Release Notes for Cisco Identity Services Engine, Release 3.3

First Published: 2023-07-05

Last Modified: 2026-09-23

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 Group Based Policy solution and supports TrustSec software-defined segmentation.

Cisco ISE is available on Cisco Secure Network Server appliances with different performance characterizations, virtual machines (VMs), and on public clouds.

Cisco ISE has a scalable architecture with centralized management and control. It supports both standalone with high availability and distributed deployment. 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 3.3?

This section lists the new and changed features in Cisco ISE release 3.3.

Table 1: New and changed information

Date	Description
2026-09-14	General availability of Cisco ISE release 3.3 cumulative patch 12.
2026-04-17	General availability of Cisco ISE release 3.3 cumulative patch 11.
2026-03-05	General availability of Cisco ISE release 3.3 cumulative patch 10.
2025-12-25	General availability of Cisco ISE release 3.3 cumulative patch 9.
2025-11-17	General availability of Cisco ISE release 3.3 cumulative patch 8.

Date	Description
2025-07-15	General availability of Cisco ISE release 3.3 cumulative patch 7.
2025-06-04	General availability of Cisco ISE release 3.3 cumulative patch 6.
2025-04-10	General availability of Cisco ISE release 3.3 cumulative patch 5.
2024-10-30	General availability of Cisco ISE release 3.3 cumulative patch 4.
2024-07-17	General availability of Cisco ISE release 3.3 cumulative patch 3.
2024-04-18	General availability of Cisco ISE release 3.3 cumulative patch 2.
2023-12-07	General availability of Cisco ISE release 3.3 cumulative patch 1.
2023-07-05	General availability of Cisco ISE release 3.3.

New features in Cisco ISE release 3.3 cumulative patch 12

Support for Windows Server

You can use Windows Server 2025 Active Directory domains as an external identity source in Cisco ISE for your identity management needs. This support allows you to integrate with the latest Windows Server infrastructure to manage user and machine authentications. Due to enhanced security settings in Windows Server 2025, password changes done through EAP-MS-CHAPv2 and EAP-GTC are disabled by default.

For more information, refer to Modify password changes, machine authentications, and machine access restriction settings and Allowed Protocols in the Cisco ISE Administrator guide, release 3.3

New features in Cisco ISE release 3.3 cumulative patch 11

Allow server EKU certificates for Cisco pxGrid

Cisco ISE will support using server certificates with only the server authentication EKU for Cisco pxGrid. This update ensures your services remain compatible with new public CA standards.

For more information, refer to Allow server EKU certificates for Cisco pxGrid.

New features in Cisco ISE release 3.3 cumulative patch 10

There are no new features in Cisco ISE release 3.3 cumulative patch 10.

New features in Cisco ISE release 3.3 cumulative patch 9

There are no new features in Cisco ISE release 3.3 cumulative patch 9.

New features in Cisco ISE release 3.3 cumulative patch 8

OAuth support for SMTP

You can enable or disable authentication settings for your Simple Mail Transfer Protocol (SMTP) servers in the Cisco ISE GUI. This release adds support for Microsoft OAuth authentication, in addition to basic password authentication.

For more information, refer to Configure SMTP Server to Support Notifications.

New Cisco ISE configuration option

This node-specific configuration option is added to the **application configure ise** command:

[45] Enable/Disable Fragmentation of RADIUS Packets

Option 45 allows you to manage the behavior of Don't Fragment (DF) bit. By default, Cisco ISE sets the DF bit on packets that exceed the interface MTU. Because this behavior may cause packet-handling conflicts depending on your network configuration, use Option 45 to enable or disable the setting of the DF bit.

New features in Cisco ISE release 3.3 cumulative patch 7

Support for Cisco Secure Network Server 3800 series appliance

The Cisco Secure Network Server (Cisco SNS) 3800 series appliances are based on the Cisco Unified Computing System (Cisco UCS) C225 M8 Rack Server and are configured specifically to support Cisco Identity Services Engine (Cisco ISE). Cisco SNS 3800 series appliances are designed to deliver high performance and efficiency for a wide range of workloads.

The Cisco SNS 3800 series appliances are available in these models:

- Cisco SNS 3815 (SNS-3815-K9)
- Cisco SNS 3855 (SNS-3855-K9)
- Cisco SNS 3895 (SNS-3895-K9)

Cisco SNS 3815 appliance is ideal for small deployments. Cisco SNS 3855 and Cisco SNS 3895 appliances have several redundant components such as hard disks and power supplies and are suitable for larger deployments that require highly reliable system configurations. Cisco SNS 3895 is recommended for PAN and MnT personas.

Note

- You must use only this ISO file to install Cisco ISE on a Cisco SNS 3800 appliance:

  Cisco-ISE-3.3.0.430.SPA.x86_64_SNS-38x5_APPLIANCE_ONLY.iso

- Cisco SNS 3800 appliances are supported from Cisco ISE release 3.3 patch 7.

