the page and let your thoughts flow!

Introduction to Cisco Identity Services Engine

Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. An administrator can then use this information to make proactive governance decisions by creating access control policies for the various network elements, including access switches, wireless controllers, Virtual Private Network (VPN) gateways, Private 5G networks, and data center switches. Cisco ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation.

Cisco ISE is available on secure network server appliances with different performance characterizations, and also as software that can be run on a virtual machines (VMs). Note that you can add more appliances to a deployment for better performance.

Cisco ISE has a scalable architecture that supports standalone and distributed deployments, but with centralized configuration and management. It also enables the configuration and management of distinct personas and services, thereby giving you the ability to create and apply services where needed in a network, but operate the Cisco ISE deployment as a complete and coordinated system.

For detailed Cisco ISE ordering and licensing information, see the *Cisco Identity Services Engine Ordering Guide*.

For information on monitoring and troubleshooting the system, see the "Monitoring and Troubleshooting Cisco ISE" section in the *Cisco Identity Services Engine Administrator Guide*.

What is New in Cisco ISE, Release 3.0?

Cisco ISE Release 3.0 uses Essentials, Advantage, and Premier licenses.

For more information about the licenses that are supported in this Cisco ISE release, see the Chapter "Licensing" in the Cisco Identity Services Engine Administrator Guide.

The new features are organized by according to the license required for the features.

Essentials License

The following features require the Cisco ISE Essentials license.

Debug Wizard by Function

The Debug Wizard contains predefined debug templates that you can use to troubleshoot issues on ISE nodes. You can configure the Debug Profiles and the Debug Logs.

Business Outcome: Cisco TAC can now enable the debug logs easily over multiple nodes in an Cisco ISE deployment. This feature helps in quicker troubleshooting.

SAML SSO for Multi-Factor Authentication

Edit the authentication context value in SAML request headings to support multifactor authentications.

Business Outcome: SAML authentication will now support multifactor authentications.

Support for Cisco ISE on VMware Cloud on Amazon Web Services and Azure VMware Solution

The process of installing Cisco ISE on VMware Cloud is exactly the same as that of installing Cisco ISE on VMware virtual machine. See Supported Virtual Environments, on page 6.

Business Outcome: Cisco ISE can be hosted on VMware Cloud on Amazon Web Services (AWS) and Azure VMware Solution (AVS).

Multiple Attributes Lookup for ODBC Identity Store

Click the **Advanced Settings** option while adding an ODBC identity store to use the attributes under the following dictionaries as input parameters in the **Fetch Attributes** stored procedure (in addition to the username and password):

- RADIUS
- Device
- Network Access (AuthenticationMethod, Device IP Address, EapAuthentication, EapTunnel, ISE Host Name, Protocol, UserName, VN, and WasMachineAuthenticated)

You can configure the stored procedures to retrieve the following output parameters from the ODBC database:

- ACL
- Security Group
- VLAN (name or number)
- Web-redirect ACL
- Web-redirect portal name

Business Outcome: You can use these attributes to configure the authorization profiles. For example, you can configure an authorization profile to use the VLAN that is returned from the ODBC database based on the specified input attributes (such as MAC address, username, called-station-ID, or device location), instead of manually specifying the VLAN for each authorization profile.

Cisco ISE API Gateway

Cisco ISE API gateway is an API management solution, which acts as a single entry point to multiple Cisco ISE Service APIs to provide better security and traffic management. The API requests from the external clients are routed to the API gateway on Cisco ISE. The requests are further forwarded to the Cisco ISE nodes where service APIs are running, based on the rules configured on the API Gateway.

Business Outcome: Enhanced conversion of information exchange and cross-domain automation for a Cisco Software Defined Access (SDA) fabric in combination with Cisco ACI infrastructure.

Certificate Fingerprinting

The certificate fingerprinting process is used to evaluate immediate issuer fingerprint SHA256 certificate with the trusted certificates. This enforces a secured mechanism for multiple certificates to support different domains. Certificate fingerprinting also allows you to lock the trusted certificates for the 802.1x protocol.

Business Outcome: Several domains are supported by multiple trusted certificates.

MSRPC Protocol for Passive ID Service

From Cisco ISE Release 3.0 onwards, you can use MS-Eventing API or Microsoft Remote Procedure Call (MSRPC) protocol for Passive Identity. Use the MSRPC protocol to establish node communication and monitor heartbeats between nodes in Cisco ISE. This option is available in addition to the WMI protocol for the Passive ID service.

The MSRPC protocol promotes a reliable mechanism when Cisco ISE or Cisco ISE-PIC collects and monitors the events from several domain controllers. It also reduces latency on the Active Directory Domain Controllers user login events.

Business Outcome: Provides a reliable mechanism for monitoring DC events.

Health Check

An on-demand health check option is introduced to diagnose all the nodes in your deployment. Running a health check on all the nodes prior to any operation helps identify critical issues, if any, that may cause downtime or blocker. Health Check provides the working status of all the dependent components. On failure of a component, it immediately provides troubleshooting recommendations to resolve the issue for a seamless execution of the operation.

Ensure that you run Health Check before initiating the upgrade process.

Business Outcome: Identify critical issues to avoid downtime or blockers.

For more information about Health Check, see the chapter "Troubleshooting" in the Cisco Identity Services Engine Administrator Guide.

Telemetry Updates

Additional network statistics are collected.

Business Outcome: The more information you can gather about customer networks, the better job you can do analyzing how to improve your products.

TCP Dump Enhancements

You now have more control over TCP dump files. You can also run TCP dump on additional interfaces.

Business Outcome: Collecting data about TCP traffic is now easier.

Resource Owner Password Credentials Flow to Authenticate Users with Microsoft Entra ID

The Resource Owner Password Credentials (ROPC) flow allows Cisco ISE to carry out authorization and authentication in a network with cloud-based identity providers. This is a controlled introduction feature. We recommend that you thoroughly test this feature in a test environment before using it in a production environment.

Business Outcome: The ROPC flow allows Cisco ISE to authorize and authenticate Microsoft Entra ID users.

Interactive Help

Interactive Help provides tips and step-by-step guidance to complete tasks with ease.

Business Outcome: This helps the end users to easily understand the work flow and complete their tasks with ease.

Advantage License

The following features require the Cisco ISE Advantage License.

New pxGrid Pages

The new pxGrid interface has new pages that separate pxGrid v1 and pxGrid v2. There is also a new Summary window with session and client information.

Business Outcome: Improves workflow when managing pxGrid sessions.

Note pxGrid 1.0, which uses legacy Extensible Messaging and Presence Protocol (XMPP) is in maintenance mode, and will be deprecated soon. We introduced pxGrid 2.0 in Cisco ISE, Release 2.4. pxGrid 2.0 uses REST and Websocket protocols, which are a simple and standardized application-to-application communications interface. We encourage partners to switch their pxGrid client implementations to these new protocols.

For more information about why we recommend a switch to pxGrid 2.0, see Welcome to Learning Cisco Platform Exchange Grid (pxGrid)

Configuration of Baseline Policies from Desktop Device Manager

When you upgrade to Cisco ISE Release 3.0, we recommend that you do not use root patches to select configuration baseline policies from the connected Desktop Device Manager servers.

You can also verify Windows endpoints with Device Identifiers instead of MAC addresses for greater accuracy, when dongles, docking stations, or MAC address randomization techniques are in use.

Business Outcome: You can check for endpoint compliance using configuration baseline policies created in Desktop Device Manager servers. Use device identifiers instead of MAC addresses for greater accuracy in endpoint identification.

Cisco ISE ACI-SDA Integration with VN Awareness

Cisco ISE Release 3.0 provides enhanced conversion of information exchange and cross-domain automation for a Cisco Software Defined Access (SDA) fabric in combination with Cisco ACI infrastructure. This implementation supports the exchange and translation of EPG and SGT information, extension of SDA Virtual Networks(VNs) into the Cisco ACI fabric, SDA and ACI fabric data plane automation, along with the exchange of IP-SGT bindings and sending the bindings to pxGrid and SXP domains.

Business Outcome: Better security and traffic management.

Minimum Version of Antivirus and Antimalware

From Cisco ISE Release 3.0 onwards, you can create a posture policy to set a minimum version of antivirus and antimalware for the endpoints in your network. This policy ensures that the endpoints comply with the minimum version of antivirus and antimalware of your network policy. It also automatically updates the condition with new versions of antivirus and antimalware, thus reducing the manual effort required to revise the condition.

Business Outcome: Enhanced security because the endpoints comply with the network policy.

Posture Session Sharing

Posture status is shared between PSNs. The status is not configurable; it is always on.

Business Outcome: Client connections do not need to rerun posture, when switching to a different PSN.

Agentless Posture

This new posture type delivers an agent to the client through SSH, and optionally removes the client when posture is complete. AnyConnect is not required. The agentless posture package is available as part of the default Cisco ISE client provisioning resources. You can select this package while creating an agent configuration to be used for the client provisioning policy.

Business Outcome: Lower footprint, and temporary posture agent is not visible to the customer.

Multi-DNAC Support

Cisco DNA Center systems cannot scale to more than the range of 25 to 100 thousand endpoints. Cisco ISE can scale to two million endpoints. Currently, you can only integrate one Cisco DNA Center system with one Cisco ISE system. Large Cisco ISE deployments can benefit by integrating multiple DNA Center clusters with a single Cisco ISE. Cisco now supports multiple Cisco DNA center clusters per Cisco ISE deployment, also known as Multi-DNAC.

Business Outcome: This feature for the Access Control app in Cisco DNA Center allows you to integrate up to four Cisco DNA Center clusters with a single Cisco ISE system.

Premier License

The following features require Cisco ISE Premier License.

Endpoint Scripts Wizard

The Endpoint Scripts Wizard allows you to run scripts on connected endpoints to carry out administrative tasks that comply with your organization's requirements. This includes tasks such as uninstalling obsolete software, starting or terminating processes or applications, and enabling or disabling specific services.

Business Outcome: Easily carry out administrative tasks on connected endpoints to comply with your organization's requirements.

System Requirements

For an uninterrupted Cisco ISE configuration, ensure that the following system requirements are fulfilled.

For more details on hardware platforms and installation of this Cisco ISE release, see the *Cisco Identity Services Engine Hardware Installation Guide*.

Supported Hardware

Cisco ISE, Release 3.0, can be installed on the following platforms:

Table 1: Supported Platforms

Hardware Platform	Configuration
Cisco SNS-3515-K9 (small)	For appliance hardware specifications, see the *Cisco Secure Network Server Appliance Hardware Installation Guide*.
Cisco SNS-3595-K9 (large)	
Cisco SNS-3615-K9 (small)	
Cisco SNS-3655-K9 (medium)	
Cisco SNS-3695-K9 (large)	

After installation, you can configure Cisco ISE with specific component personas such as Administration, Monitoring, or pxGrid on the platforms that are listed in the above table. In addition to these personas, Cisco ISE contains other types of personas within Policy Service, such as Profiling Service, Session Services, Threat-Centric NAC Service, SXP Service for TrustSec, TACACS+ Device Admin Service, and Passive Identity Service.

Caution

- *Cisco ISE 3.1 Patch 6 and above versions support Cisco SNS 3700 series appliances.
- Cisco ISE 3.1 and later releases do not support Cisco Secured Network Server (SNS) 3515 appliance.
- Cisco SNS 3400 Series appliances are not supported in Cisco ISE, Release 2.4, and later.
- Memory allocation of less than 16 GB is not supported for VM appliance configurations. In the event of a Cisco ISE behavior issue, all the users will be required to change the allocated memory to at least 16 GB before opening a case with the Cisco Technical Assistance Center.
- Legacy Access Control Server (ACS) and Network Access Control (NAC) appliances (including the Cisco ISE 3300 Series) are not supported in Cisco ISE, Release 2.0, and later.

Supported Virtual Environments

Cisco ISE supports the following virtual environment platforms:

- VMware ESXi 5.x, 6.x, 7.x, 8.x

  For Cisco ISE Release 3.0 and later releases, we recommend that you update to VMware ESXi 7.0.3 or later releases.

  - Cisco ISE has been validated with Cisco HyperFlex HX-Series with VMware ESXi 6.5.
  - You can deploy Cisco ISE on VMware cloud solutions on the following public cloud platforms:
    - VMware cloud in Amazon Web Services (AWS): Host Cisco ISE on a software-defined data centre provided by VMware Cloud on AWS.
    - Azure VMware Solution: Azure VMware Solution runs VMware workloads natively on Microsoft Azure. You can host Cisco ISE as a VMware virtual machine.
    - Google Cloud VMware Engine: Google Cloud VMware Engine runs software defined data centre by VMware on the Google Cloud. You can host Cisco ISE as a VMware virtual machine on the software defined data centre provided by the VMware Engine.

- Microsoft Hyper-V on Microsoft Windows Server 2012 R2 and later
- KVM on QEMU 1.5.3-160

  Note Cisco ISE cannot be installed on OpenStack.

- Nutanix AHV 20201105.2096

For information about the virtual machine requirements, see the *Cisco Identity Services Engine Installation Guide* for your version of Cisco ISE.

Note From Cisco ISE Release 3.0 onwards, the CPUs of the virtualization platform that hosts Cisco ISE virtual machines must support the Streaming SIMD Extensions (SSE) 4.2 instruction set. Otherwise, certain Cisco ISE services (such as ISE API gateway) will not work, and the Cisco ISE GUI cannot be launched. Both Intel and AMD processors support SSE Version 4.2 since 2011.

Federal Information Processing Standard (FIPS) Mode Support

Cisco ISE uses embedded Federal Information Processing Standard (FIPS) 140-2-validated cryptographic module, Cisco FIPS Object Module Version 6.2 (Certificate #2984). For details about the FIPS compliance claims, see Global Government Certifications.

When FIPS mode is enabled on Cisco ISE, consider the following:

- All non-FIPS-compliant cipher suites will be disabled.
- Certificates and private keys must use only FIPS-compliant hash and encryption algorithms.
- RSA private keys must be 2048 bits or greater.
- Elliptical Curve Digital Signature Algorithm (ECDSA) private keys must be 224 bits or greater.

- Diffie–Hellman Ephemeral (DHE) ciphers work with Diffie–Hellman (DH) parameters of 2048 bits or greater.
- SHA1 is not allowed to generate ISE local server certificates.
- The anonymous PAC provisioning option in EAP-FAST is disabled.
- The local SSH server operates in FIPS mode.
- The following protocols are not supported in FIPS mode for RADIUS:
  - EAP-MD5
  - PAP
  - CHAP
  - MS-CHAPv1
  - MS-CHAPv2
  - LEAP

Supported Browsers

The supported browsers for the Admin portal include:

- Mozilla Firefox 96 and earlier versions from version 82
- Mozilla Firefox ESR 91.3 and earlier versions
- Google Chrome 97 and earlier versions from version 86
- Microsoft Edge, the latest version and one version earlier than the latest version

Validated External Identity Sources

Note The supported Active Directory versions are the same for both Cisco ISE and Cisco ISE-PIC.

Table 2: Validated External Identity Sources

External Identity Source	Version
Active Directory[1]	
Microsoft Windows Active Directory 2012	Windows Server 2012
Microsoft Windows Active Directory 2012 R2[2]	Windows Server 2012 R2
Microsoft Windows Active Directory 2016	Windows Server 2016

External Identity Source	Version
Microsoft Windows Active Directory 2019	Windows Server 2019
LDAP Servers	
SunONE LDAP Directory Server	Version 5.2
OpenLDAP Directory Server	Version 2.4.23
Any LDAP v3 compliant server	Any version that is LDAP v3 compliant
Token Servers	
RSA ACE/Server	6.x series
RSA Authentication Manager	7.x and 8.x series
Any RADIUS RFC 2865-compliant token server	Any version that is RFC 2865 compliant
Security Assertion Markup Language (SAML) Single Sign-On (SSO)	
Microsoft Azure MFA	Latest
Oracle Access Manager (OAM)	Version 11.1.2.2.0
Oracle Identity Federation (OIF)	Version 11.1.1.2.0
PingFederate Server	Version 6.10.0.4
PingOne Cloud	Latest
Secure Auth	8.1.1
Any SAMLv2-compliant Identity Provider	Any Identity Provider version that is SAMLv2 compliant
Open Database Connectivity (ODBC) Identity Source	
Microsoft SQL Server	Microsoft SQL Server 2012 Microsoft SQL Server 2022
Oracle	Enterprise Edition Release 12.1.0.2.0
PostgreSQL	9.0
Sybase	16.0
MySQL	6.3
Social Login (for Guest User Accounts)	
Facebook	Latest

[1] Cisco ISE OCSP functionality is available only on Microsoft Windows Active Directory 2008 and later.