  Do not roll back the first patch (patch 7 or higher) after installation. If you roll back the first patch, Cisco ISE services will not start.

  However, you can roll back patches that you install subsequently.

- Cisco SNS 3855 appliance can be configured with one hard disk or four hard disks. It is recommended to enable only the PSN or pxGrid persona if your Cisco SNS 3855 appliance is configured with only one hard disk.

For more information, see the Cisco Secure Network Server 3800 Series Appliance Hardware Installation Guide.

New features in Cisco ISE release 3.3 cumulative patch 6

There are no new features in Cisco ISE release 3.3 cumulative patch 6.

New features in Cisco ISE release 3.3 cumulative patch 5

Blast RADIUS vulnerability fix

To address the Blast RADIUS vulnerability reported in CSCwk67747, the **Message Authenticator Required On Response** check is introduced in **External RADIUS Server**, **RADIUS Token ID Store**, and **Device Profile**.

This check box is not enabled by default after a patch upgrade. Once the check box is enabled, Cisco ISE will not validate any packet that lacks a **Message-Authenticator** attribute in the response, causing the RADIUS flow to fail.

For more information, see the topics "Network Device Profiles Settings" and "External RADIUS Server Settings" in the chapter *Threat Containment* and the topic "Add a RADIUS Token Server" in the chapter *Asset Visibility* in the *Cisco ISE Administrator Guide, Release 3.3*.

Integrate Cisco pxGrid Cloud applications using Integration Catalog

From Cisco ISE Release 3.3 Patch 5, you can use a native integration catalog interface in Cisco ISE to integrate with Cisco pxGrid Cloud applications for a simplified integration experience. Cisco pxGrid Cloud apps can be integrated with Cisco ISE using the **Integration Catalog** (**Administration** > **System** > **Deployment** > **Integration Catalog**). You can integrate both single-instance and multi-instance Cisco pxGrid Cloud apps. For more information, see the Cisco pxGrid Cloud Solution Guide.

Time restricted debug enabling

The time restricted debug enabling feature allows you to select a log level and set a reset timer to revert to default settings. The selected node reverts to the default state after the timer expires.

For more information, refer to Configure Debug Log Settings in chapter "Troubleshooting" in *Cisco Identity Services Engine Administrator Guide, Release3.3*.

New features in Cisco ISE release 3.3 cumulative patch 4

API keys and certificate authentication support for Tenable Security Center

From Cisco ISE 3.3 Patch 4 onwards, the following authentication methods are additionally supported for Tenable Security Center:

- **API Keys**: Enter the Access key and Secret key of the user account that has access privileges in Tenable Security Center.

  API keys authentication is supported for Tenable Security Center 5.13.x and later releases.



Note Before choosing this option in Cisco ISE, you must log in as an Admin user and enable API key authentication in Tenable Security Center.

- **Certificate Authentication**: From the **Authentication Certificate** drop-down list, choose the required certificate.

  After successful authentication, Cisco ISE will retrieve the customer configured template from Tenable Security Center.

Note Before enabling this option in Cisco ISE, you must configure Tenable Security Center to allow SSL client certificate authentication.

For more information, see "Configure Tenable Adapter" in the chapter "Threat Containment" in the *Cisco Identity Services Engine Administration Guide, Release 3.3*.

Assign dedicated resources for join points

From Cisco ISE Release 3.3 Patch 4, you can reserve resources for the join points in each PSN. This resource segmentation will help reduce the performance impact caused by resource sharing among the join points.

For more information, see "Assign dedicated resources for join points" in the Chapter "Asset Visibility" in the *Cisco Identity Services Engine Administrator Guide, Release 3.3*.

Security identifiers in certificates will not be used for authentication

From Cisco ISE Release 3.3 Patch 4, Cisco ISE supports a new format of certificates with Security Identifiers (SID).

The SIDs present in the Subject Alternative Name (SAN) fields will not be used for authentication in Cisco ISE. This enhancement prevents authentication failures caused due to incorrect SID parsing in the authentication process.

SSHD service cryptographic algorithms enhancement

You can use these new algorithms under service sshd to manage a service using the Cisco ISE CLI:

- **MAC-algorithm**
- **Hostkey**
- **Hostkey-algorithm**
- **Key-exchange-algorithm**
- **SSH-client-hostkey-algorithm**

For more information, refer to service sshd in chapter "Cisco ISE CLI Commands in Configuration Mode" in the *Cisco Identity Services Engine CLI Reference Guide, Release 3.2*service sshd in chapter "Cisco ISE CLI Commands in Configuration Mode" in the *Cisco Identity Services Engine CLI Reference Guide, Release 3.3*.

Support for osquery condition

From Cisco ISE 3.3 Patch 4, you can create an osquery condition to check the posture compliance status of an endpoint or fetch the required attributes from an endpoint.