[2] Cisco ISE supports all the legacy features in Microsoft Windows Active Directory 2012 R2. However, the new features in Microsoft Windows Active Directory 2012 R2, such as Protective User Groups, are not supported.

See the *Cisco Identity Services Engine Administrator Guide* for more information.

Supported Antivirus and Antimalware Products

For information about the antivirus and antimalware products supported by the Cisco ISE posture agent, see Cisco AnyConnect ISE Posture Support Charts.

Validated OpenSSL Version

Cisco ISE is validated with OpenSSL 1.0.2.x (CiscoSSL 6.0).

Known Limitations and Workarounds

This section provides information about the various known limitations and the corresponding workarounds.

Hot Patch for RADIUS Live Log Delays

In Cisco ISE Release 3.0 Cumulative Patch 8, you may experience RADIUS live logs delay as explained in CSCwi06794. You must install the following hot patch to fix this issue: ise-apply-CSCwi06794_3.0.0.458_patch8-SPA.tar.gz.

Incorrect Smart Licensing Consumption Reports

After you upgrade to Cisco ISE Release 3.0 Patch 7, if your smart licensing configuration uses the connection methods Direct HTTPS or HTTPS Proxy, you may witness incorrect compliance statuses being reported. Incorrect license consumption counts may be reported due to a communication error between Cisco ISE and CSSM.

To troubleshoot the communication error, in the **Licensing** window of the Cisco ISE administration portal, deregister and then reregister your smart licensing.

Authentication Might Fail for SNMP Users After Upgrade due to Wrong Hash Value

If you are upgrading from Cisco ISE 2.7 or earlier release to Cisco ISE 3.0, you must reconfigure the settings for SNMP users after the upgrade. Otherwise, authentication might fail for SNMP users because of wrong hash value.

Use the following commands to reconfigure the settings for SNMPv3 users:

no snmp-server user ***<snmp user> <snmp version> <auth password> <priv password>***

snmp-server user ***<snmp user> <snmp version> <auth password> <priv password>***

Online Help in Japanese

If you have configured your localization settings to enable Japanese in your Cisco ISE, note that the Online Help does not include information on new features introduced in this release. See *Cisco ISE Administration Guide, Release 3.0* for information on these features.

Radius Logs for Authentication

Details of an authentication event can be viewed in the **Details** field of the **Radius Authentications** window. The details of an authentication event are available only for 7 days, after which no data on the authentication event will be visible. All the authentication log data will be removed when a purge is triggered.

LDAP Server Reconfiguration after Upgrade

Limitation

The primary Hostname or IP is not updated which causes authentication failures. This is because while upgrading the Cisco ISE deployment, the deployment IDs tend to reset.

Condition

When you enable the **Specify server for each ISE node** option in the **Connection** window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **External Identity Sources** > **LDAP** > **Add** or choose and an existing server, and then upgrade your Cisco ISE deployment which has PSNs, the deployment IDs tend to reset.

Workaround

Reconfigure the LDAP Server settings for each node. For more information, see **LDAP Identity Source Settings** section in the *Administrative Access to Cisco ISE Using an External Identity Store* chapter in the "Cisco Identity Services Engine Administrator Guide, Release 2.4".

Valid User-Agent Header

From Cisco ISE Release 2.7, Cisco ISE requires a valid User-Agent header sent along in a web request to a Cisco ISE end-user facing portal, such as a Cisco ISE sponsor portal, to receive successful or redirects responses.

Response Status Lines

From Cisco ISE Release 2.7, Cisco ISE web services and portals return response status lines containing only the HTTP versions and the status codes, but not the corresponding reason phrases.

Server IP Update Under Trustsec AAA Server List

When the IP address of the Cisco ISE instance is changed using the CLI, Cisco ISE services are restarted. After the services are up, you must change the IP address of the Trustsec AAA server. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Workcenters** > **TrustSec** > **Components** > **Trustsec Servers** > **Trustsec AAA Servers**.

Upgrade Information

- License Changes, on page 12
- Upgrade Procedure Prerequisites

Upgrading to Release 3.0

You can directly upgrade to Release 3.0 from the following Cisco ISE releases:

- 2.4
- 2.6
- 2.7

If you are on a version earlier than Cisco ISE, Release 2.4, you must first upgrade to one of the releases listed above, and then upgrade to Release 3.0.

Note We recommend that you upgrade to the latest patch in the existing version before starting the upgrade.

Upgrade Packages

For information about the upgrade packages and the supported platforms, see Cisco ISE Software Download.

License Changes

The licenses that are used for Cisco ISE Releases 2.x, such as Base, Plus, and Apex, have been replaced with new license types. Cisco ISE Release 3.0 uses Essentials, Advantage, and Premier licenses. See the Chapter “Licensing” in the *Cisco Identity Services Engine Administrator Guide*.

You must convert your existing smart or traditional licenses to the new license type through the Cisco Smart Software Manager (CSSM), to enable license consumption in Cisco ISE Release 3.0.

Upgrade Procedure Prerequisites

- Run the Upgrade Readiness Tool (URT) before the upgrade to check whether the configured data can be upgraded to the required Cisco ISE version. Most upgrade failures occur because of data upgrade issues. The URT validates the data before the actual upgrade and reports the issues, if any. The URT can be downloaded from the Cisco ISE Download Software Center.
- We recommend that you install all the relevant patches before beginning the upgrade.

For more information, see the Cisco Identity Services Engine Upgrade Guide.

Telemetry

After installation, when you log in to the Admin portal for the first time, the Cisco ISE Telemetry banner is displayed. Using this feature, Cisco ISE securely collects nonsensitive information about your deployment, network access devices, profiler, and other services that you are using. This data will be used to provide better services and more features in the forthcoming releases. By default, telemetry is enabled. To disable or modify the account information, choose **Administration** > **Settings** > **Network Settings Diagnostics** > **Telemetry**. The account is unique for each deployment. Each admin user need not provide it separately.

Telemetry provides valuable information about the status and capabilities of Cisco ISE. Telemetry is used by Cisco to improve appliance lifecycle management for IT teams who have deployed Cisco ISE. Collecting this data helps the product teams serve customers better. This data and related insights enable Cisco to proactively identify potential issues, improve services and support, facilitate discussions to gather additional value from new and existing features, and assist IT teams with inventory report of license entitlement and upcoming renewals.

It may take up to 24 hours after the Telemetry feature is disabled for Cisco ISE to stop sharing telemetry data.

Types of data collected include Product Usage Telemetry and Cisco Support Diagnostics.

Cisco Support Diagnostics

The Cisco Support Diagnostics Connector enables Cisco Technical Assistance Center (TAC) and Cisco support engineers to obtain support information on the deployment through the primary administration node. By default, this feature is disabled. See the Cisco Identity Services Engine Administrator Guide for instructions on how to enable this feature.

Cisco ISE Live Update Portals

Cisco ISE Live Update portals help you to automatically download the **Supplicant Provisioning** wizard, AV/AS support (Compliance Module), and agent installer packages that support client provisioning and posture policy services. These live update portals are configured in Cisco ISE during the initial deployment to retrieve the latest client provisioning and posture software directly from Cisco.com to the corresponding device using Cisco ISE.

If the default Update portal URL is not reachable and your network requires a proxy server, configure the proxy settings. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration > System > Settings > Proxy** before you access the Live Update portals. If proxy settings allow access to the profiler, posture, and client-provisioning feeds, access to a Mobile Device Management (MDM) server is blocked because Cisco ISE cannot bypass the proxy services for MDM communication. To resolve this, you can configure the proxy services to allow communication to the MDM servers. For more information on proxy settings, see the "Specify Proxy Settings in Cisco ISE" section in the Cisco Identity Services Engine Administrator Guide.

Client Provisioning and Posture Live Update Portals

You can download Client Provisioning resources from:

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Posture** > **Settings** > **Software Updates** > **Client Provisioning.**

The following software elements are available at this URL:

- Supplicant Provisioning wizards for Windows and Mac OS X native supplicants
- Windows versions of the latest Cisco ISE persistent and temporal agents
- Mac OS X versions of the latest Cisco ISE persistent agents
- ActiveX and Java Applet installer helpers
- AV/AS compliance module files

For more information on automatically downloading the software packages that are available at the Client Provisioning Update portal to Cisco ISE, see the "Download Client Provisioning Resources Automatically" section in the "Configure Client Provisioning" chapter in the Cisco Identity Services Engine Administrator Guide.

You can download Posture updates from:

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Posture** > **Settings** > **Software Updates** > **Posture Updates**

The following software elements are available at this URL:

- Cisco-predefined checks and rules
- Windows and Mac OS X AV/AS support charts
- Cisco ISE operating system support

For more information on automatically downloading the software packages that become available at this portal to Cisco ISE, see the "Download Posture Updates Automatically" section in the Cisco Identity Services Engine Administrator Guide.

If you do not want to enable the automatic download capabilities, you can choose to download updates offline.

Cisco ISE Offline Updates

This offline update option allows you to download client provisioning and posture updates, when direct internet access to Cisco.com from a device using Cisco ISE is not available or is not permitted by a security policy.

To download offline client provisioning resources:

Procedure

Step 1 Go to: https://software.cisco.com/download/home/283801620/type/283802505/release/3.0.0.

Step 2 Provide your login credentials.

Step 3 Navigate to the Cisco Identity Services Engine download window, and select the release.

The following Offline Installation Packages are available for download:

- **win_spw-<*version*>-isebundle.zip**—Offline SPW Installation Package for Windows
- **mac-spw-<*version*>.zip**—Offline SPW Installation Package for Mac OS X
- **compliancemodule-<*version*>-isebundle.zip**—Offline Compliance Module Installation Package
- **macagent-<*version*>-isebundle.zip**—Offline Mac Agent Installation Package
- **webagent-<*version*>-isebundle.zip**—Offline Web Agent Installation Package

Step 4 Click either **Download** or **Add to Cart**.

For more information on adding the downloaded installation packages to Cisco ISE, see the "Add Client Provisioning Resources from a Local Machine" section in the Cisco Identity Services Engine Administrator Guide.

You can update the checks, operating system information, and antivirus and antispyware support charts for Windows and Mac operating systems offline from an archive in your local system, using posture updates.

For offline updates, ensure that the versions of the archive files match the versions in the configuration file. Use offline posture updates after you configure Cisco ISE and want to enable dynamic updates for the posture policy service.

To download offline posture updates:

Procedure

Step 1 Go to https://www.cisco.com/web/secure/spa/posture-offline.html.

Step 2 Save the **posture-offline.zip** file to your local system. This file is used to update the operating system information, checks, rules, and antivirus and antispyware support charts for Windows and Mac operating systems.

Step 3 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture**.

Step 4 Click the arrow to view the settings for posture.

Step 5 Click **Updates**.
The **Posture Updates** window is displayed.

Step 6 Click the **Offline** option.

Step 7 Click **Browse** to locate the archive file (posture-offline.zip) from the local folder in your system.

Note The **File to Update** field is a mandatory field. You can select only one archive file (.zip) containing the appropriate files. Archive files other than .zip, such as .tar, and .gz are not supported.

Step 8 Click **Update Now**.

Configuration Prerequisites

- The relevant Cisco ISE license fees should be paid.
- The latest patches should be installed.
- Cisco ISE software capabilities should be active.

See the following resources to configure Cisco ISE:

- Getting started with Cisco ISE
- Videos on the Cisco ISE Channel on YouTube
- *Cisco ISE Design and Integration Guides*
- *Cisco Identity Services Engine Administrator Guide*

Monitoring and Troubleshooting

For information on monitoring and troubleshooting the system, see the "Monitoring and Troubleshooting Cisco ISE" section in the *Cisco Identity Services Engine Administrator Guide*.

Ordering Information

For detailed Cisco ISE ordering and licensing information, see the *Cisco Identity Services Engine Ordering Guide*.

Cisco ISE Integration with Cisco Catalyst Center

Cisco ISE can integrate with Catalyst Center. For information about configuring Cisco ISE to work with Catalyst Center, see the *Cisco Catalyst Center documentation*.

For information about Cisco ISE compatibility with Catalyst Center, see the *Cisco SD-Access Compatibility Matrix*.

Cisco AI Endpoint Analytics

Cisco AI Endpoint Analytics is a solution on Cisco DNA Center that improves endpoint profiling fidelity. It provides fine-grained endpoint identification and assigns labels to various endpoints. Information gathered through deep-packet inspection, and probes from sources such as Cisco ISE, Cisco SD-AVC, and network devices, is analyzed for endpoint profiling.

Cisco AI Endpoint Analytics also uses artificial intelligence (AI) and machine learning capabilities to intuitively group endpoints with similar attributes. IT administrators can review such groups and assign labels to them. These endpoint labels are then available in Cisco ISE if your Cisco ISE account is connected to on-premises Cisco DNA Center.

These endpoint labels from Cisco AI Endpoint Analytics can be used by Cisco ISE administrators to create custom authorization policies. You can provide the right set of access privileges to endpoints or endpoint groups through such authorization policies.

Install a New Patch

To obtain the patch file that is necessary to apply a patch to Cisco ISE, log in to the Cisco Download Software site at https://software.cisco.com/download/home (you will be required to provide your Cisco.com login credentials), navigate to **Security** > **Access Control and Policy** > **Cisco Identity Services Engine** > **Cisco Identity Services Engine Software**, and save a copy of the patch file to your local machine.

For instructions on how to apply the patch to your system, see the "Cisco ISE Software Patches" section in the Cisco Identity Services Engine Upgrade Journey.

For instructions on how to install a patch using the CLI, see the "Patch Install" section in the *Cisco Identity Services Engine CLI Reference Guide*.

Note Cisco ISE Release 3.0 Patch 2 and later releases support the licensing feature SSM On-Prem connection method. If you enable this feature and need to roll back to Cisco ISE 3.0 Patch 1 or earlier, you must disable the licensing feature before you uninstall the patch with the licensing feature.

Automatic Root CA Certificate Regeneration

From Cisco ISE Release 3.0 Patch 6, you must regenerate the root CA certificate when you install a new patch.

- In a standalone node, when you install a patch through the CLI or the GUI, the root CA certificate is automatically regenerated.
- In a distributed deployment, if you install a patch through the CLI, you must regenerate the root CA certificate after the patch is installed. If you install a patch through the Cisco ISE GUI, root CA certificate is automatically regenerated.

If you roll back from Cisco ISE Release 3.0 Patch 6 or later releases to Cisco ISE Release 3.0 Patch 5 or earlier releases, you must regenerate the root CA certificate in the Cisco ISE release that you roll back to.

For information on how to generate a root CA certificate, see the topic "Generate Root CA and Subordinate CAs on the Primary PAN and PSN" in the Chapter "Basic Setup" in the *Cisco ISE Administrator Guide*.

Caveats

The Caveats section includes the bug ID and a short description of the bug. For details on the symptoms, conditions, and workaround for a specific caveat, use the Cisco Bug Search Tool (BST).

Note The Open Caveats sections list the open caveats that apply to the current release and might apply to releases earlier than Cisco ISE 3.0. A caveat that is open for an earlier release and is still unresolved applies to all future releases until it is resolved.

Resolved Caveats in Cisco ISE Release 3.0 - Cumulative Patch 8

The following table lists the resolved caveats in Release 3.0 cumulative patch 8.

Identifier	Headline
CSCwd45783	pxGrid session publishing stops when reintergrating FMC while P-PIC is down
CSCwe17954	Cisco Identity Services Engine Information Disclosure Vulnerability
CSCwe17953	Cisco Identity Services Engine Path Traversal Vulnerability
CSCwe55215	ISE smart licensing now using smart transport
CSCvy86859	Mac OS Beta Monterey (MacOS 12 beta 2) failing NSP MacOsXSPWizard v3.1.0.2
CSCwe37978	while exporting Scheduled report with huge size coming as empty on the repository.
CSCwe37018	ISE-DNAC Integration Fails If There Are Invalid Certificates In ISE Trusted Store
CSCwe86494	ISE displaying tomcat stacktrace when using a specific URL
CSCwd51812	ISE 3.1 patch 4 : GUI : Certificate Authentication : Permissions

Identifier	Headline
CSCwf21960	During upgrade the deregister call fails to remove all the nodes from the DB
CSCwe53550	ISE and CVE-2023-24998
CSCwe36063	No validation of PBIS reg key configuration on advance tuning page.
CSCwf66237	ISE Get All Endpoints request takes much longer time to execute since 2.7
CSCwe69189	LSD is causing high bandwidth utilization
CSCwd26845	ISE 3.2 : APIC Integration : missing fvIP subscription
CSCwd97551	ISE cannot retrieve multiple attribute values from client certificate in EAP-TLS session resumption
CSCwe84609	guest sponsor portal country code issue
CSCwe63320	ISE 3.2/3.1/3.0 displays mismatched information on "Get All Endpoints" report
CSCwb28410	/ in Command Arguments not Preserved after CSV Import of T+ Command Set
CSCwf33421	Update warning message while changing Timezone
CSCwd93719	Cisco Identity Services Engine XML External Entity Injection Vulnerability
CSCwd92835	Network Device Profile shows HTML code as name
CSCwf33128	Radius used space reports incorrect usage as it also taken into account few TACACS tables
CSCwe96739	TLS 1.0/1.1 accepted at ISE 3.0 admin portal
CSCwd35608	ISE is sending old Audit Session ID in reath CoA after previously successful port-bounce CoA
CSCwa52678	GUI TCPDUMP gets stuck on Stop_In_Progress
CSCwe00424	ISE- SQLException sent to the Collection Failure Alarm caused by NAS-Port-id length
CSCwe14808	ISE fails to translate AD attribute of msRASSavedFramedIPAddress
CSCwc57162	Certificate based GUI admin login stuck
CSCwd47111	ISE is unable to save the Subnet/IP Address Pool Name for voice vlans.
CSCwd13201	UI crashed while loading authz policy on chrome and edge browser
CSCwd38137	Cisco Identity Services Engine XML External Entity Injection Vulnerability
CSCwd38136	Cisco Identity Services Engine Denial of Service Vulnerability
CSCwe07354	Radius Token Server config accepts empty host IP for Secondary Server
CSCwd51409	ISE cannot retrieve repositories and scan policies of Tenable Security Center

Identifier	Headline
CSCwe36242	TACACS Command Accounting report export is not working
CSCwf13630	Mnt Log Processor service stops every night
CSCwd24286	ISE not sending hostname attribute to DNAC
CSCwe44750	Persisting of Reprofiling result is not updating to Oracle/VCS after feed incremental update
CSCwf31477	profiler is triggering Port Bounce when there are multiple sessions exist on a switch port
CSCwc79321	Unable to change the Identity source from internal to external RSA/RADIUS-token server
CSCwe68336	Posture Assessment By Condition generates ORA-00904: "SYSTEM_NAME": invalid identifier
CSCwc05718	ISE Debug Wizard Posture profile does not contain client-webapp component to DEBUG
CSCwd97606	Multiple requests for same IP+VN+VPN combinations with diff session ID creating duplicate records
CSCwd39746	For SCCM integration with ISE need MSAL support as MS is deprecating ADAL
CSCwd90870	Improvement of logs in association with ISE SXP conflict causing warning in DNAC
CSCwa62202	ISE with 2 interfaces configured for portal access is broken
CSCwe33360	Anomalous behavior detection is not working as expected
CSCwf26951	Profiler CoA sent with the wrong session ID
CSCwe57764	MDM - Connection to Microsoft SCCM fails after Windows DCOM Server Hardening for CVE-2021-26414
CSCwc48311	ISE vPSN with IMS performance degrades by 30-40% compared to UDP syslog
CSCwd05040	Unable to import certificates on Secondary node post Registration to the deployment
CSCwd12357	SXP service gets stuck in initializing due to an exception on 9644.
CSCwe27438	Launch page level help not working for Patch Management, Upgrade, and Health Checks
CSCwd69072	Session directory write failed alarm with Cisco NAD using "user defined" NAD profile
CSCvz86446	ISE Replication: SyncRequest timeout monitor thread does not kill file transfer after timeout
CSCwb18744	SG and contracts with multiple backslash characters in a row in the description cannot sync to ISE

Identifier	Headline
CSCwf42496	Attempt to delete "Is IPSEC Device" NDG causes all subsequent RADIUS/T+ authentications to fail
CSCwe02315	Online Page level Help IDs for meraki-connector pages in ISE GUI
CSCwd89657	ISE 3.1 certain SFTP servers stopped working after upgrade to patch 4/5
CSCwd87161	ISE 3.1/ Certificate based login asks for license file if only the Device Admin license is enabled
CSCvv90394	ISE 2.6 p7 is not able to match "identityaccessrestricted equals true" in Auth Policy.
CSCwb85502	CIAM: xstream 1.4.17
CSCwd30039	Cisco Identity Services Engine Command Injection Vulnerability
CSCwf80292	ISE cannot retrieve a peer certificate during EAP-TLS authentication
CSCwc93253	ISE - Network device captcha only prompting when filter matches only 1 Network device
CSCwe54318	SXP service gets stuck into initializing due to H2 DB delay in querying Bindings
CSCwe08177	URT failing for upgrade from 2.6/2.7 to 3.1
CSCwc47015	Fix for CSCvz85074 breaks AD group retrieval in ISE
CSCwa65723	Unable to login successfully into ISE GUI through ipv6 address
CSCwe92624	ISE Africa/Cairo Timezone DST
CSCvg66764	[ENH] Session stitching support with ISE PIC Agent
CSCwe92177	ISE: Mexico Time Zone Incorrectly Changing to Daylight Saving
CSCwf07855	ISE SXP Bindings API call returns 2xx response when the call failed
CSCwe30235	Vulnerabilities in jszip 3.0.0
CSCwf15130	Permission for collector.log file is set as root root automatically
CSCwe30606	Not able to download support bundle with size over 1GB from GUI
CSCwd64649	Cisco DNA Center integration issue due to more internal CA certificates
CSCwe44886	ISE 2.7 patch 8 lowers read test speeds from CLI causing "Insufficient Virtual Machine Resources"
CSCwf26226	CPU spike due memory leak with EP purge call
CSCvo61351	ISE: Live Session get stuck at "Authenticated" state
CSCwd57978	All NADs are getting deleted while doing Filter on NDG Location and IP

Open Caveats in Cisco ISE Release 3.0 - Cumulative Patch 8

There are no open caveats in Cisco ISE Release 3.0 Patch 8.

New Features in Cisco ISE Release 3.0 - Cumulative Patch 7

Support for Cisco Secure Client

Cisco ISE 3.0 Patch 7 supports both AnyConnect and Cisco Secure Client for Windows, macOS, and Linux operating systems. The following Cisco Secure Client versions are supported for these operating systems:

- Windows: Cisco Secure Client version 5.00529 and later
- macOS: Cisco Secure Client version 5.00556 and later
- Linux: Cisco Secure Client version 5.00556 and later

You can configure both AnyConnect and Cisco Secure Client for your endpoints on these operating systems but only one policy will be considered at run time for an endpoint.

Required URL for Smart Licensing

Cisco ISE Release 3.0 Patch 7 uses https://smartreceiver.cisco.com to obtain Smart Licensing information.

Resolved Caveats in Cisco ISE Release 3.0 - Cumulative Patch 7

The following table lists the resolved caveats in Release 3.0 cumulative patch 7.

Caveat ID Number	Description
CSCwb99693	User Attributes fetching from ODBC even didn't config on ISE
CSCwc71060	Deleted network device groups still show up in policy sets
CSCwc51239	Make a Wish link is updated to a new location
CSCwd10864	XML External Entity Injection Vulnerability
CSCwd30994	Static default route with gateway of interfaces other than Gig 0 breaks network connectivity
CSCwc61320	Support Bundle page loads slowly due to Download Logs page loading in the background
CSCwc09435	Error handling/ messaging for mobile number format not clear
CSCwc24126	Profiler Condition does not display the Attribute Value
CSCwc57294	Duplicate Manager does not remove packet when there is an exception in reading configuration
CSCwc00162	Certificate based administrator login does not work when client/browser sends more than one certificate
CSCwd27506	ISE 3.0 patch 6 : Missing Scheduled Reports

Caveat ID Number	Description
CSCvw51787	ISE does not allow import of CA signed certificate on top of self-signed certificate
CSCwc30811	Underscore is vulnerable in Guest Portals
CSCwb24002	ERS SDK authentication settings are not disabled via API call
CSCwd94235	31p5 : App server and API gateway service do not run
CSCwc52685	ENH: ISE with Twilio MessagingServiceSid for SMS gateway
CSCwb56878	No Replication Stopped Alarm triggered
CSCwb55232	Create a nested endpoint group using ERS API
CSCvv87286	Fail to import Internal CA and key from ISE 2.7P2 to 3.0
CSCwc64346	ERS SDK network device bulk request documentation is not correct
CSCwc30019	CIAM: openssl 1.0.2n
CSCwd42311	Unable to download rest-id-store from Download Logs on GUI
CSCwc12303	PGA memory used by the instance exceeds PGA_AGGREGATE_LIMIT on MNT node
CSCwc31482	NetworkSetupAssistance.exe digital signature certificate expired in BYOD flow using Windows SPW
CSCwc74531	Hourly cron should clean up the cached buffers instead of 95% memory usage
CSCwc91917	Unable to add quotation character in TACACS authorization profile
CSCwd71574	High CPU Utilization when Agentless Posture is configured
CSCwc21890	Passive Easy Connect does not work in ISE with Dedicated MnT nodes
CSCwb29498	High Operations DB Usage Alarm percentage need to be configurable.
CSCwc69492	Metaspace exhaustion causes crashes on ISE node
CSCwb75959	Stored Cross-Site Scripting vulnerability
CSCwc87670	ISE 3.1 Patch 3 is unable to import endpoints from csv file if SAML is used
CSCwb82141	Context Visibility Endpoints and NADs from an existing deployment are not removed after restore operation
CSCwc72251	PxGrid publishing changed for accounting stop
CSCwc18751	Unable to download a created support bundle from GUI when logging in using the format DomainName\UserName
CSCvy32277	TLSv1.1 enabled on port 8084

Caveat ID Number	Description
CSCwd03009	RMQForwarder thread to control based on hardware appliance in platform.properties on 2.7 p7
CSCwb52396	PRA failover
CSCwc59570	ISE send SXP MSG size and 4096 bytes in SXP Version 4
CSCwa55233	Queue Link Errors "Unknown CA" when utilizing third-party signed certificate for IMS
CSCvz57222	ISE 3.0: Admin access is allowed for ISE GUI with secondary interfaces GigabitEthernet 1 and Bond 1
CSCwc75572	3.2:Maxscale: PPAN application server stuck at initializing state
CSCwd45843	Auth Step latency for policy evaluation due to GC activity
CSCwc74206	ISE 3.0 does not save SCCM MDM server object with new password, works when new instance is used
CSCwb88851	Inconsistent IP to SGT mapping after several re-authentication attempts when VN value changes
CSCwb26965	ISE 3.1: Error while creating network device groups through REST API
CSCwc57939	ISE detects large VMs as Unsupported
CSCwc62413	Cross-Site Scripting vulnerability
CSCwb79056	ISE 3.1 ERS call /ers/config/sgmapping/{id} does not return SGT value for custom SGTs
CSCwc98828	Interface feature insufficient access control vulnerability
CSCwc07283	ISE 3.1: Context visibility endpoint authentication tab does not show data
CSCwc98823	Command injection vulnerability
CSCwc57240	GUI does not validate default value while adding custom attributes
CSCwb59162	ISE 3.1 REST API typo in SNMP password parameters
CSCwc26241	ISE 3.2 displays the error: "TypeError: Cannot read properties of undefined (reading 'attr')"
CSCwa95889	Unable to add SSH/SFTP to hosts w/ newer HostKey algorithms (e.g. rsa-sha2-512)
CSCwb26227	CIAM: jackson-databind 2.9.8
CSCwb88360	Disable temporary MNT persona on upgraded node fails in split upgrade
CSCwb85456	CIAM: openssl upgrade to 1.0.2ze and 1.1.1o
CSCwc65802	Save button for SAML configuration grayed out

Caveat ID Number	Description
CSCwc12693	ERS validation error - mandatory fields missing: [validDays]
CSCwb91392	Health check and full upgrade precheck times out when third party CA certificate is used for admin
CSCwc65711	MAC - CSC 5.0554 web deployment packages fail to upload
CSCwc09104	Guest redirect with Auth vlan no longer works on ISE 3.1
CSCvv10712	Sec_txnlog_master table should be truncated post 2M record count
CSCwb86283	All nodes thrown OUT_OF_SYNC as a result of incorrect cert expiry check
CSCvx49736	containerd.io RPM package openssl 1.0.2r CIAM CVE-2021-23841 + others
CSCwc64275	Precheck may get timed out with optimistic locking failed in ise-psc.log on ppan
CSCwc98833	Cross-site scripting vulnerability
CSCwc98831	Stored cross-site scripting vulnerability
CSCwb47255	Supported HTTP methods are visible
CSCwd74560	PUT operation failure with payload through DNAC to ISE (ERS)
CSCwc42712	ISE RADIUS and PassiveID session merge
CSCwc15013	Add serviceability and fix "Could not get a resource since the pool is exhausted" error on ISE 3.0
CSCwd31405	Latency observed during query of Session.PostureStatus
CSCvz65945	"Invalid Length" TACACS auth failures within Live Logs for non-TACACS traffic
CSCwc85867	Change Configuration Audit Report does not clearly indicate SGT create and delete events
CSCwb27894	EAP-TEAP with EAP-TLS unable to match condition that has "CERTIFICATE.Issuer - Common Name"
CSCvz91479	Schema upgrade fails while modifying constraints for 3.1 and 3.2.0.804 upgrade
CSCwb81416	ISE 3.1 GUI does not load post login
CSCwc23593	LSD is causing high CPU
CSCwc93451	Profiler should ignore non-positive RADIUS syslog messages for forwarding from default RADIUS probe
CSCvv54351	Device administration using RADIUS does not consume base license
CSCwa59924	SSH from ISE to FIPS enabled device does not work

Caveat ID Number	Description
CSCwc44614	Using "Export Selected" under Network Devices aborts to login screen with more than x selections
CSCwc27765	ISE configuration backup fails due to SYS_EXPORT_SCHEMA_01
CSCwb62192	Scheduled backup failure when ISE indexing engine backup fails
CSCwc65821	ERS API does not allow for use of minus character in "Network Device Group" name.
CSCwa37580	ISE 3.0 NFS share stuck
CSCwb84779	Changing Parent Identity Group name breaks authorization references
CSCwc80574	ISE AD Connector fails during join operation
CSCwc51219	CSV NAD import is rejected if += characters are at the beginning of the RADIUS shared secret
CSCwd13555	ISE abruptly stops consuming passive-id session from a 3rd party Syslog server
CSCwd24304	ISE 3.2 ERS POST /ers/config/networkdevicegroup fails - broken attribute othername/type/ndgtype
CSCwb84440	Sponsor portal breaks after removing endpoint groups.
CSCvx94685	CIAM: rpm 4.11.3 CVE-2021-20271
CSCwc39844	ISE 3.1 Services auto restart fails with an internal error during IP address change in eth 1
CSCwa55866	TACACS responses are not sent sometimes with single connect enabled
CSCwc07082	"The phone number is invalid" when trying to import users from csv file.
CSCwb93156	TrustCertQuickView giving the same info for all trusted certificates
CSCwc60997	SAML flow with loadbalancer fails due to incorrect token handling on ISE
CSCwc49580	ANC COA is sent to the NAS IP address instead of the device IP address
CSCwd32758	Repository name is not updated on export summary page after renaming.
CSCwc30643	My Devices portal does not open after reloading the node unless CRUD is done
CSCwc11613	Certificate signing request shoule not be case sensitive

Open Caveats in Cisco ISE Release 3.0 - Cumulative Patch 7

There are no open caveats in Cisco ISE Release 3.0 Patch 7.