For more information, see "Add an osquery condition" in the Chapter "Compliance" in the *Cisco Identity Services Engine Administrator Guide, Release 3.3*.

Note For osquery condition support, you must use compliance module 4.3.3394 or later and Cisco Secure Client 5.1.7 or later versions.

Support for usgv6 command

Use the **usgv6** command in EXEC mode to enable, disable, or check the usgv6 compliance status of a Cisco ISE node with the underlying operating system.

For more information, see "usgv6" in the chapter "Cisco ISE CLI Commands in EXEC Mode" in the *Cisco Identity Services Engine CLI Reference Guide, Release 3.3*.

New features in Cisco ISE release 3.3 cumulative patch 3

CLI option to enable or disable the explicit curve check

From Cisco ISE release 3.3 patch 3, administrators can use the following option in the **application configure ise** CLI command to verify the Elliptic Curve Digital Signature Algorithm (ECDSA) explicit curve certificate:

```
[39]Enable/Disable Explicit EC Check
```

The certificate verification applies to EAP TLS server mode, secure syslog, and secure LDAP.

For more information, see "Application Configure ISE" in the chapter "Cisco ISE CLI Commands in EXEC Mode" in the *Cisco Identity Services Engine CLI Reference Guide, Release 3.3*.

Add identity sync after creating a Duo connection

If you do not want to configure user data synchronization between Active Directory and Duo while creating a Duo connection, click **Skip** in the **Identity Sync** page. You will be taken to the **Summary** page directly.

After you create a Duo connection, you can add identity sync configurations at any time.

For more information, see "Integrate Cisco Duo With Cisco ISE for Multifactor Authentication" in the Chapter "Segmentation" in the *Cisco Identity Services Engine Administrator Guide, Release 3.3*.

New features in Cisco ISE release 3.3 cumulative patch 2

Configure Virtual Tunnel Interfaces with Native IPsec

From Cisco ISE release 3.3 patch 2, you can configure Virtual Tunnel Interfaces (VTIs) using the **Native IPsec** configuration page. You can use this to establish security associations between Cisco ISE PSNs and NADs across an IPsec tunnel using IKEv1 and IKEv2 protocols. Native IPsec configuration ensures that Cisco ISE is FIPS 140-3 compliant. For more information, see "Configure Native IPsec on Cisco ISE" in the "Secure Access" chapter in the *Cisco ISE Administrator Guide, Release 3.3*.

End of support for Legacy IPsec (ESR)

From Cisco ISE release 3.3 patch 2, Legacy IPsec (ESR) is not supported on Cisco ISE. All IPsec configurations on Cisco ISE will be Native IPsec configurations. We recommend that you migrate to native IPsec from legacy IPsec (ESR) before upgrading to Cisco ISE release 3.3 cumulative patch 2 to avoid any loss of tunnel and

tunnel configurations. For more information, see "Migrate from Legacy IPsec to Native IPsec on Cisco ISE" in the chapter "Secure Access" in the *Cisco ISE Administrator Guide*.

Enhanced password security

Cisco ISE now improves password security through the following enhancements:

- You can choose to hide the Show button for the following field values, to prevent them from being viewed in plaintext during editing:

  Under **Network Devices**,

  - **RADIUS Shared Secret**
  - **Radius Second Shared Secret**

  Under **Native IPSec**,

  - **Pre-shared Key**

  To do this, choose **Administration** > **Settings** > **Security Settings** and uncheck the **Show Password in Plaintext** checkbox.

  For more information, see "Configure Security Settings" in the Chapter "Segmentation" in the *Cisco ISE Administrator Guide, Release 3.3*.

- To prevent the RADIUS Shared Secret and Second Shared Secret from being viewed in plaintext during network device import and export, a new column with the header **PasswordEncrypted:Boolean(true|false)** has been added to the Network Devices Import Template Format. No field value is required for this column.

  If you are importing network devices from Cisco ISE Release 3.3 Patch 1 or earlier releases, you must add a new column with this header to the right of the **Authentication:Shared Secret:String(128)** column, before import. If you do not add this column, an error message is displayed, and you will not be able to import the file. Network devices with encrypted passwords will be rejected if a valid key to decrypt the password is not provided during import.

  For more information, see the table in "Network Devices Import Template Format" in the Chapter "Secure Access" in the *Cisco ISE Administrator Guide, Release 3.3*.

Localized ISE installation

While reinstalling Cisco ISE, you can use the **Localized ISE Install** option (option 38) in the **application configure ise** command to reduce the installation time. Though this option can be used for both Cisco Secure Network Server and virtual appliances, it significantly reduces the reinstallation time for Cisco Secure Network Servers.