Resolved Caveats in Cisco ISE Release 3.0 - Cumulative Patch 6

Identifier	Headline
CSCwa80359	CIAM: sqlite 3.7.17
CSCwb09045	Cisco ISE PSN nodes crash due to incorrect cryptoLib initialization
CSCwb22662	64-character limit is too small to accommodate external user identities, such as user principal name
CSCwa80547	CIAM: unixodbc 2.3.0
CSCwa37040	backup-logs using public key encryption on the ISE CLI does not allow for caputure of core files
CSCwb64656	When Essential license disabled on ISE GUI, smart licensing portal not reporting license consumtion.
CSCwa61347	ISE-PIC not forwarding live sessions beginning with special characters
CSCwa96229	ISE allowing user to change admin password without validating current password
CSCwb36849	ISE must avoid sending Empty Cisco AV-Pairs in access-accept packets.
CSCwb29140	Threads getting exhuast post moving to latest patches were nss rpm is updated(Only 3.0p5&2.7p7,3.1P1
CSCvz95478	ISE 2.7 EST service not running and CA service stuck in initializing state after installing P5
CSCwa35293	ISE 2.7:Authentication success settings shows success/success url
CSCwb39964	ISE Can login to GUI with disabled shadow admin accounts with external identity source.
CSCwa80553	CIAM: samba 4.8.3
CSCwb53455	RMQ TLS syslogs related to internal docker ip 169.254.2.2 are sent to Audit logs
CSCwa53499	REST ID is fething the groups from Cloud once the connector settings page is opened
CSCwa78479	Cisco Identity Services Engine Assessment of CVE-2021-4034 Polkit
CSCwa55996	new objects doesnt exist in condition studio
CSCwb14106	CIAM: cyrus-sasl 2.1.27
CSCwa16401	Get-By-Id server sequence, returns empty server list after first change made on the sequence via GUI
CSCwa48465	Reports are unusable due to misshandling fields with multiple values
CSCvx54894	Sponsor Portal admin unable to create random guest accounts 60mins/1hr duration or less

Identifier	Headline
CSCwa89443	DNA Center - ISE Integration: ISE shows an old DNAC certificate for pxGrid endpoint
CSCvx58736	3.1:Maxscale: Core generated by /opt/CSCOcpm/prrt/diag/bin/diagRunner start
CSCwa97123	NTP Sync Failure Alarms with more than 2 NTP Servers Configured.
CSCwa40040	Session Directory Write failed, SQLException: String Data right truncation on ISE3.0P4
CSCwa80710	CIAM: jszip 2.5.0
CSCwa06912	High Latency observed for Tacacs+ requests with date time condition in authorization policies
CSCwb33727	ISE 3.1 : Special character in attributes not supported
CSCvz75902	ISE replacing pxgrid cert when generating ISE internal CA
CSCwa57705	IP-SGT mapping does not link with new network access device group.
CSCwa80520	CIAM: libpng 1.6.20
CSCwa80679	CIAM: net-snmp 5.7.2
CSCwb61614	guest users (AD or internal) cant delete/add their own devices on specific node
CSCwa33462	CSV NAD import is rejected due to special symbol @ at the beginning of RADIUS shared secret
CSCvz85074	Fix for CSCvu35802 breaks AD group retrieval with certificate attribute as identity in EAP-Chaining
CSCwb27857	ISE 3.0 P5: Unable to login into GUI of MnT nodes using RSA 2FA in distribusted deployment.
CSCwa94984	ISE API add user operation with long custom attribute string takes 4min using Curl
CSCwa13696	ISE 3.1 Guest Username/Password Policy is not modifiable
CSCwa23207	Multiple runtime crashes seen due to memory allocation inconsistency
CSCwa47190	AD security groups cannot have their OU end with dot character on Posture Policy
CSCwa76896	Duplicated culomn "Failure Reasons" in RADIUS Authentications Report
CSCwc06638	3.0P6 : system summary not getting updated post Patch RollBack and Patch Install
CSCwa95892	ui_time_left variable showing wrong duration
CSCwb19256	Pingnode call causing App server to crash (OOM exception) during CRL validation
CSCwa57955	Posture Firewall remmediation action unchangeable
CSCwa17925	After fixing failed pre-upgrade check, proceed button still not available

Identifier	Headline
CSCwa25731	Last 7 days filter not working in Reports
CSCwb21669	Unable to enter ipv6 address for on-prem SSM server
CSCwa49859	Attribute value dc-opaque causing issues with Live Logs.
CSCwa80484	CIAM: nss 3.44.0
CSCvy91805	Max Sessions not Being Enforced with EAP-FAST-Chaining--ISE
CSCwa83517	Guest posrtal registration page gives "error loading page" when email address contains apostrophe
CSCwb34910	Multiline issues for Guest SMS notification under ISE Portal
CSCwa04454	ISE 3.0 & 3.1: Device Admin License alone should allow access to all TACACS required menu's
CSCwa26210	nextPage field is missing from the json response of API 'GET /ers/config/radiusserversequence'
CSCwa20309	Unknown NAD and Misconfigured Network Device Detected Alarms
CSCwa80501	CIAM: perl 5.16.3
CSCwa18443	Need to handle Posture expiry when 8 octet MAC is present in endpoint on the deployment node
CSCwb09861	CIAM: glib 2.56.4
CSCwa79799	Missing PermSize attribute on sysodbcini file
CSCwa15191	EP stuck in posture unknown Not able to find session in LSD by MAC
CSCwa97357	ISE is not sending $mobilenumber$ value in the SMTP API body
CSCwa13877	ISE Smart Licensing Authorization Renewal Failure: Details=Invalid response from licensing cloud
CSCwa46758	Deleted Root Network Device groups are still referenced in the Network Devices exported CSV Report
CSCvz43123	CIAM: jspdf 2.3.0
CSCwb67934	CIAM: openjdk - multiple versions
CSCwa90930	Need hard Q cap on RMQ in 3.x
CSCvz24558	Spring Hibernate TPS upgrade (hibernate 5.5.2, Spring 5.3.8)
CSCwa75348	ODBC Behavior Failover Issues
CSCwb04898	Unable to restore CFG backup from linux SFTP repository if the file owned by a group name w/ space

Identifier	Headline
CSCvz94133	Config backup fails due to "EDF_DB_LOG"
CSCvs55875	Existing routes are not installed in routing table after MTU change
CSCwa47566	ISE Conditions Studio - Identity Groups Drop-down limited to 1000
CSCwa20152	CoA was not initiated on ISE for switches for which matrix wasnâ€™t changed, hence Policy sync failed
CSCwb05532	Location of "Location" and "Device Type" exchanging every time clicking Network Devices &gt; Add
CSCwa91335	Default domain configuration in Passive-Syslog provider does not work in ISE 3.1
CSCwb40349	ISE 3.X: Invalid Characters in External RADIUS Token shared Secret.
CSCwb01854	upgrade External Radius server List not showing up after migration to 3.0
CSCwa43187	ISE Queue Link Error: Message=From Node1 To Node2; Cause=Timeout in NAT'ed deployment
CSCwa59924	ISE 3.1 Patch 1 : SSH : FIPS : error: Xkey_sign: invalid digest
CSCvw90778	T+ ports (49) are still open if disable Device admin process under deployment page
CSCwb03231	application server stuck initializing after installing p5 or p6 due to missing table
CSCwa52110	SNMP config set on the N/w device, a delay of 20seconds is introduced while processing SNMP record
CSCwb41741	ISE - Invalid character error in Admin Groups
CSCwb32466	ISE 3.1: Unable to delete endpoint identity group created via REST API when setting no description.
CSCwa59237	Deployment-RegistrationPoller causing performance issues on PAN node with 200+ internal certificates
CSCvw74930	CIAM: kafka CVE-2019-12399
CSCwb40942	From address to send email is invalid if it does not end with .com or .net
CSCwa32814	ISE Configured with 15 Collection Filters Hides the 15th Filter
CSCwa60873	Optimize bouncy-castle class to improve performance on PAN
CSCwb11147	Improvement to logs needed with Conflict handling SGT-IP mapping w/VN
CSCwa77161	PLR returned upon 3.0P5 -&gt; 3.0P3
CSCwa27766	Context Visibility broken after restore of backup ISE 3.0 P4
CSCwb23028	Inaccurate dictionary word evaluation for passwords

Identifier	Headline
CSCwb03479	hotpatch.log needs to be included in support-bundle
CSCwa16291	Guest Portal's Button's text element is causing words to be repeated for Apple VoiceOver
CSCwb01843	DST/TZ update should happen automatically
CSCvz92898	SCM js files browser download during admin login
CSCwb29357	ISE 3.0 AD User SamAccountName parameter is null for user session
CSCwa82247	ISE Queue Link Error : Cause=Timeout due to 169.254.2.0/25 in ISE iptables
CSCwb75964	ISE 3.0: Unable to edit PAN Auto Failover alarms
CSCwb07504	Sorting internal users based on User Identity Groups doesn't work in Identity Mangement-&gt;Identities
CSCvw85860	ISE pxGrid Exceptions should have ERROR log level instead of DEBUG
CSCwa56771	ISE 3.0p2- Monitor All setting displays incorrectly with multiple matrices and different views
CSCwa60903	ISE is adding extra 6 hours to nextUpdate date for CRL
CSCwa41166	Unsafe Characters in T+ Commands Stored in Hex Numeric Character References
CSCwa47221	AD security groups cannot have their OU end with dot character on Client Provisioning Policy
CSCvk25808	Unable to edit or remove Scheduled Reports if Admin who created them is no longer available
CSCwa56934	Inconsistent sorting on ERS API(s) for endpoint group
CSCwa80477	CIAM: dom4j 1.6.1
CSCwb40131	Getting 400 Bad Request while enabling the Internal User with external password type using Rest API.
CSCwa11633	ISE 3.0 : APIC Integration : Failed to create secGroup
CSCwb32492	Application server restart on all nodes after changing the Primary PAN Admin certificate
CSCvz88327	CA initializing on PAN, Root CA regeneration fails with "no message defined" error
CSCwa59621	Inconsistent sorting on ERS API(s) for identity group

Open Caveats in Cisco ISE Release 3.0 - Cumulative Patch 6

Identifier	Headline
CSCwc25830	Formatting of the Open New Case window is not correctly displayed.

New Features in Cisco ISE, Release 3.0 - Cumulative Patch 5

Microsoft Intune Integration Changes Due to Microsoft Graph Updates

Microsoft is deprecating Azure Active Directory (Azure AD) Graph and will not support Azure AD Graph-enabled integrations after June 30, 2022. You must migrate any integrations that use Azure AD Graph to Microsoft Graph. Cisco ISE typically uses the Azure AD Graph for integration with the endpoint management solution Microsoft Intune.

For more information on the migration from Azure AD Graph to Microsoft Graph, see the following resources:

- Migrate Azure AD Graph apps to Microsoft Graph
- Azure AD Graph to Microsoft Graph migration FAQ
- Update your applications to use Microsoft Authentication Library and Microsoft Graph API

Cisco ISE Release 3.0 Patch 5 supports Microsoft Intune integrations that use Microsoft Graph. To avoid any disruption in the integration between Cisco ISE and Microsoft Intune, update your Cisco ISE to Cisco ISE Release 3.0 Patch 5. Then, update your Cisco ISE integration in Microsoft Azure to use Microsoft Graph instead of Azure AD Graph, before June 30, 2022. In Cisco ISE, you must update your Microsoft Intune integrations to update the **Auto Discovery URL** field—Replace **https://graph.windows.net<*Directory (tenant) ID*>** with **https://graph.microsoft.com**.

See Connect Microsoft Intune to Cisco ISE as a Mobile Device Management Server for more information on the configuration steps.

Resolved Caveats in Cisco ISE Release 3.0 - Cumulative Patch 5

Caveat ID Number	Description
CSCvo39514	MnT log processor is not running because collector log permission is denied
CSCvu58986	Replace "black list/blacklist" and "white list/whitelist" with appropriate terms in all ISE Syslogs
CSCvz77905	Cisco Identity Services Engine RADIUS Service Denial of Service Vulnerability
CSCvu94544	ISE 3.0 BH : TACACS live logs do not give an option to select Network Device IP
CSCvv43120	ISE-2.x: Intune MDM Alarm for connectivity || 401 Unauthorized
CSCvv96532	DOC: unknown maximum time difference between ISE system time and OCSP response. Update of OCSP response
CSCvw09460	Updated fields list for PUT on /erc/config/authorizationprofile/{id} is usually empty
CSCvw65181	CIAM found poi vulnerable

Caveat ID Number	Description
CSCvx43866	3.0P2:Accounting Report Export is taking more time to complete
CSCvx48255	CIAM: screen 4.1.0 CVE-2021-26937
CSCvx59893	Inconsistency between ISE syslog level and message level
CSCvx98746	DOC: Agentless posture documentation requirements for Windows is incorrect
CSCvy36887	TCP port 19444 is open only on ISE 3.0
CSCvy45345	EAP-chaining authorization fails as machine authentication flag is incorrectly set to "True"
CSCvy53842	Certificate Validation Syslog Message Sent During Specific Certificate Audits--ISE
CSCvy56983	DOC: ISE: SAML certificate shouldn't be removed from ISE deployment
CSCvy66537	ISE Document Bug: Agentless and Temporal Posture Limitations : explanation incomplete
CSCvy71261	CIAM: nettle 3.4.1
CSCvy72028	ISE 2.7 Patch 4 pxGrid Services -> All Clients ends up with java.lang.NullPointerException
CSCvy75191	Cisco Identity Services Engine XML External Entity Injection Vulnerability
CSCvy82023	Incorrect Posture Compound Condition Hotfixes
CSCvy84989	Enabling cookies for POST /ers/config/internaluser/ causes Identity Group(s) does not exist error
CSCvy89317	ISE: DST Root CA X3 Certificate Authority - Expires by 30 Sep 2021 (within 90 days)
CSCvy92040	ISE restore popup menu displays wrong text
CSCvy96761	Session cache needs to be updated during EAP chaining flow to handle relavent identities
CSCvz00034	Changing log level of log "this update field is earlier than currunet time more than week"
CSCvz00617	PnSLongevity: 3.0P3 observing replication failed error in Longevity testbed
CSCvz00706	"interesting groups" are returned as a SINGLE STRING with an embedded new line
CSCvz07191	ISE GUI stuck at loading if AD group does not exist when using certificate based authorization for GUI access
CSCvz17020	ISE GUI shows all the licenses as Out of Compliance - Smart Licensing
CSCvz18044	VN's are not replicating from Author to Reader

Caveat ID Number	Description
CSCvz21417	Upgrade ISE 3.0 and earlier patches with CiscoSSL 1.0.2za
CSCvz22331	Authentication is not blocked in policy set with TimeAndDate condition for a specific minute of the day
CSCvz27791	ISE: Application server stuck initializing after backup restore due to MDM configuration
CSCvz28133	User unable to generate support bundle
CSCvz35550	ISE Health Check during MDM Validation creates false alarm
CSCvz36192	GET for dacls using /ers/config/downloadableacl does not add the nextPage or previousPage of exist
CSCvz37241	Queue Link Error:WARN:{socket_closed_unexpectedly;'connection.start'}
CSCvz37623	NTP (' - ') source state description missing in ISE CLI
CSCvz40708	ISE reaching out to NTP servers is not defined in configuration
CSCvz43183	Sponsor Permissions are not passed to Guest REST API for "By Name" calls.
CSCvz44488	ISE 3.0 Agentless posture doesn’t use domain authenitcation if same local user exists
CSCvz44655	ISE manage account selection issue
CSCvz46560	ISE using jquery v1.10.2 is vulnerable
CSCvz46893	ISE Documentation Update : Microsoft Intune Integration : Permissions
CSCvz46933	CIAM: jsoup 1.10.3
CSCvz48491	ISE CTS TLSv1.2 Support
CSCvz49871	ISE GUI : net::ERR_ABORTED 404 : /admin/ng/nls/fr-fr/
CSCvz50255	CIAM: bind 9.11.20
CSCvz55258	Cisco:cisco-av-pair AuthZ conditions stopped working
CSCvz55293	The secondary PAN ISE node causes services to restart on Primary PAN node, mismatch on documentation
CSCvz56358	ISE 3.0 checks only the first SAN entry
CSCvz60870	High Active Directory latency during high TPS causes HOL Blocking on ADRT
CSCvz63405	ISE client pxgrid certificate is not delivered to DNAC
CSCvz63643	ISE 2.7: EndpointPersister thread getting stopped
CSCvz65057	"Add" button under Context Visibility>Endpoints, "Guest" tab gives nullpoint error
CSCvz65576	Full upgrade won't work with patch when CLI repo or disk repo is used

Caveat ID Number	Description
CSCvz66279	Radius reports older than 7 days are empty (regression of CSCvw78289)
CSCvz66577	SMS Javascript customization is not working for SMS Email gateway
CSCvz67479	Local Log Settings tooltip on all fields shows irrelevant and unuseful 'Trust Certificates'
CSCvz68091	Configuration changes to Guest types is not updated in audit reports
CSCvz71284	SNMPv3 COA request is not issued by ISE 2.7
CSCvz71872	CIAM: nss - multiple versions
CSCvz72208	ISE 3.1 : Authentication tab shows blank result in Context Visivility
CSCvz72225	Adding FQDN in discovery host, Discovery host: invalid IP address or host name
CSCvz73445	Agentless Posture not passing AntiMalware check
CSCvz74457	ERS API does't allow for use of dot character in "Network Device Group" name or create / update
CSCvz77482	ISE 3.0 Can't deselect the 'location' settings as part of the guest self registration portal
CSCvz77836	ISE 3.0 evaluation expiry error on registered ISE
CSCvz80829	Version pre-check fails for 3.2 full upgrade.
CSCvz83204	ISE unable to fetch the URL attribute value from improper index during posture flow
CSCvz83753	Empty User Custom Attribute included in Authorization Advanced Attributes Settings results in incorrect AVP
CSCvz85117	ISE Health Check I/O bandwidth performance check creates false Alarm
CSCvz86020	Live log/session is not showing the latest data due to "too many files open" error
CSCvz87476	Unsupported message code 91104 and 91105 Alarms
CSCvz88188	TACACS authorization policy querying for username fails because username from session cache is null
CSCvz90468	Internal users using External Password Store are getting disabled if we create users using API flow
CSCvz91603	Unable to fetch the attributes from ODBC after upgrading ISE to 3.0 patch 3
CSCvz93230	Guest portal does not load if hosted is on a different interface from Gig0
CSCvz95326	Unable to add more than one ACI IP address / hostname when trying to enable ACI integration in ISE
CSCwa00729	All NADs got deleted due to one particular NAD deletion
CSCwa03126	ISE CPP is not loading correctly for some languages

Caveat ID Number	Description
CSCwa05404	Stale sessions observed for TACACS could not find selected service error
CSCwa07580	Could not create Identity User if username includes $
CSCwa08484	Missing IPv4 mappings if sessions have both IPv4 and IPv6 addresses
CSCwa17718	Session service unavailable for PxGrid Session Directory with dedicated MNT
CSCwa19573	Catalina.out file is huge because of SSL audit events
CSCwa23393	ISE 2.7 p 4,5,6 reports error "There is an overlapping IP Address in your device"
CSCwa32312	RCM and MDM flows are getting failed because session cache is not populated
CSCwa35288	KONG is not able to reach postgres which is impacting the ISE GUI access
CSCwa47133	ISE Evaluation log4j CVE-2021-44228

Open Caveats in Cisco ISE Release 3.0 - Cumulative Patch 5

Caveat ID Number	Description
CSCwa36485	High latency observed for UDN pxgrid assign Device API
CSCwa77161	PLR returned upon 3.0P5 -> 3.0P3

Resolved Caveats in Cisco ISE Release 3.0 - Cumulative Patch 4

Caveat ID Number	Description
CSCvs66551	Multiple Vulnerabilities in Apache log4j.
CSCvu56753	CIAM: Multiple vulnerabilities in openjdk.
CSCvv04957	GRUB2 Arbitrary Code Execution Vulnerability.
CSCvv07101	Memory Leak: PKCS11 key store creates memory leak when endpoints are in Cisco ISE.
CSCvw78019	Cisco ISE: NTP out of sync after upgrade to Cisco ISE Release 2.7.
CSCvy07088	Cisco ISE 3.0 Agentless Posture doesn't install CA certificate chain in endpoint Trusted Store.
CSCvy11865	Cisco Identity Services Engine Cross-Site Scripting Vulnerability.
CSCvy14905	CTS-SXP-CONN : ph_tcp_close from device to Cisco ISE SXP connection - Hawkeye.
CSCvy42885	Cisco ISE Application server crashes or restarts due to cancellation of configuration backup.

Caveat ID Number	Description
CSCvy43246	[CFD] User unable to create a guest SSID during Portal Creation step - Cisco ISE is busy error.
CSCvy48766	Cisco ISE installation fails with database priming failed error when all-numbers subdomain is used.
CSCvy62875	Cisco ISE 2.7 p2 : [400] Bad Request with SAML SSO OKTA on Apple devices.
CSCvy71313	CIAM: cpio 2.12.
CSCvi53134	Account used for Cisco ISE AD join may be locked after passive-id service is enabled.
CSCvn27270	Cisco ISE: cannot create network device group with name Location or Device Type.
CSCvp88242	[400] Bad Request error when refreshing the Mydevice portal.
CSCvr76539	Changes to Network Device Groups not reflected in Change Audit Logs.
CSCvt94587	Cisco ISE Root CA cannot be regenerated due to Plus License is out of compliance error.
CSCvu58927	Update "blacklist portal" to "blocked list portal" everywhere in the ISE UI + code.
CSCvv09910	SYSAUX tablespace full despite fix for CSCvr96003.
CSCvw09827	High CPU on PSN node - extension of CSCvt34876.
CSCvw90586	Unable to change network Device group Name and Description at the same time.
CSCvx01272	Generate bulk certificates do not include Cisco ISE self-signed certificate.
CSCvx23375	Cisco ISE authorization profiles option gets truncated during editing or saving (Chrome only).
CSCvx43866	3.0P2:Accounting Report Export takes long time to complete.
CSCvx47691	Session Directory topic does not update user SGT attribute after a dynamic authorization.
CSCvx60818	ERS Self-Registration portal update does not delete fields as expected in PSN.
CSCvy90691	In case of a duplicated Radius Vendor ID, any network device change can cause PSN to crash.
CSCvy94427	Posture lease breaks for EAP chianing from Cisco ISE Release 2.7.
CSCvz00258	Not clearing SessionCache for TACACS AuthZ failures results in high heap usage and auth latency.
CSCvz34849	DELETE /ers/config/networkdevicegroup/{id} not working; CRUD exception.
CSCvx91688	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability.
CSCvx96190	Cisco ISE reports: Top Authorization does not show filter in scheduled reports.

Caveat ID Number	Description
CSCvx97501	Cisco ISE Release 3.0 ROPC authentication is failing with non Base64 characters in the password.
CSCvx99151	Cisco ISE internal ERS user attepting to authenticate occasionly via external ID store causes REST delays.
CSCvx99675	Cisco ISE 2.7P3 sends packet to other node with src add :169.254.2.2 if backup interface is configured.
CSCvy04443	MNT REST API for ReAuth fails when used in a distributed deployment (separate MnT).
CSCvy04665	Cisco ISE Release 2.6 and Release 2.7 TACACS Reports Advance Filters do not work when matching full numeric ID entries.
CSCvy05954	All SXP Mapping not displaying IPv6 mappings learned via Session.
CSCvy10026	Cisco ISE Release 3.0 Agentless Posture fails if Cisco ISE admin certificate CN is not equal to FQDN.
CSCvy11617	Cisco ISE Release 3.0 Agentless posture breaks if Windows username includes space.
CSCvy16894	Authorization profile throws an error if we use some symbols.
CSCvy18560	RADIUS Accounting Details Report does not display Accounting Details.
CSCvy20277	Special characters previously allowed in the Descriptions field for few objects cannot be used.
CSCvy24370	Cisco ISE not accepting more than 6 attributes to be modified in the RADIUS sequence attributes.
CSCvy25533	Cisco ISE: "/opt/CSCOcpm/config/cpmenv.sh:line 396:<ipv6>:command not found" error during CLI backup.
CSCvy25550	Cisco ISE does not accept name of custom attribute for Framed-IPv6-Address in the authZ profile.
CSCvy30119	LDAP groups dissapear from Sponsor groups when you make other changes to the options and save them.
CSCvy30295	Cisco ISE does not send certificate chain on admin portal.
CSCvy34977	Application Server stuck in initializing state due to certificate template curve type P-192.
CSCvy36868	Cisco ISE Release 2.3 and later releases do not support "cariage return" <cr> character in command-set.
CSCvy36887	TCP port 19444 is open on Cisco ISE Release 3.x.
CSCvy38459	Cisco ISE Release 2.7 P3 GUI doesn't show complete device admin Authz policies.

Caveat ID Number	Description
CSCvy40845	Updating single custom attribute through ERS request causes deletion of another.
CSCvy41066	TACACS custom AV pair as condition in policies is not working.
CSCvy45015	Cisco ISE Guest Self-Registration Error for duplicate user when "Use Phone number as username" is enabled.
CSCvy46504	Intermittent error on Cisco DNA Center while trying to deploy a policy from Cisco DNA Center.
CSCvy51073	Cisco ISE authorization profile ERS update ignores accessType attribute changes.
CSCvy51210	Cisco ISE Release 2.7 should display an error when attempting to delete IP default label of NAD on GUI.
CSCvy58771	While editing a NAD, the wrong device profile is being mapped.
CSCvy60752	Setup wizard password supports hyphen, but after configuration reset through the CLI the wizard no longers supports hyphen.
CSCvy60865	Cisco ISE Release 2.4 CoA failure upon endpoint change to a new switch-port and EP IdGroup Remove/Remove-All EP.
CSCvy61564	Cisco ISE Release 2.7 Patch 3 ERS call does not accept 3 characters RADIUS shared secret.
CSCvy61894	UI: Generate key pair, accepts space but then cannot export key.
CSCvy63778	REST API for CoA works with any server IP.
CSCvy65786	PassiveID: Configuring WMI with an AD account password that contains a % result in an error.
CSCvy71690	Customer fields in guest portal contains & - $ #.
CSCvy74919	Cisco ISE internal users are not disabled after they hit the inactivity timer.
CSCvy76262	Cisco ISE DACL syntax validator does not comply with ASA's code requirements.
CSCvy76328	IPv6 changes the Subnet to /128 when using the duplicate option in the Network Device tab.
CSCvy76617	Cisco ISE: Need the Select ALL check box device with or without filter in the NAD page.
CSCvy81435	Cisco ISE Guest SAML authentication fails with "Access rights validated" HTML page.
CSCvy82114	Wrong display as Unicode of Chinese in First/Last name under Network Access Users.
CSCvy89317	ISE: DST Root CA X3 Certificate Authority - Expires by 30 Sep 2021 (within 90 days)

Caveat ID Number	Description
CSCvy92536	Cisco ISE Release 3.0 Device Admin License should only allow access to the Administration > System > Logging menu.
CSCvy93847	Possible to choose secondary PAN without Policy persona in NAD, and to send configuration changes to device CoA.
CSCvy94511	TACACS report showing duplicate entries due to EPOCH time being null.
CSCvy94553	TACACS authentication report shows duplicate entries.
CSCvy94818	Endpoints incorreclty profiled as "cisco-router" due to NMAP performing aggressive guesses.
CSCvy99582	When upgrading from Cisco ISE Release 2.4 patch 13 to Cisco ISE Release 2.7, if an external RADIUS server is configured, the upgrade process fails.
CSCvz00659	Special characters in Banner blocking SFTP repository.
CSCvz01485	Cisco ISE Release 2.7 patch 4 unable to upload .json file for Umbrella security profile.
CSCvz05704	Platform check fails for Cisco ISE that has disk size more than 1 TB.
CSCvz05966	Cisco ISE Release 2.6 Patch 9: default permissions cannot go back to default group Internal after adding a new group.
CSCvz07823	Cisco ISE Release 2.7: Failed to add endpoint to group.
CSCvz18627	PEAP session timeout value restricted to maximum value 604800.
CSCvv55602	Policy engine - enhancements.
CSCvz33839	Menu access customization is not working.
CSCvz49086	Cisco ISE Release 3.0 TimesTen connection closes when an SQLException is encountered.
CSCvy32461	Sponsor user cannot edit data when phone or email fields are filled.
CSCvv63395	Cisco ISE Release 3.0 cannot locate REST ID store after services restart.
CSCvy88861	Policy change doesn’t get pushed to the network device after Cisco ISE failover.
CSCvs95495	Reauth issue - Aruba - third-party device.
CSCvz08813	Not able to scroll to different pages in Issued Certficates page.
CSCvy29454	Reset Password mobile number validation does not satisfy e.164 format.

Open Caveats in Cisco ISE Release 3.0 - Cumulative Patch 4

There are no open caveats in Cisco ISE Release 3.0 Patch 4.

New Features in Cisco ISE, Release 3.0 - Cumulative Patch 3

Full Upgrade and Split Upgrade Options Added to Cisco ISE GUI

You can select one of the following options in the **Administration > System > Upgrade> Upgrade Selection** window to upgrade your Cisco ISE deployment:

- **Full Upgrade**: Full upgrade is a multi-step process that enables a complete upgrade of your Cisco ISE deployment sequentially. This method will upgrade all nodes in parallel and in lesser time compared to the split upgrade process. The application services will be down during this upgrade process because all nodes are upgraded parallelly.

Note The Full Upgrade method is supported for Cisco ISE 3.1 and above. For more information about the Full Upgrade method, see Cisco Identity Services Engine Upgrade Journey, Release 3.1.

- **Split Upgrade**: Split upgrade is a multi-step process that enables the upgrade of your Cisco ISE deployment while allowing services to remain available during the upgrade process. This upgrade method allows you to choose the Cisco ISE nodes to be upgraded on your deployment.

Resolved Caveats in Cisco ISE Release 3.0 - Cumulative Patch 3

Caveat ID Number	Description
CSCuo73496	ISE RADIUS session-timeout value restricted to max 65535
CSCvh04231	Guest remember me radius accounting and access accept not sending guest username
CSCvi59005	Unable to see complete list of AD groups when using Scrollbar.
CSCvn25548	Receiving Alarms - Account is suspended temporarily due to excessive failed auth
CSCvn31249	GNU gettext default_add_message Double-Free Vulnerability
CSCvo04728	MIT Kerberos 5 KDC krbtgt Ticket S4U2Self Request Denial of Service ...
CSCvo56767	error when attempting to change ISE-PIC GUI admin user settings
CSCvq26124	ISC BIND managed-keys Trust Anchor Denial of Service Vulnerability
CSCvq58506	Show running-config fails to complete
CSCvr47716	Info-ZIP UnZip File Overlapping Denial of Service Vulnerability CVSS v3.0 Base 7.5
CSCvr55906	cURL and libcurl tftp_receive_packet() Function Heap Buffer Overflow Vulner CVSS v3.1 Base: 9.8
CSCvr77653	cURL and libcurl tftp_receive_packet() Function Heap Buffer Overflow ...
CSCvr77655	GNU patch pch_write_line Function Denial of Service Vulnerability

Caveat ID Number	Description
CSCvr80914	SSSD Group Policy Objects Implementation Improper Access Control Vulner
CSCvr80921	ISC BIND Dynamically Loadable Zones Unauthorized Access Vulnerability
CSCvr81463	libssh2 packet.c Integer Overflow Vulnerability CVSS v3.1 Base: 8.1
CSCvr97388	Samba Filename Path Separators Unauthorized Access Vulnerability
CSCvs29611	ISE 2.4 p5 crashes continuously around midnight, generating core files.
CSCvs39800	gllibc LD_PREFER_MAP_32BIT_EXEC Environment Variable ASLR Bypass Vulner
CSCvs45350	Live Log and NADs show Anonymous when User Fail Machine Success
CSCvs76914	libxml2 xmlParseBalancedChunkMemoryRecover Memory Leak Vulnerability
CSCvs85273	Multiple Vulnerabilities in libcurl
CSCvs91984	Systemd button_open Memory Leak Vulnerability
CSCvt30558	Multiple Vulnerabilities in python
CSCvt85370	Posture Condition failed Check vc_visInst_v4_CiscoAnyConnectSecureMobility Client_4_x is not found
CSCvu04874	suspected memory leak in io.netty.buffer.PoolChunk
CSCvu13139	In filter.c in slapd in OpenLDAP before 2.4.50, LDAP search filters wit
CSCvu14215	Sponsor group membership being removed when adding/removing AD group
CSCvu22058	ISE with DUO as External Radius Proxy drops access-reject
CSCvu22259	CIAM: batik 1.7
CSCvu24402	CIAM: cups 1.6.3
CSCvu30439	CIAM: ksh
CSCvu31098	CIAM: libssh
CSCvu37728	CIAM: perl 5.14.1
CSCvu37765	CIAM: procps 3.3.10
CSCvu37775	CIAM: python (version 2.7.5, 2.7.14 & 3.7.1)
CSCvu38141	CIAM: vim 7.4.160
CSCvu58927	Update "blacklist portal" to "blocked list portal" everywhere in the ISE UI + code
CSCvu62938	Posture fails when primary PSN/PAN are unreachable
CSCvu72744	Replace "blacklist" with "blocked list" across all authentication and authorization rules/profiles

Caveat ID Number	Description
CSCvu81838	CIAM: d-bus 1.10.24
CSCvu84184	certificate chain is not sent on the portal
CSCvu84773	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvu91859	CIAM: libjpeg & libjpeg-turbo
CSCvv10683	Session Cache for dropped session not getting cleared; causing High CPU on the PSN's
CSCvv14390	Max Sessions Limit is not working for Users and Groups
CSCvv18317	Invalid objects in Database
CSCvv19065	ISE customer could not see the guest identity in the DNAC Assurance page
CSCvv27690	ISE 2.4 While renewing ISE cert for HTTPS,EAP,DTLS,PORTAL, only PORTAL and Admin roles gets applied.
CSCvv29737	DNA ACA SG Sync Fails with JDBCException:could not prepare statement
CSCvv30161	Live session details report show incorrect Authorization profile and policy for VPN Posture scenario
CSCvv30226	Livelog sessions show incomplete Authorization policy for VPN Posture scenario
CSCvv43383	NFS Repository is not working from GUI
CSCvv44401	Generate self-signed certificates and CSR default params doesn't correspond to pre-installed cert
CSCvv45063	Internal CA Certificate Not Getting Deleted When Node Is Removed From Deployment
CSCvv45340	Error storing the running-config lead to loss of startup config
CSCvv46958	TrustSec enabled NADs not showing in trustSec Matrices when NDG column exceeds 255 characters.
CSCvv47849	[CFD] Mapped SGT entry cleared from AuthZ Rules on ISE if SG name is modified in Cisco DNA Center
CSCvv50028	Heap Dump generation fails post reset-config of ISE node
CSCvv52637	ISE Hotspot guest portal broken flow
CSCvv60353	Authentication summary report gets stuck if the total records are more than 5M
CSCvv60686	ISE SXP should have a mechanism to clear stale mappings learned from Session
CSCvv60923	ISE adding the ability to use a forward slash in the IP data type of internal user custom attribute
CSCvv61732	Unable to Create unique community string for different SNMP servers