For more information, see "Localized ISE Installation" in the Chapter "Cisco ISE CLI Commands in EXEC Mode" in the *Cisco Identity Services Engine CLI Reference Guide, Release 3.3.*

Locking identities with repeated authentication failures

You can now limit the maximum number of unsuccessful authentication attempts an identity (username or hostname) can make while authenticating through the EAP-TLS protocol, by specifying the number of authentication failures after which the identity must be locked. Identities can be locked permanently or for a specific time period. Successful authentications by a locked identity will also be rejected until the identity is unlocked again.

For more information, see the table in "RADIUS Settings" in the Chapter "Segmentation" in the *Cisco Identity Services Engine Administrator Guide, Release 3.3*.



Note From Cisco ISE release 3.3 patch 4, **Identity Lock Settings** are not supported in the **RADIUS Settings** page (**Administration > System > Settings > Protocols > RADIUS**).

On-demand pxGrid Direct data synchronization using Sync Now

You can use the **Sync Now** feature to perform on-demand synchronization of data for pxGrid Direct URL Fetcher connectors. You can perform both full and incremental syncs on-demand. On-demand data synchronization can be performed through the Cisco ISE GUI or using OpenAPI.

For more information, see "On-demand pxGrid Direct Data Synchronization using Sync Now" in the "Asset Visibility" chapter in the *Cisco ISE Administrator Guide, Release 3.3*.

Opening TAC support cases in Cisco ISE

From Cisco ISE release 3.3 patch 2, you can open TAC support cases for Cisco ISE directly from the Cisco ISE GUI.

For more information, see "Open TAC Support Cases" in the chapter "Troubleshoot" in *Cisco ISE Administrator Guide, Release 3.3*.

New session directory topic available using pxGrid

From Cisco ISE release 3.3 patch 2 onwards, you can subscribe to the Session Directory All topic using pxGrid. The sessionTopicAll is similar to the existing sessionTopic (which continues to be supported), with one key difference. The sessionTopicAll also publishes events for sessions without IP addresses. For more information, see the pxGrid API Guide.

Support for Transport Gateway removed

Cisco ISE no longer supports Transport Gateway. The following Cisco ISE features used Transport Gateway as a connection method:

- Cisco ISE Smart Licensing

  If you use Transport Gateway as the connection method in your smart licensing configuration, you must edit the setting before you upgrade to Cisco ISE release 3.3 patch 2. You must choose a different connection method as Cisco ISE release 3.3 patch 2 does not support Transport Gateway. If you upgrade to Cisco ISE release 3.3 patch 2 without updating the connection method, your smart licensing configuration is automatically updated to use the Direct HTTPS connection method during the upgrade process. You can change the connection method at any time after the upgrade.

- Cisco ISE Telemetry

  Transport Gateway is no longer available as a connection method when using Cisco ISE Telemetry. The telemetry workflow is not impacted by this change.

TLS 1.3 support for Cisco ISE workflows

Cisco ISE release 3.3 patch 2 and later releases allow TLS 1.3 to communicate with peers for the following workflows:

- Cisco ISE is configured as an EAP-TLS server
- Cisco ISE is configured as a TEAP server

Attention TLS 1.3 support for Cisco ISE configured as a TEAP server has been tested under internal test conditions because at the time of Cisco ISE release 3.3 patch 2 release, TEAP TLS 1.3 is not supported by any available client OS.

- Cisco ISE is configured as a secure TCP syslog client

Note For Cisco ISE release 3.3 patch 2, the **Manually Configure Ciphers List** option is not supported for TLS 1.3.

For more information, see "Configure Security Settings" in the Chapter "Segmentation" in the *Cisco Identity Services Engine Administrator Guide, Release 3.3*.

New features in Cisco ISE release 3.3 cumulative patch 1

Cisco Duo integration for multifactor authentication

From Cisco ISE release 3.3 patch 1, you can directly integrate Cisco Duo as an external identity source for multifactor authentication (MFA) workflows. In earlier releases of Cisco ISE, Cisco Duo was supported as an external RADIUS proxy server and this configuration continues to be supported.

This Cisco Duo integration supports the following multifactor authentication use cases:

1. VPN user authentication
2. TACACS+ admin access authentication

For more information on this feature, see "Integrate Cisco Duo with Cisco ISE for Multifactor Authentication" in the Chapter "Segmentation" of the Cisco ISE Administration Guide, Release 3.3.

Customer experience surveys

Cisco ISE now presents customer satisfaction surveys to its users within the administration portal. The periodic administration of customer satisfaction surveys helps us better understand your Cisco ISE experiences, track what is working well, and identify areas of improvement. After you submit a survey, you are not presented with another survey for the next 90 days.

The surveys are enabled by default in all Cisco ISE deployments. You can disable the surveys at a user level or for a Cisco ISE deployment.

For more information, see "Customer Experience Surveys" in the chapter "Basic Setup" in the Cisco ISE Administrator Guide, *Release 3.3*.

Microsoft Intune ends support for UDID-based queries for its MDM integrations

From March 24, 2024, Microsoft Intune will not support UDID-based queries for its MDM integrations, as detailed in this Field Notice. The Cisco ISE APIs that fetch required endpoint information from Microsoft Intune MDM integrations have changed in response to this end of support.