Caveat ID Number	Description
CSCvv62382	proxy bypass settings does not allow upper characters
CSCvv63548	Memory Leak: PSN rmi GC collection not working properly causing memory leak in passive id flow
CSCvv64012	ISE 3.0 REST ID Process failed action used too often
CSCvv66302	Domain doesnt get assigned to sxp peer
CSCvv67091	Cisco Identity Services Engine Untrusted File Upload Vulnerability
CSCvv68293	ISE not consuming plus license when using local or global exceptions
CSCvv72418	ISE 3.0 REST ID log file not included in support bundle
CSCvv77007	ISE constantly requesting internal "Super Admin" users against to external RADIUS token server.
CSCvv77928	Bulk certificate generation failed with 'An unexpected error occurred' message after RMA'd pPAN
CSCvv79940	ISE generating CSR with hostname-x in SAN gives an error
CSCvv80297	Need DigitCert Global Root G2 in CTL for ROPC
CSCvv80307	REST error in ropc.log should include the endpoint URL
CSCvv82625	Policy set not saving if any authz rule has only security group but no authz profile
CSCvv85588	Memory Leak : High Allocation in by CAD_ValidateUser during PassiveID stress
CSCvv90612	WebUI restore not working in IE11
CSCvv91268	ISE 3.0 shows "PxGrid disabled" when you open PxGrid Services menu in new window
CSCvv93442	ISE 2.6p3 Adding Double Slash "//" in File Path with SFTP Servers
CSCvv94791	[CFD] ACA Sync broken - "Error occurs during migration: Waiting for Sync Runtime timed out"
CSCvv95150	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability
CSCvw00375	Unable to load Context Visibility page for custom view in ISE 2.7p2
CSCvw01225	ISE Config Restore fails at 40% with error "DB Restore using IMPDP failed"
CSCvw01818	Replace Keyword kong in ISE Admin Web UI and CLI to API GW
CSCvw01829	ISE admin/portal Login with Chrome 85/86 could show error Oops. Something went wrong.
CSCvw02887	Memory leak after adding AD Groups for passiv-id flow

Caveat ID Number	Description
CSCvw06722	Sponsor is unable to display the list of created guest users when accessing portal with his User ID.
CSCvw08330	Posture does not work with dynamic redirection on 3rd party NADs
CSCvw10671	GNU.org bash rbash BASH_CMDS Modification Privilege Escalation Vulnerab
CSCvw16237	Scheduled OPS backups not being triggered after PMNT reload
CSCvw17908	Pushing IP to SGT mapping from ISE to switch doesnt work if default route is tagged
CSCvw19785	Editing external data source posture condition is showing always the wrong AD
CSCvw20021	NAD Location is not updating in Context Visibility ElasticSearch
CSCvw20060	ISE 2.6 p5 Agent marks DC as down if agent service comes up before windows network interface
CSCvw20636	Authorization Profiles showing "No data available" after NAD profile deleted
CSCvw22228	pxGrid ANC applyEndpointPolicy does not handle all MAC address formats correctly
CSCvw24227	Purging not purging endpoints due to an exception
CSCvw24268	Cisco Identity Services Engine Untrusted File Upload Vulnerability
CSCvw25615	ISE TACACS logging timestamp shows future date
CSCvw26415	ISE 3.0 not importing certificates missing CN and SAN into Trusted Certificate Store
CSCvw28084	DOC: ISE: Need to include OVA Template reservations table in ISE 2.7 Installation guide
CSCvw28441	NADs shared secrets are visible in the logs while using APIs
CSCvw29490	Internal User custom attributes are not sent in CoA-Push
CSCvw31269	SAML groups do not work if they are applied in the Sponsor Portal Groups
CSCvw33115	ISE MNT Live Session status is not changing to Postured in VPN use case
CSCvw36190	Scheduled operational backup stuck at "Backup is in progress..."
CSCvw36486	GUI Not Accessible After Applying IP Access Restrictions
CSCvw36743	ISE Service Account Locked and WMI not established due to special characters in password
CSCvw37844	ANC CoA not working as ISE uses hostname for internal calls
CSCvw38530	SBET: Exception w.r.t Repository in ise-psc.log while loading Backup & Restore page.
CSCvw44120	Functional:Guest portal creation failure with ISE 3.0

Caveat ID Number	Description
CSCvw46096	ISE 3.0 Syslog provider cannot apply configuration
CSCvw47011	same Idenity Group creating multiple times and showing in Ui using ers rest api sending
CSCvw48396	Cisco ADE-OS Local File Inclusion Vulnerability
CSCvw48403	SNMPv3 | ISE is not processing gathered SNMP information for endpoint : String index out of range: 8
CSCvw48697	API IP SGT mapping not returning result for [No Devices]
CSCvw49938	no TACACS Command Accounting Report for third party device with a space before TACACS command
CSCvw50381	CoA-disconnect is not issued by ISE for Aruba WLC once grace access expires
CSCvw50829	AD security groups cannot have their OU end with dot character on RBAC policies
CSCvw51801	ISE Live Session Postured session is moving to Started upon Interim Update
CSCvw53187	ACI endpoint livelog stuck on 'loading' without showing any information
CSCvw53412	SB should collect Hibernate.log
CSCvw54878	ISE does not display Full Authorization Rules if it has 50 rules or more in Japanese GUI
CSCvw55793	ISE fails to send CoA from PSN's with "Identifier Allocation Failed" error
CSCvw58538	GNOME GLib file_copy_fallback Function Improper Permission Vulnerability
CSCvw58824	XStream before version 1.4.15 multiple vulnerabilities
CSCvw59312	Heap buffer overflow in Freetype CVE-2020-15999, CVE-2018-6942
CSCvw59314	Moment Module Date String Regular Expression Denial of Service Vulnerab
CSCvw59855	In js/parts/SvgRenderer.js in Highcharts JS before 6.1.0, the use of ...
CSCvw59920	Multiple Vulnerabilities in c3p0
CSCvw60197	Multiple Vulnerabilities in glibc
CSCvw61589	ISE Policy Evaluation : RADIUS requests dropped after deleting policy sets
CSCvw61786	Restore Process All Processes need to be stopped before dropping schema Objects
CSCvw63264	ISE 3.0 policy condition studio GUI bug
CSCvw64840	CIAM found mariadb vulnerable
CSCvw65262	CIAM: go 1.12 CVE-2019-9634 and others
CSCvw66468	Doc: lack of documentation for ISE 3.0 on syslog categories

Caveat ID Number	Description
CSCvw66483	RADIUS server sequence gets corrupted after selected external servers list was changed
CSCvw66601	CIAM found jspdf vulnerable
CSCvw68480	ISE incorrect number for the TOTAL field
CSCvw68512	Guest user is created with incorrect lifetime
CSCvw69977	"All SXP Mapping" table contains terminated sessions on ISE
CSCvw73928	NTP sync failure alarms not relevant needs change
CSCvw74703	CIAM: libssh2 CVE-2019-17498 and others
CSCvw74712	CIAM: libcurl CVE-2016-8622 and others
CSCvw74932	CIAM: json-sanitizer 1.2.0 CVE-2020-13973
CSCvw75397	MNTHA: MNT node name set to NULL when IP access enabled.
CSCvw75563	HotSpot Guest portal displays Error Loading Page when passcode field contains special characters
CSCvw77219	Dot1x authentication failed due to duplicate manager: add=false
CSCvw78269	CWE-20: Improper Input Validation for Create Node Group
CSCvw78289	Auth Passed live logs are not seen when using a profile name with more than 50 characters
CSCvw80520	"Radius Authentication Details" Report takes time when IMS(ISE Messaging Service) is disabled
CSCvw82774	ISE 2.6/2.7 Sorting based on username doesn't work in User Identity Groups
CSCvw82784	ISE 3.0 TACACS+ Endstation Network Conditions scrollbar not working
CSCvw82815	Authz profile CWA option don't work correctly with some network device profiles
CSCvw84127	ISE:Configuration Audit detail does not show which Policy Set was modified
CSCvw85599	TACACS+ N/W cond and PORT N/W condition scrollbar is not working
CSCvw87147	Live session is not showing correct active session
CSCvw87173	ISE 2.4 p13 break AD Authorization lookup for MAB authenticated endpoints
CSCvw87175	MAB authentication via Active Directory passes with AD object disabled
CSCvw88881	DB Clean up hourly cron acquiring DB lock causing deployment registration failure
CSCvw89326	for PKI based SFTP, exporting GUI key for MnT node is only possible when it is promoted to be PAN

Caveat ID Number	Description
CSCvw90961	RBAC rules not enforced in 2.7
CSCvw93570	ISE 2.4 patch 8 Unable to edit,duplicate or delete guest portals.
CSCvw94096	iPod not shown as an option in ISE BYOD portal
CSCvw94603	External MDM server(Microsoft_intune), change in Polling interval not taking effect
CSCvw96371	Static policy and group assignment is lost from EP when updating custom attributes from API
CSCvw97905	Internal user export feature no error with invalid character in password
CSCvx01798	ISE RBAC - adding a network device gives an error "Unable to load NetworkDevices"
CSCvx03047	ACI learned mappings do not show up in xgrid bulk download
CSCvx04512	Admin access with certificate based authentication can be bypassed by going directly to login.jsp
CSCvx09383	ISE 2.7: Context Visibility: all shards failed when sorting endpoint Applications by Running process
CSCvx10186	ISE remains in eval expire state even after registering with smart Licensing
CSCvx14332	CIAM: json-sanitizer 1.2.0 CVE-2021-23899 and others
CSCvx15010	Upgrade flow via CLI from 2.7 P3 to 3.1.236 failed with certificate issue for multinode deployment
CSCvx15427	Health Checks:DNS Resolvability: False failures with ISE FQDN as CNAME (alias)
CSCvx15448	Health Checks:Disk space: insufficient failure info
CSCvx18730	Sudo Privilege Escalation Vulnerability Affecting Cisco Products: January 2021
CSCvx22229	ISE "ipv6 address autoconfig" gets removed when changing IP address of bond interface
CSCvx22594	ISE 3.0 GUI certificate authentication - unsupported certificate purpose
CSCvx23205	Add IdenTrust Commercial Root CA 1 Certificate to ISE truststore
CSCvx27632	Authorization Should Look Up MAC address in Format Configured in ODBC Stored-Procedures Page
CSCvx28402	Support Bundle does not capture ise-jedis.log files on ISE 2.7 and newer version
CSCvx30276	ISE 2.7 : On Re-creating Root CA, Jedis DB connection pool is not re-created
CSCvx32666	NetworkAccess:Authentication Method conditions not matching in Policy Set entry evaluation
CSCvx32764	TC-NAC services not running after unexpected power event

Caveat ID Number	Description
CSCvx34413	Paging from Azure AD is not implemented on ROPC
CSCvx36013	ISE Health Check Platform Support should update directly UI with results
CSCvx37149	SGA value Under-Provisioned for SNS3515 running all personas on same node
CSCvx37297	Error 400 While authenticating to Sponsor portal with Single Sign-on/Kerberos User.
CSCvx37467	Sponsor portal gives "Invalid Input" if the "mobile number" field is unchecked in portal settings
CSCvx41826	Unable to get all tenable adapter repositories with Tenable SC 5.17
CSCvx43566	No login fail log when using external username with Wrong Password
CSCvx43825	Receiving acct stop without NAS-IP address keep session in started state
CSCvx44815	ISE AD runtime should support rewrite a1-a2-a3-a4-a5-a6 to a1a2a3a4a5a6
CSCvx45481	ISE 2.4 CoA failure upon endpoint change to a new switch-port and Endpoint Identity Group change
CSCvx46638	In EAP chaining scenario, posture policy failed to retrieve machine AD group membership.
CSCvx47891	ISE not mapping correctly AMP events for new endpoints
CSCvx48922	Memory leak on TACACS flow
CSCvx49538	CIAM: bind - multiple versions CVE-2020-8625
CSCvx50752	Add IdenTrust Commercial Root CA 1 Certificate for Smart Call Home and Smart Licensing
CSCvx51738	Add IdenTrust Commercial Root CA 1 Certificate for Network Success Diagnostics
CSCvx53205	NIC bonding prevents MAR Cache replication
CSCvx53905	ISE 3.0 Authorization policy conditions are not correctly formatted
CSCvx54213	Network Devices > Default Device page requires PLUS license to allow config
CSCvx57433	TrustSec policy matrix allows limited scrolling in ISE 3.0
CSCvx57545	isedailycron temp1 tracking is causing delay in AWR reports
CSCvx58456	User can select only one option either full upgrade or split upgrade at a given time.
CSCvx58516	Top N Authentication by Network Device details not showing
CSCvx58520	With PLR, Profiler Online Updates error : Failed to get License file data : null
CSCvx61462	ISE Log Collection error "Session directory write failed"

Caveat ID Number	Description
CSCvx61664	ISE not updating the Json file info into the AnyConnect output config file
CSCvx64247	"Invalid phone number format." on Mobile devices using the country-code drop-down
CSCvx69701	PnSLongevity: Deployment went out of sync due to unavailabiltiy of db connections
CSCvx70633	ISE don't accept % in EXEC or Enable Mode password under configiration deployment of Adv Trustsec
CSCvx72642	REST auth Service will be disabled if backup interface configured
CSCvx78643	ISE 2.7 | Emails sent for all system alarms even when there is no email address configured
CSCvx79693	Qualys integration is failing with ISE
CSCvx85391	internal user inactivity timer don't get updated due to login letter case
CSCvx85675	ISE can't handle deletion/addition of SXP-IP mappings propagation due to race condition
CSCvx85807	Smart license of de-registration flow is not working in ISE and ISE-PIC
CSCvx86571	The instruction box should be removed when the login-page message is empty
CSCvx86915	UI Issues on TrustSec page
CSCvx86921	RADIUS Token Identity Source Prompt vs Internal User prompt for TACACS authentication
CSCvx94452	EST service not running on 2/7 p2 and above
CSCvx96915	vulnerabilities fixed in XStream 1.4.16
CSCvx99176	ISE NAD IP definitions using - or * do not perform full IP comparison after patch
CSCvy06719	Manual ActiveSession report is empty
CSCvy08724	Read-only admin should not be allowed to perform Upgrade
CSCvy14259	Remove 3515 from upgrade support
CSCvy14342	High CPU seen on PSN nodes from ISE 2.6P3 onwards due to PIP query evaluation
CSCvy15058	Unable to update domains to be blocked/allowed via API
CSCvy15172	Cisco Identity Services Engine Self Cross-Site Scripting Issue
CSCvy17893	ISE REST API returns duplicate values for IP-SGT mappings.
CSCvy23354	max-height too small in FF 88
CSCvy37878	Access-Reject if any authz rule has only security group but no authz profile

Caveat ID Number	Description
CSCvy38896	AAA requests without Framed-IP value will cause exception in sxp process
CSCvy42972	Full upgrade should throw warning if data size is more than 40GB overall
CSCvy76601	Delete 'All' function in Context Visibility, shows {0} Endpoint(s) on CAPTCHA popup

Open Caveats in Cisco ISE Release 3.0 - Cumulative Patch 3

Caveat ID Number	Description
CSCvz00617	PnSLongevity: 3.0P3 Observing replication failed error in Longevity testbed

New Features in Cisco ISE, Release 3.0 - Cumulative Patch 2

Licensing Methods for Air-Gapped Networks

Cisco ISE Release 3.0 Patch 2 supports the following licensing solution for air-gapped networks:

- **Smart Software Manager (SSM) On-Prem Connection Method**

  SSM On-Prem is a connection method in which you configure an SSM On-Prem server that manages smart licensing in your Cisco ISE-enabled network. With this connection method, Cisco ISE does not require a persistent connection to the Internet.

See Chapter Licensing in the *Cisco ISE Administrator Guide, Release 3.0*.

DNS Cache

The DNS requests for hosts can be cached, thereby reducing the load on the DNS server.

This feature can be enabled in the configuration mode using the following command:

service cache enable hosts ttl *ttl*

To disable this feature, use the **no** form of this command.

no service cache enable hosts ttl *ttl*

Admin can choose the Time to Live (TTL) value, in seconds, for a host in the cache while enabling the cache. There is no default setting for *ttl*. The valid range is from 1 to 2147483647.

Note TTL value is honored for negative responses. The TTL value set in the DNS server is honored for positive responses. If there is no TTL defined on the DNS server, then the TTL configured from the command is honored. Cache can be invalidated by disabling the feature.

Business Outcome: Load on DNS Server is reduced.

Resolved Caveats in Cisco ISE, Release 3.0 - Cumulative Patch 2

Caveat ID Number	Description
CSCvq44063	Incorrect DNS configuration can lead to TACACS or Radius authentication failure
CSCvu94025	ISE should either allow IP only for syslog targets or provide DNS caching
CSCvv02998	BYOD certificate provisioning flow failed in macOS 11
CSCvv27690	While renewing ISE certificate for HTTPS, EAP, DTLS, PORTAL, only PORTAL and Admin roles gets applied
CSCvv30274	Context Visibility shows incorrect Authorization profile and policy for VPN Posture scenario
CSCvv46034	Device admin service is getting disabled while updating TACACS configuration
CSCvv53221	When RADIUS Shared Secret is missing for ISE_EST_Local_Host, ISE application server goes to intializing state
CSCvv54798	Context Visibility CVS exported from CLI not showing IP addresses
CSCvv55663	ISE 2.6/2.7 Repositories get deleted post ISE node reload
CSCvv57628	Suspended Guest User is not automatically removed from Endpoint Group
CSCvv74361	ISE 3.0 Health Check License validation false Alarm
CSCvv91007	Smart Licensing Entitlement Tab gets stuck at "Refreshing" if there is connection failure
CSCvw08602	Not Throwing error for ip overlap case
CSCvw25285	Passive ID is not working stable with multi-connect syslog clients
CSCvw34491	Enabling Essentials licenses only block access to Network Devices tab add/modifiy
CSCvw54878	ISE does not display Full Authorization Rules if it has 50 rules or more in Japanese GUI
CSCvw61537	ISE 3.0 Evaluations Specs to be pulled from cisco.com
CSCvw73529	No option for OnPrem Satellite for Smart licensing and Permanent License Reservation
CSCvw76847	ISE Conditions Library corruption during Pen test
CSCvw78269	CWE-20: Improper Input Validation for Create Node Group
CSCvw81454	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerabilities
CSCvw82927	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerabilities
CSCvw83296	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerabilities
CSCvw83334	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerabilities

Caveat ID Number	Description
CSCvw89818	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerabilities
CSCvx00245	Itune Integration is throwing error while saving but Test Connection works fine
CSCvx00345	Unable to fetch Azure AD groups

Open Caveats in Cisco ISE Release 3.0 - Cumulative Patch 2

Caveat ID Number	Description
CSCvz00617	PnSLongevity: 3.0P3 Observing replication failed error in Longevity testbed

Known Limitations in Cisco ISE 3.0 Patch 2

Special Characters Usage Limitations in Name and Description Fields

- The following special characters cannot be used in the **Description** field for TACACS+ profiles and Device Administration Network conditions: [%\<>*^:"|',=/()$.@;&-!#{}.?]. Supported characters are: alphanumeric, underscore(_), and space.
- The following special characters cannot be used in the **Name** and **Description** fields for Authorization Profiles: %\<>*^:\"|',=. Supported characters for the **Name** and **Description** fields are: alphanumeric, hyphen(-), dot(.), underscore(_), and space.
- The following special characters cannot be used in the **Name** and **Description** fields for Time and Date conditions: [%\#$&()~+*@{}!/?;:',=^`]"<>". Supported characters for the **Name** and **Description** fields are: alphanumeric, hyphen(-), dot(.), underscore(_), and space.

Resolved Caveats in Cisco ISE Release 3.0 - Cumulative Patch 1

Caveat ID Number	Description
CSCvf61114	ERS Update/Create for "Authorization Profile" failing XML Schema Validation
CSCvm47584	Unable to configure grace period for over 1 day because of posture lease
CSCvr22065	Import NAD is failing with unsupported error when shared secret key has special character
CSCvt64739	Application Server takes more time to initialize
CSCvu05121	Guest email fails to send after changing SMTP server
CSCvu58892	Update "master guest report" to "primary guest report" everywhere in the ISE GUI
CSCvu58927	Update "blacklist portal" to "blocked list portal" everywhere in the ISE GUI
CSCvu58954	Update "blacklist identity group" to "blocked list identity group" everywhere in the ISE GUI

Caveat ID Number	Description
CSCvu59038	Update "master/slave" terms to "primary/subordinate" in "show interface" command
CSCvu72744	Replace "blacklist" with "blocked list" across all authentication and authorization rules/profiles
CSCvu87758	Guest password policy settings cannot be saved when set to ranges for alphabets or numbers
CSCvu90761	ISE Radius Live Sessions page showing No Data Found
CSCvu91039	ISE 2.6 patch 7 not doing lookup for all mac addresses in mac list causing redirect less Posture to fail
CSCvu97657	ISE 2.4 Application server going to Initializing state on enabling endpoint debugs
CSCvv00951	Application server crashes while transitioning into Stop state
CSCvv04416	Endpoint data not visible on secondary Admin node
CSCvv08466	Log Collection Error alarms appear
CSCvv14001	Authorization profile not saved with proper attributes when Security Group selected under common tasks
CSCvv16401	Pxgrid internal client ping failed
CSCvv25102	Modify TCP settings to enhance TACACS+ and TCP on ISE
CSCvv29190	BYOD Flow is broken in iOS 14 beta
CSCvv30133	Discovery host description text is misleading
CSCvv35921	Cannot start CSV exporting for Selected User in internal ID Store
CSCvv36189	Radius passed-auth live logs not sent due to invalid IPv6 address
CSCvv38249	Manual NMAP not working when only custom ports are enabled
CSCvv39000	Unable to create posture condition for LANDESK
CSCvv41935	PSK cisco-av-pair throws an error if the key contains < or > symbols
CSCvv45174	Static hostname sgt mapping creation does not allow to choose SXP Domain
CSCvv48544	Health check does not work when ISE has NIC teaming enabled
CSCvv50721	Cannot get the download link of NetworkSetupAssistant.exe using Aruba dynamic URL redirect
CSCvv52637	ISE Hotspot guest portal flow broken
CSCvv54761	Export of Current Active Session reports only shows sessions that have been updated since midnight

Caveat ID Number	Description
CSCvv57639	Saving command with parenthesis in TACACS command set gives an error (ISE 2.7 patch 2)
CSCvv57822	Deadlock in pxgrid nodes due to TRACE level debug
CSCvv57830	Group lookup failed as empty value is appended to the context
CSCvv58629	Certificate Authority Service initializing EST Service not running after upgrade to ISE 2.7 patch 2
CSCvv59233	ISE RADIUS Live Log details missing AD-Group-Names under Other Attributes section
CSCvv62549	Custom Attribute from Culinda not shown in endpoint GUI page
CSCvv62729	Network Device API call throws error 500 if you query a nonexistent network device
CSCvv64190	Case sensitivity on User Identity Groups causes "Select Sponsor Group Members" window not to load
CSCvv67051	Radius Server Sequence page showing "no data available"
CSCvv67101	TAC Support Cases redirection issue
CSCvv67743	Posture Assessment by Condition Report displays No Data with Condition Status filter
CSCvv67935	Security Group values in Authorization Profile disappear shortly after fetching
CSCvv68028	Cannot modify AUP text
CSCvv74373	ISE 3.0 DNS resolvability false alarm
CSCvv74517	ISE 3.0 GUI glitch in SAML Identity Providers
CSCvv77530	Unable to retrieve LDAP Groups/Subject Attributes when % character is used twice or more in bind password.
CSCvv77894	Bias-free text/code in upgrade and database
CSCvv78097	Local repository usage information not displayed
CSCvv80113	ISE Posture auto-update not running
CSCvv82806	Network Device IP filter does not match IPs that are inside subnets
CSCvv83510	ISE 3.0 Upgrade failing at RuleResultsSGTUpgradeService step
CSCvv91234	ISE 2.6 scheduled reports are not working when primary MNT is down
CSCvv91684	Collection Filters not displayed in Logging page
CSCvv92203	ISE 2.6 Patch 6: The following error message is displayed while trying to create SGT with the name "Employees": `NetworkAuthZProfile with entered name exists`

Caveat ID Number	Description
CSCvv92613	Users that do not belong to the sponsor group are unable to log in to the sponsor portal
CSCvw01829	ISE GUI Login page shows the following error with Chrome 85/86: `Oops. Something went wrong`
CSCvw08292	ACI mappings not deleted even after delete message is sent
CSCvw38853	ISE 2.6 patch 7: Sophos 10.x definition missing from Anti-malware condition for MAC OSX
CSCvw61595	ISE 3.0 Config Backup Restore failing at step UPSUpgradeHandler

Open Caveats in Cisco ISE Release 3.0 - Cumulative Patch 1

Caveat ID Number	Description
CSCvw73529	Porting changes of OnPrem Satellite option for Smart licensing

Resolved Caveats in Cisco ISE Release 3.0

The resolved caveats in Cisco ISE Release 3.0, have parity with these Cisco ISE patch releases: 2.4 Patch 13, 2.6 Patch 7, and 2.7 Patch 2.

Caveat ID Number	Description
CSCuo02920	ISE not returning configured Radius AVP 18 in access-reject
CSCuz02795	GET-BY-ID Not Implemented exception when home page is refreshed
CSCva44035	ISE shows IP Addr. instead MAC Addr. for VPN users in live auth sometime
CSCvb55884	ISE RBAC Network Device Type/Location View not working
CSCvd38796	No AD domain attributes retrieved for RA-VPN/CWA if AD used for both authC and authZ
CSCve89689	MNT API does not support special charactor
CSCvf30470	MAC OX fails after upgrade to 3.6.11362.2 compliance module
CSCvg50777	nas-update=true accounting attribute will cause session to not be deleted.
CSCvh77224	ENH // Smart License registration using HTTPS Proxy fails
CSCvi35647	Posture session state need to be shared across PSNs in multi-node deployment
CSCvi62805	CSCvi62805 ISE ODBC does not convert the mac address as per configured stored procedure
CSCvj47301	ISE sends CoA to active-compliant sessions when a node-group member is unreachable
CSCvj59836	Typo in Onboard Portal For IOS Devices

Caveat ID Number	Description
CSCvj77817	2.3P4, 2.4P3 upgrade is failing during OS upgrade
CSCvk04307	ISE Guest/BYOD Portal Retry Redirects to 1.1.1.1
CSCvk50684	RADIUS DTLS and Portal usage not being assigned to new self-signed certificate on hostname change
CSCvn02461	Include profiler update for Cisco IP phones - 8832,7832
CSCvn12644	ISE Crashes during policy evaluation for AD attributes
CSCvn48096	Selecting checkbox All endpoints across pages on context visibility doesn't work
CSCvn73740	EAP-TLS authentications with Endpoint profile set to not unknown fails in second authorization.
CSCvn99149	Request cache controll set to private, no-cache and no-store
CSCvo15770	address shows as HTML code in context visibility
CSCvo22887	ISE 2.4 URT does not check is node is on a supported appliance
CSCvo28970	AnyConnect displays Cisco NAC agent error when using Cisco temporal agent
CSCvo84056	Enable or disable "Username/password" in Self-Reg Success Page doesn't hold in Page customization
CSCvo87602	Memory leak on ISE node with the openldap rpm running version 2.4.44
CSCvp42493	Guest ERS API "SearchResult" total is inconsistent with other APIs
CSCvp59038	ISE Secondary PAN node sending RST to other ISE node with src ip address 169.254.2.2
CSCvp61452	[ENH] Remove archives during patch installation phase
CSCvp85813	ISE TACACS livelogs does not have the option to filter using specific NAS ip address.
CSCvp88443	ISE CoA is not sent even though new Logical Profile is used under Authz Policy Exceptions
CSCvp93322	Significant memory increase in MNT during Longevity test
CSCvq12204	ISE 2.4 SNMPv3 user added with wrong hash after reload causing SNMPv3 authentication failure.
CSCvq13431	ISE PSN node crashing while fetching context attributes during posture plus RADIUS flow
CSCvq43600	Disabled PSN persona but TACACS port 49 still open.
CSCvq48396	Replication failed alarm generated and ORA-00001 exceptions seen on ise-psc.log

Caveat ID Number	Description
CSCvq61089	My Device Portal does not show a device after BYOD on-boarding with SAML authentication
CSCvq70247	Preview of of the self registration guest portal does not display "Registration Code" label
CSCvq88821	SNMP traps on access switch connected to APs causes incorrect profiling.
CSCvq90601	EAP Chaining: Dynamic Attribute value is unavailable
CSCvr07294	Radius Authentication and Radius Account Report performance is slow
CSCvr22373	ENH: Support native event log API's, EVT API for the passive ID functionality
CSCvr39943	Blank Course of Action for Threat events received from CTA cloud to TC-NAC adapter
CSCvr40545	EAP-FAST authentication failed with no shared cipher in case of private key encryption failed.
CSCvr40574	Export failed in ISE gui in case of private key encryption failed no ERROR msg in ISE GUI
CSCvr44495	pxGrid not publishing MnT events
CSCvr48726	[enh] Increase Range of Time Interval For Compliance Device ReAuth Query for SCCM
CSCvr68432	2.4P10 Endpoint added via REST has visible policy assignment only in "edit" mode
CSCvr68971	ISE IP routing precedence issue
CSCvr70044	" No policy server detect" on ISE posture module during high load .
CSCvr81384	Failing Network Devices CSV import, process silently terminating without reason
CSCvr83696	ISE: prefers cached AD OU over new OU after changing the Account OU
CSCvr84143	tzdata needs to be updated in ISE guest OS
CSCvr85363	ISE App crash due to user API
CSCvr87373	ACI mappings are not published to SXP pxGrid topic
CSCvr95948	ISE fails to re-establish External syslog connection after break in connectivity
CSCvr96003	SYSAUX tablespace is getting filled up with AWR and OPSSTAT data
CSCvs03810	ISE doesn't display the correct user in RADIUS reports if the user was entered differently twice
CSCvs04433	ISE : TACACS : PSN crashes for TACACS+
CSCvs05260	App server and EST services crash/restart at 1 every morning

Caveat ID Number	Description
CSCvs07344	ISE: Reset config on 2.4 patch 9 throws some errors despite finishing successfully.
CSCvs09981	Add the capability to filter out failed COA due to MAR cache checks among group nodes in ISE
CSCvs19481	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvs23628	Policy engine continues to evaluate all Policy Sets even after rule is matched
CSCvs25258	Improve behavior against brute force password attacks
CSCvs25569	Invalid root CA certificate accepted
CSCvs36036	ISE 2.6 should allow multiple blank lines in dACL syntax, even if user chooses IPv4 (or) IPv6.
CSCvs36150	ISE 2.x Network Device stuck loading
CSCvs36758	Unable to configure CRL URL with 2 parenthesis at ISE 2.6
CSCvs38883	Trustsec matrix pushing stale data
CSCvs39633	NAD group CSV imports should allow all supported characters in description field.
CSCvs39880	Highload on Mnt nodes with Xms value
CSCvs40406	SEC_ERROR_BAD_DATABASE seen in system/app debug logs while removing a trusted CA cert
CSCvs41571	Self Registered Guest portal unable to save guest type settings
CSCvs42072	Unable to edit static group assignment
CSCvs42441	Service account passwords returned from server in SMS and LDAP page
CSCvs42758	The CRL is expired with specific condition
CSCvs44006	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvs44795	ISE not updating SGT's correctly
CSCvs46274	Radius Accounting report doesn't work - no accounting records show
CSCvs46399	AuthZ profile advanced profile for url-redirect does not allow custom HTTPS destination
CSCvs46853	ISE 2.6 CA Certificate with the same CN removed from Trusted Store while integrating with DNA-C
CSCvs46998	Condition disappeared from the library but is still in DB
CSCvs47941	Fail to import Internal CA and key on ISE2.6