From Cisco ISE release 3.3 patch 1, Microsoft Intune only provides the following endpoint details in response to compliance APIs:

- Device compliance status
- Managed by Intune
- MAC address
- Registration status

For more information on these changes, see *Integrate MDM and UEM Servers with Cisco ISE*.

New features in Cisco ISE release 3.3

Access the Cisco ISE admin GUI using HTTPS with TLS 1.3

From Cisco ISE release 3.3, you can access the Cisco ISE Admin GUI using HTTPS with TLS 1.3 version. For more information, see "Configure Security Settings" in the chapter "Secure Access" in the *Cisco Identity Services Engine Administrator Guide, Release 3.3*.

Bulk update and bulk delete support for context-in API in pxGrid Cloud

From Cisco ISE release 3.3, you have context-in API support in pxGrid Cloud for bulk updation and bulk deletion of endpoints. For more information, see the Cisco ISE API Reference Guide.

Certificate-based authentication for API calls

From Cisco ISE release 3.3, you can configure authentication settings for API admin users such as API admin and OpenAPI admin in the **Admin** > **System** > **Admin Acess** > **Authentication** > **Authentication Method** window. The **API Authentication Type** section allows you to permit password-based or certificate-based authentications or both. These authentication settings do not apply to REST admin users such as pxGrid REST, MnT REST, and other REST admin users. For more information, see "Enable API Service" in the chapter "Basic Setup" in the *Cisco Identity Services Engine Administrator Guide, Release 3.3*.

Cisco AI-ML rule proposals for endpoint profiling

Cisco ISE now provides profiling suggestions based on continuous learning from your networks, helping you to enhance endpoint profiling and management. You can use these suggestions to reduce the number of unknown or unprofiled endpoints in your network.

For more information, see "Cisco AI-ML Rule Proposals for Endpoint Profiling" in the chapter "Asset Visibility" in the *Cisco Identity Services Engine Administration Guide, Release 3.3*.

Configure Native IPsec in Cisco ISE

From Cisco ISE release 3.3, you can configure IPsec using **Native IPsec** configuration. You can this to establish security associations between Cisco ISE PSNs and NADs across an IPSec tunnel using IKEv1 and IKEv2 protocols. For more information, see "Configure Native IPSec on Cisco ISE" in the chapter "Secure Access" in the *Cisco Identity Services Engine Administrator Guide, Release 3.3*.

Disable endpoint replication to all nodes in a Cisco ISE deployment

From Cisco ISE release 3.3, dynamically discovered endpoints are not replicated to all the nodes in the Cisco ISE deployment automatically. You can choose to enable or disable the replication of dynamically discovered endpoints across all nodes in your Cisco ISE deployment. For more information, see "Data Replication from Primary to Secondary Cisco ISE Nodes" in the chapter "Deployment" in the *Cisco Identity Services Engine Administrator Guide, Release 3.3*.

Data Connect

From Cisco ISE release 3.3, the Data Connect feature uses the admin certificate to provide database access to Cisco ISE using an Open Database Connectivity (ODBC) or Java Database Connectivity (JDBC) driver, so that you can directly query the database server to generate reports of your choice. For more information, see "Data Connect" in the chapter "Basic Setup" in the *Cisco Identity Services Engine Administrator Guide, Release 3.3*.

Enhanced support for unvalidated operating systems releases in posture workflows

Cisco ISE now supports unvalidated versions of operating systems in agent-based and agentless posture workflows. In the earlier releases of Cisco ISE, only the endpoints that ran validated operating systems successfully met posture agent policies.

As a result, endpoints running an unvalidated operating system failed posture agent workflows with the error message, **The operating system is not supported by the server**.

For information on supported operating systems, see the Compatibility Matrix for your Cisco ISE release.

For example, posture agent flows for endpoints running operating system versions Windows 10 IoT Enterprise LTSC or Mac 14 failed while these operating system versions were not validated. When Cisco ISE validated these versions and the operating system data was published to the Feed Service, posture agents successfully matched these endpoints.

You can download the latest operating system data to Cisco ISE from the Feed Service in the **Administration** > **System** > **Posture** > **Updates** page of the Cisco ISE administration portal.

From Cisco ISE release 3.3, unvalidated operating systems are matched to a known operating system listed in the Policy pages (Posture, Requirements, and Conditions pages) of the Cisco ISE administration portal, so that posture agent workflows can be completed successfully. For example, if Mac xx is not validated and an endpoint is running it, a posture agent can now match the endpoint with MacOSX. When Mac xx is validated and published to the Feed Service, and the posture agent runs on the endpoint again, the endpoint is matched with Mac xx. Posture reports display the operating system that an endpoint is matched with.

All the posture agents that are supported by Cisco ISE release 3.3 are impacted by this change. No other Cisco ISE features, such as BYOD, are impacted.