Caveat ID Number	Description
CSCvs50437	ISE versions use old JDBC version (11.2.0.3) which is not compatible with new Oracle Database
CSCvs51296	ISE allows to insert a space before command under Command Sets
CSCvs51519	NFS mounting causes crash
CSCvs51537	Backups are not triggering with special characters for encryption key
CSCvs52031	MACAdress API is not working(API/mnt/Session/MACAddress)
CSCvs53606	ISE 2.4: Administrator Login Report, Auth failed when using cert based admin auth
CSCvs55464	Creating a new user in the sponsor portal shows "invalid input"
CSCvs55594	Days to Expiry value, marked as 0 for random authentications
CSCvs56617	In captive portal user can trigger the sending of emails at will
CSCvs58106	NAD CSV imports should allow all supported characters in the TrustSecDeviceID
CSCvs60518	ISE Admin User Unable To Change The Group For Internal Users
CSCvs62081	collector log filled with repeated pxGrid and DNAC messages
CSCvs62586	Tacacsprofile not retrieved properly using REST API
CSCvs62597	Authz Profiles not pulling properly using REST API (Pagination is missing)
CSCvs65467	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability
CSCvs65989	After importing network device / groups, unable to add new Location
CSCvs67042	ISE 2.2+ affected with memory leak. Everyday 1-2% increase in native memory due to Inflater()
CSCvs68914	ISE errors when Security Group is created with an underscore via ERS API
CSCvs69726	ISE 2.2+ affected with memory leak. Everyday 1-2% increase in native memory by PORT_Alloc_Util()
CSCvs70997	ISE: 2.4p9 Intermediate CA cert not installed when configuring SCEP RA
CSCvs75068	Cannot add registry key value condition containing % or < as it throws an error
CSCvs75274	Unable to do portal customization for "certificate provisioning portal"
CSCvs76257	ISE crashes due to empty string instead of username in RadiusProxyFlow::stripUserName()
CSCvs77182	ISE: Unable to use attribute "url-redirect" with HTTPS, same URL with HTTP works fine.
CSCvs78160	URT fails on a ConditionsData clause from INetworkAuthZCheck

Caveat ID Number	Description
CSCvs79836	Expired Certificates not listed for deletion
CSCvs82557	SXP Bindings are not published to pxGrid 2.0 clients
CSCvs83303	API is not retrieving the data when interim-updates are not stored DB
CSCvs85970	Having string 'TACACS' in AD join-point causes AD joinpoint to not show in AuthZ condition
CSCvs86344	ISE 2.4 Guest ERS Call Get-By-Name fails when guest username contains @ sign (guest@example.com)
CSCvs86775	ISE 2.6 Install: Input Validation- Check IP Domain Name
CSCvs88368	ISE SNMP server crashes when using Hash Password.
CSCvs89440	CEPM schema stats not collected/scheduled for PAN only node
CSCvs89683	RabbitMQ user password printed in plain text in ADE-OS log, should be masked or removed
CSCvs91026	Docker image ise-rabbitmq could not be successfully loaded post config reset
CSCvs91408	LONG:Significant memory increase in PMNT node of longevity test
CSCvs91808	Importing metadata xml file with special characters results in unsupported tags error
CSCvs96516	Multiple Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerabilities
CSCvs96541	TACACS auth/acc reports are not visbile after restoring OP backup
CSCvs96544	Importing Endpoint CSV file to CV 2.4 patch 9 does not retain 'description' field
CSCvs96560	ISE ERS API lookup slow when large number of endpoints exist
CSCvs97302	.dmp files not deleted from /opt/oracle/base/admin/cpm10/dpdump even after the reset-config on ISE
CSCvs98094	File Remediation check is failing while tested with ISE 2.7 server
CSCvt00283	404 error upon refresh of success page of guest sponsored portal
CSCvt00780	We are not able to Localize message for OS detection message in BYOD welcome page
CSCvt01161	NMAP - MCAFeeEPROOrchestratorClientscan fails to execute on 2.6 version of ISE
CSCvt03094	ISE expired TACACS sessions are not cleared in a timely manner from session cache
CSCvt03292	Cert Revoke and CPP not functioning without APEX license.
CSCvt03935	Change "View" Options Wording in TrustSec Policy Matrix--ISE

Caveat ID Number	Description
CSCvt04047	POST getBackupRestoreStatus occures on every ISE page after navigating to Backup/Restore menu
CSCvt04144	No threshold option for High disk Utilization in Alarm Settings
CSCvt05201	Posture with tunnel group policy evaluation is eating away Java Mem
CSCvt07230	ISE shouldnt be allowing ANY in egress policy when imported
CSCvt08143	Time difference in ISE 2.6
CSCvt09164	ISE 2.2 P16 Already extended guest user cannot be extended again
CSCvt09434	Add proper logging and reporting to handle SCCM server timeout
CSCvt09458	ISE MDM integration - misleading COA type in the debugs
CSCvt10214	[ENH] Add the ability to "GET|PUT|DELETE by Name" using the API for network devices
CSCvt11130	Sh version command is not working ISE non-admin CLI user
CSCvt11179	"AD-Operating-System" attribute is not being fetched when this OS attribute changes on the AD Server
CSCvt11366	Exporting Endpoints from CLI results in java exception
CSCvt11380	Still Possible to Create SGTs within Policy Sets Eventhough DNAC Manages GBAC
CSCvt11664	ISE Feed Server fails via 'createLicenseSource' method "FlexlmListException: Error"
CSCvt12236	IP SGT static mapping import not working correctly with hostnames
CSCvt13707	pxGrid 2.0 WebSocket distributed upstream connect issue
CSCvt13719	pxGrid 2.0 WebSocket ping pong too slow even on idled standalone
CSCvt13746	ISE doesn't display all device admin authz rules when there are more authz policies and exceptions
CSCvt14248	Certificate Authority Service initializing EST Service not running after upgrade to ISE 2.6/2.7
CSCvt15256	Authentication goes to process fail when "Guest User" ID Store is used.
CSCvt15893	Preventive bug :Radius Errors/Misconfigured supplicants tables do not exist after upgrade to ISE2.6
CSCvt15935	High Load Alarms coinciding with System Summary Dashboard not populating for some nodes
CSCvt16882	When accessing the portal with iPad using Apple CNA and AUP as a link we get 400 Bad Request error.

Caveat ID Number	Description
CSCvt17283	GUI Slowness while enabling AVC
CSCvt17783	ISE shouldn't allow ANY SGT or value 65535 to be exposed over SGT import or export
CSCvt18613	AuthZ Conditions with AD Groups Not matched for TEAP - EAP-Chaining
CSCvt19657	ISE ERS API Endpoint update slow when large number of endpoints exist
CSCvt22900	"*Endpoint Consumption Count Updated :" not updated in Licensing
CSCvt24276	Cannot add/modify allowed values more than 6 attributes to System Use dictionaries
CSCvt25610	ISE2.7 compliance counter is 0
CSCvt26108	ISE 2.7 Anyconnect configuration's deferred updates do not get saved
CSCvt34876	ISE latency in responding to RADIUS and high CPU
CSCvt35044	EP lookup takes more time causing high latency for guest flow
CSCvt35239	NullpointerException thrown in catalina.out during posture flow when clientMac is null
CSCvt36117	Identity group update for an internal user in ISE via ERS
CSCvt36322	ISE 2.6 MDM flow fails if redirect value is present in the URL
CSCvt36452	Expired Evaluation profiler lic on ISE will cause default radius probe to enable
CSCvt37910	[ENH] Add the ability to "GET|PUT|DELETE by Name" using the API for /ers/config/internaluser
CSCvt38308	ISE: If min pwd length is increased then exisiting shorter pwd fails to login via GUI with no error
CSCvt40534	MNT node election process is not properly designed.
CSCvt42064	ISE wrongly reports posture session lookup calls as SSH login
CSCvt43844	ISE: runtime-aaa debugs do not print packet details in ascii; breaking Endpoint debugs
CSCvt46584	Backups failing due to disk space issue not purged ENDPOINTS_REJECT_RELEASE table
CSCvt46850	Unavailability to edit saved compound conditions using conditions library.
CSCvt49961	Syslog Target configured with FQDN can cause Network Outage
CSCvt53541	SMS over HTTPS is not sending username/password to gateway
CSCvt55300	"Current IP address" is displayed in CV even though IP attribute in redis has been removed

Caveat ID Number	Description
CSCvt55312	ISE BYOD with Apple CNA fails with 9800
CSCvt57274	Authentication summary report for yesterday and today not showing adata
CSCvt57571	App-server crashes if IP-access submitted w/o any entries
CSCvt57805	Intermittent password rule error for REST API Update Operation
CSCvt61181	ISE ERS API - GET calls on network devices is slow while processing SNMP configuration
CSCvt63793	Posture - non redirection flow fails with "No policy server detected" when LSD is disbaled
CSCvt65332	Description using two lines, or <Enter> was used, under Client provisioning resources throws errorA
CSCvt65719	Misleading Null Pointer exception, post Manual sync is performed
CSCvt65853	ISE-2.x || MNT REST API for ReAuth fails when using in distributed deployment
CSCvt67595	Livelogs are not showing for User authentication failed
CSCvt69912	ISE still generates false positive alarm "Alarms: Patch Failure"
CSCvt70689	Application server may crash when MAR cache replication is enabled
CSCvt71355	pxGrid unable to delete user in INIT state
CSCvt71559	Alarm Dashlet shows 'No Data Found'.
CSCvt73953	Mismatched Information between CLI export and Context Visibility
CSCvt76509	ISE Backup file transfer logs show Success although there is no space in the SFTP Repository
CSCvt80285	Cannot select 45 or more products when creating Anti-Malware Condition for definition
CSCvt81194	CPU spikes are being observed at policy HitCountCollector
CSCvt82384	Rotation of diagnostics.log is not working on ISE
CSCvt85722	No debug log for non working MNT widgets
CSCvt85757	Sponsor portal display ? for non English characters
CSCvt85836	Session cache getting filled with incomplete sessions
CSCvt87409	ISE DACL Syntax check not detecting IPv4 format errors
CSCvt89098	ISE does not reattempt wildcard replication for failed nodes
CSCvt91871	ISE RADIUS Accounting Report details shows "No data found" under Accounting Details

Caveat ID Number	Description
CSCvt93117	ise-psc.log filled up with "check TTConnection is valid" causing relevant logs to roll over
CSCvt93603	ISE 2.6p6 Unable to delete custom endpoint attribute
CSCvt96594	ISE 2.6 : Create Guest User using external sponsor users via ERS fails with 401 Unauthorized Error
CSCvu04874	suspected memory leak in io.netty.buffer.PoolChunk
CSCvu05164	ISE is not allowing to disable Radius in NAD via API
CSCvu10009	Mandatory values when using Update-By-Name method with Internal Users
CSCvu15948	TC-NAC adapter stopped scanning with nexpose (insiteVM)
CSCvu16067	Changes in IP-TABLES ISE 2.6 causing TCP delays, TACACS latency
CSCvu20359	Markup langauge error when use file check condition with dot(.) in file name
CSCvu21093	ISE 2.6p6 // Portal background displays incorrectly
CSCvu25625	ISE is returning an incorrect version for the rest API call from DNAC
CSCvu25975	Import option is not working under Tacacs command sets
CSCvu28305	ISE logging timestamp shows future date
CSCvu29434	ISE2.6P6 services fail to initialize after reload on SNS 3655 PSN
CSCvu30286	ERS SGT create is not permitted after moving from Multiple matrix to Single matrix
CSCvu31176	2.4P11 VPN + Posture : Apex Licenses are not being consumed,
CSCvu31853	NDG added through ERS became associated with all network devices in DB
CSCvu32240	When running ISR ERS API for internaluser update the existing identityGroups value is set to null
CSCvu32865	High cpu on ISE 2.7 causing authentication latency
CSCvu33416	License out of compliance alarm with a valid license
CSCvu33861	ISE 2.4 p6 - REST API MnT query to get device by MAC address taking more than 2 seconds
CSCvu34433	ISE 2.x, Free space on Undo tablespace not cleared as per isehourlycron.sh cron script
CSCvu34895	Report repository export is not working with dedicated mnt enable.
CSCvu35802	Shared email for AD users fail to retrieve groups,ISE shows multiple account found in forest
CSCvu39653	Session API for MAC Address returning Char 0x0 out of allowed range

Caveat ID Number	Description
CSCvu41815	[CFD] GBAC sync breaks on deleting VN from SG if AuthZ profile is mapped to the same VN for diff SG
CSCvu42244	Machine Authentications via EAP-TLS fail during authorization flow citing a user not found error
CSCvu47395	ISE 2.x, 3.x : Drop_Cache required for systems with High Memory Issues
CSCvu48417	ISE ERS API DELETE device returns 500 error with more than 1 call
CSCvu49019	suspected Memory Leak in Elastic search
CSCvu49724	Devices configured SNMP v2c version on DNAC is not seen on Network devices in ISE
CSCvu53022	ISE: prefers cached AD OU over new OU after changing the Account OU
CSCvu53836	ISE Authorize-Only requests are not assessed against Internal User Groups
CSCvu55332	REST API call can remove Network Device Group referenced in Policy Set
CSCvu55557	Radius secret 4 chars min requirement is not checked when REST API used to create NAD
CSCvu58476	Improve error messaging on My Device Portal when the identity store has issues
CSCvu58793	ERS REST API returns duplicate values multiple times when use filter by locations
CSCvu59093	SessionDB columns are missing from ISE (>=2.4)
CSCvu59491	ISE creates new site in insiteVM (tc-nac server)
CSCvu63642	Context Visibility fuses endpoint parameters on username update
CSCvu63833	Failed Logins to ISE GUI Are Not Seen in Audit Report When AD Is Selected as the Identity Source
CSCvu67707	CWE-937 Use of JavaScript Library with Known Vulnerability
CSCvu68700	ISE 2.6 p5 ERS API res for XML or JSON req with invalid creds is HTTP 401 with unexpected HTML body
CSCvu70683	Alarm Suppression required for ERS queries along with suppression on iselocalstore.log
CSCvu70768	Alarms and system summary is not showing up on ISE GUI
CSCvu73387	authentication failure with reason"12308 Client sent Result TLV indicating failure"
CSCvu74198	ISE: LDAP and ODBC identity store names do not allow hyphen
CSCvu83759	ISE is deleting Key pairs after changes perfomed in sftp repository
CSCvu90107	ISE allows duplicates device ID in ERS flow in all version.

Caveat ID Number	Description
CSCvu90703	CLDAP thread is hung and running infinite
CSCvu91016	InternalUser Attributes in ATZ policy will fail TACACS+ ASCII Authentication
CSCvu91601	ISE Authentication Status API Call Duration does not work as expected
CSCvu94733	Guest authentication fails with "Account is not yet active" for incorrect password
CSCvv00377	Overlap of network devices using subnet and IP range
CSCvv07049	ISE unable to connect with ODBC "Connection failed" with a port number
CSCvv09167	TACACS Aggregate table is not purged properly.
CSCvv15811	ISE TCP ports 84xx not opened if there is shutdown interface with IP address assigned
CSCvv23256	ISE Authentication Status API Call does not return all records for the specified time range
CSCvv26811	Policy Export Is Not Being Saved Without Encryption After It is Saved With Encryption
CSCvv44914	isedataupgrade.sh failed. ISE global data upgrade failed -2.7,3.0 from ISE 2.6P6
CSCvr63698	pxGrid 2.0 authorization profile attribute missing from the session directory
CSCvp93901	pxGrid to publish ADUser, ADHost, SamAccountName and QualifiedName
CSCve58268	Add to ISE SCCM query possibility to check Baseline status
CSCve58212	Add to ISE SCCM query possibility to check Configuration Item status

Open Caveats in Cisco ISE Release 3.0

Caveat ID Number	Description
CSCvq75448	FMC subscription to ISE unavailable with large count of SGTs
CSCvr24059	Source SGT correlation doesn't work for FMC and FTD 6.5
CSCvv45728	few labels in the ISE Admin GUI are not translated into Japanese
CSCvv54305	"Support TrustSec Verification reports" checkbox shouldnt be enabled
CSCvv54754	IE latest version:Portal tiles are overlapping in guest portal page on a DB restored setup.
CSCvv55971	IE GUI :Progress bars & info icons overlapping/misaligned with module names in health check page.
CSCvv57822	Deadlock in pxgrid nodes due to TRACE level debug.
CSCvv58353	HTTPS serverlist config not persistent post upgrade from 2.7 P1 to ISE 3.0

Caveat ID Number	Description
CSCvt97146	[ISE-3.0]ISED crashing continuously in WSA
CSCvu78668	[ISE3.0]:ISE-WSA Integration fails when no session is present
CSCvv66302	Domain doesnt get assigned to sxp peer
CSCvv67101	TAC Support Cases Redirection Issue
CSCwc83059	Post full upgrade VCS information is missing
CSCwe99609	Timestamps need adjustment whenever timezone is changed
CSCwe99666	Live logs and live sessions pages are displayed in incorrect sorting order when timezone is changed on PSN and MnT nodes
CSCwe99706	Session data is shown at the bottom when PSNs are in different timezones

Communications, Services, and Additional Information

- To receive timely and relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you are looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure and validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain information about general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

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

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

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

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

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

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

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

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

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

© 2020 Cisco Systems, Inc. All rights reserved.