ERS API support for LDAP profile bind account password

From Cisco ISE release 3.3, LDAP profile bind account password is supported by ERS APIs. You can configure a new LDAP server on the Cisco ISE GUI using the ERS API. The created LDAP server can be used to configure an identity source in other Cisco ISE portals. For more information, see the Cisco ISE API Reference Guide.

IPv6 support for agentless posture

Cisco ISE release 3.3 adds IPv6 support for agentless posture. Windows and MacOS clients are currently supported.

For more information, see "Agentless Posture" in the chapter "Compliance" in the *Cisco Identity Services Engine Administrator Guide, Release 3.3*.

IPv6 support for portal and profiler features

Cisco ISE release 3.3 adds IPv6 support for the following portals, portal features, and profiler features.

Cisco ISE portals with IPv6 support

- Sponsor Portal
- MyDevices Portal
- Certificate Provisioning Portal
- Hotspot Guest Portal
- Self-Registered Guest Portal

Cisco ISE portal features with IPv6 support

- Single-Click Sponsor Approval
- Grace Period
- Validation of Credentials for Guest Portal
- Active Directory
- Guest Portal Posture Flow using Temporal Agent
- Active Directory User - Posture Flow with AnyConnect
- Dot1x User - Posture Flow with AnyConnect
- Guest and Dot1x User - Posture Flow with Temporal Agent

Profiler features with IPv6 support

- DHCP Probe
- HTTP Proble
- RADIUS Probe
- Context Visibility Services
- Endpoint Profiling



Note The static IP/hostname/FQDN field for the common task of web redirection cannot take an IPv6 address.

Link external LDAP users to Cisco ISE endpoint groups

From Cisco ISE release 3.3, you can assign external LDAP user groups to Endpoint Identity Groups for guest devices using the **Dynamic** option. For more information, see "Create or Edit Guest Types" in the chapter "Guest and Secure WiFi" in the *Cisco Identity Services Engine Administrator Guide, Release 3.3*.

Managing passwords of Cisco ISE users

From Cisco ISE release 3.3, as an internal user of Cisco ISE, you can choose to add the **Date Created** and **Date Modified** columns to the **Network Access User** table in the **Network Access Users** window. For more information, see "Cisco ISE Users" in the chapter "Asset Visbility" in the *Cisco Identity Services Engine Administrator Guide, Release 3.3*.

Multi-factor classification for enhanced endpoint visibility

You can now create nuanced authorization policies using four specific attributes from the endpoints connecting to your network. The Multi-Factor Classification (MFC) profiler uses various profiling probes to fetch four new endpoint attributes to the Cisco ISE authorization policy creation workflows: MFC Endpoint Type, MFC Hardware Manufacturer, MFC Hardware Model, and MFC Operating System.

For more information, see "Multi-Factor Classification for Enhanced Endpoint Visibility" in the chapter "Asset Visibility" in the *Cisco Identity Services Engine Administration Guide, Release 3.3*.

Navigation improvement

The Cisco ISE homepage GUI has been modified for a better user experience. When you click the menu icon at the left-hand corner of the homepage, a pane is displayed. Hovering your cursor over each of the options on the pane displays the following submenus to choose from.

- **Context Visibility**
- **Operations**
- **Policy**
- **Administration**
- **Work Centers**

Click **Dashboard** for the home page.

The left pane also contains a **Bookmarks** tab where you can save your recently viewed pages. Click the menu icon again to hide the pane.

If you log out when the left pane is displayed, and log in again, the pane continues to be displayed. However, if you log out after the pane is hidden, and log in again, you must click the menu icon for the pane to be displayed again.

You can now use the  icon on the homepage to access the **Search Pages** option to search for a new page or visit recently searched pages.

For more information, see "Administration Portal" in the chapter "Basic Setup" in the *Cisco Identity Services Engine Administrator Guide, Release 3.3*.

Option to disable specific ciphers

The **Manually Configure Ciphers List** option in the **Security Settings** window allows you to manually configure ciphers for communication with the following Cisco ISE components: admin UI, ERS, OpenAPI, secure ODBC, portals, and pxGrid.

A list of ciphers is displayed with allowed ciphers already selected. For example, if the **Allow SHA1 Ciphers** option is enabled, SHA1 ciphers are enabled in this list. If the **Allow Only**

TLS_RSA_WITH_AES_128_CBC_SHA option is selected, only this SHA1 cipher is enabled in this list. If the **Allow SHA1 Ciphers** option is disabled, you cannot enable any SHA1 cipher in this list.

For more information, see "Configure Security Settings" in the chapter "Segmentation" in the *Cisco Identity Services Engine Administrator Guide, Release 3.3*.

Posture and client provisioning support for ARM64 version of agent

From Cisco ISE release 3.3, posture policies and client-provisioning policies are supported for ARM64 endpoints. You can upload the ARM64 version of agent for ARM64 endpoints.

Note the following points while configuring an ARM64 client-provisioning policy:

- ARM64 posture policies are supported for the following:
  - Windows Agent
  - Mac Agent
  - Mac Temporal Agent
  - Mac Agentless

  Windows policies run separate packages for ARM64 and Intel architectures. Windows Temporal and Windows Agentless are not supported on ARM64 architecture, but are supported on Intel architecture.

  macOS policies run the same package for both architectures.
- ARM64 package is supported for Cisco AnyConnect VPN and Cisco Secure Client.

Note Cisco Secure Client 5.0.4xxx and later versions support posture and client-provisioning policies for ARM64 endpoints.

ARM64 compliance module 4.3.3583.8192 and later versions can be used with Cisco Secure Client 5.0.4xxx and later versions along with Cisco ISE 3.3 and later versions for ARM64 endpoints. You can download the compliance modules from the Software Download Center.

- ARM64 agent auto upgrade and compliance module upgrade are supported.
- Google Chrome and Microsoft Edge 89 and later versions support web redirection for OS Architecture conditions like ARM64, 64-bit, and 32-bit.

  Firefox browser does not support web redirection for OS Architecture conditions like ARM64, 64-bit, and 32-bit. Hence, it cannot be used to match ARM64 client-provisioning policies. The following message is displayed when you use the Firefox browser:

  ```
  ARM64 endpoints do not support Firefox browser, and there may be compatibility issues if you continue downloading this agent. We recommend that you use Chrome or Microsoft Edge browser instead.
  ```
- You cannot combine BYOD and ARM64 client-provisioning policies.
- Ensure that the ARM64 condition policy is at the top of the conditions list (listed above the policies without an ARM64 condition). This is because an endpoint is matched sequentially with the policies listed in the **Client Provisioning Policy** window.

For more information, see "Configure Client Provisioning Policy for ARM64 Version of Agent" in the chapter "Compliance" in the *Cisco Identity Services Engine Administrator Guide, Release 3.3*.

pxGrid context-in enhancements

From Cisco ISE release 3.3, you have context-in API support in pxGrid. You can create custom attributes for endpoints and use OpenAPI for context-in support. For more information, see the Cisco ISE API Reference Guide.

pxGrid Cloud support for context-in

From Cisco ISE release 3.3, you have context-in API support in pxGrid Cloud. You can create custom attributes for endpoints and use OpenAPI for context-in support. For more information, see the Cisco ISE API Reference Guide.

pxGrid Direct enhancements

pxGrid Direct is no longer a controlled introduction feature. Before you upgrade to Cisco ISE release 3.3 from Cisco ISE releases 3.2 or 3.2 patch 1, we recommend that you delete all configured pxGrid Direct connectors and any authorization profiles and policies that use data from pxGrid Direct connectors. After you upgrade to Cisco ISE release 3.3, reconfigure pxGrid Direct connectors.

Note If you do not delete the configured pxGrid Direct connectors, the connectors are automatically deleted during the upgrade. This deletion results in uneditable and unusable authorization profiles and policies that you must delete and replace with new ones.

For more information on changes to the pxGrid Direct feature, see "pxGrid Direct" in the chapter "Asset Visibility" in the *Cisco Identity Services Engine Administration Guide, Release 3.3*.

RADIUS Step Latency dashboard

The **RADIUS Step Latency** dashboard (**Log Analytics > Dashboard**) displays the maximum and average latencies for the RADIUS authentication flow steps for the specified time period. You can also view the maximum and average latencies for the Active Directory authentication flow steps (if Active Directory is configured on that node) and the Top N RADIUS authentication steps with maximum or average latencies.

For more information, see "Log Analytics" in the chapter "Maintain and Monitor" in the *Cisco Identity Services Engine Administration Guide, Release 3.3*.

Schedule application restart after admin certificate renewal

After you renew an admin certificate on the primary PAN, all the nodes in your deployment must be restarted. You can either restart each node immediately or schedule the restarts later. This feature allows you to ensure that no running processes are disrupted by the automatic restarts, giving you greater control over the process. You must schedule node restarts within 15 days of certificate renewal.

For more information, see "Schedule Application Restart After Admin Certificate Renewal" in the chapter "Basic Setup" in the *Cisco Identity Services Engine Administration Guide, Release 3.3*.

Split upgrade of Cisco ISE deployment from GUI

Split upgrade is a multistep process that enables the upgrade of your Cisco ISE deployment while allowing other services to be available for users. The downtime can be limited in a split upgrade by upgrading the nodes in iterations or batches.

For more information, see "Split Upgrade of Cisco ISE Deployment from GUI" in the chapter "Perform the Upgrade" in the Cisco Identity Services Engine Upgrade Guide, *Release 3.3*.

Ukrainian language support in portals

Guest, Sponsor, My Devices, and Client Provisioning portals now include Ukrainian as a supported localization language.

Wi-Fi device analytics data from Cisco Catalyst 9800 Wireless LAN Controller

You can create profiling policies, authorization conditions, and authentication conditions and policies for Apple, Intel, and Samsung endpoints, using device analytics data from the Cisco Wireless LAN Controllers (WLCs) integrated with your Cisco ISE.

For more information, see "Wi-Fi Device Analytics Data from Cisco Catalyst 9800 Wireless LAN Controller" in the chapter "Asset Visibility" in the Cisco Identity Services Engine Administration Guide, *release 3.3*.

Deprecated features

Locking identities with repeated authentication failures

From Cisco ISE release 3.3 patch 4, **Identity Lock Settings** are not supported in the **RADIUS Settings** page (**Administration > System > Settings > Protocols > RADIUS**).

Configuring RSA or RADIUS external databases for API authentication

From Cisco ISE release 3.3 patch 3, configuring RSA or RADIUS external databases for API authentication is no longer supported.

New and changed APIs in Cisco ISE

For detailed information on new, changed, and deprecated APIs, see the Cisco ISE API Guide on Cisco DevNet.

Known limitations and workarounds

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

Known limitations in Cisco ISE release 3.3 cumulative patch 12

Change in negation operator evaluation for null attributes

You may notice a change in how your policies are evaluated when using negation operators, such as "Not Equals." If either the left-hand side (LHS) or right-hand side (RHS) attribute resolves to a null value, Cisco ISE now returns false, whereas it previously returned true. You can verify this by checking your policy-engine debug logs for the message: "Either of LHS or RHS value is null (undefined), evaluation result = false." This change could cause your existing policies to be deselected or fail to match as they did previously.

To restore the original behavior for these conditions, you can update your affected policy rule by changing the operator from "Not Equals" to "Equals" and selecting the "is-not" option in the Cisco ISE GUI. By making this adjustment, your policy continues to function as you intend, maintaining consistent evaluation logic despite the updated handling of null attributes in negation operations.

Refer to CSCws89421 for more information.

SSH host key mismatch after upgrading a Cisco ISE cloud deployment

When you upgrade an existing Cisco ISE cloud deployment, patch installation changes the SSH host key. The affected releases are:

- Cisco ISE release 3.3 patch 12 or later.
- Cisco ISE release 3.4 patch 7 or later.
- Cisco ISE release 3.5 patch 4 or later.

If your systems store the SSH public host keys of the deployment nodes in the **known_hosts** file, the first SSH connection after the upgrade might display a host key mismatch warning.

To connect to Cisco ISE through SSH, remove or update the existing Cisco ISE host key entry in the **known_hosts** file.

Known limitations in Cisco ISE release 3.3 cumulative patch 11

Patch installation becomes unresponsive on Cisco ISE release 3.3 patch 11 in MET time zones

If you are installing Cisco ISE release 3.3 patch 11 on a node configured with the MET time zone, you may encounter an unresponsive state during the "Applying database patch" phase. This is because the JRE bundled with the updated OPatch utility (version 12.2.0.1.45) does not recognize legacy POSIX 3-letter time zone abbreviations, such as MET or MEST, found in the Oracle inventory files. As a result, the patch installation process enters an infinite retry loop when it attempts to parse these timestamps, causing the installation to stall indefinitely.

You must install this hotpatch before installing Cisco ISE release 3.3 patch 11.

Refer to CSCwu17372 for more information.

Known limitations in Cisco ISE release 3.3 cumulative patch 10

Reports show up empty after upgrade

If Cisco ISE release 3.3 patch 10 is installed on top of Cisco ISE release 3.3 patch 8 or Cisco ISE release 3.3 patch 9, then the **Change Configuration Audit**, **Posture-related report**, and **Active Directory Operations report** appear empty.

Known limitations in Cisco ISE release 3.3 cumulative patch 8

Authentication and authorization policy evaluation issue with null attributes

An issue has been identified where authentication and authorization is successful even when both the left-hand side (LHS) and right-hand side (RHS) attributes within an authentication or authorization policy condition resolve to null values. When the **Equal** operator is applied to these null attributes, Cisco ISE incorrectly evaluates the policy condition as true, which can result in unintended policy enforcement and potential security gaps.

As a workaround, avoid configuring authentication and authorization policy rules that rely on attributes prone to resolving to null values.

Policy rules must be designed to prevent scenarios where both the LHS and RHS attributes evaluate to null simultaneously, thereby maintaining the intended security posture of the authentication or authorization policy. This would restore the intended security posture and prevent the unintended policy enforcement caused by CSCwo12680.

Refer to CSCwo12680 for more information.

Cisco ISE on cloud vulnerability fix

When upgrading to Cisco ISE release 3.3 patch 8 from patch 1, patch 2, or any other Cisco ISE release, Cisco ISE will perform a mandatory restart of internal services upon login. This restart is required to address the vulnerability identified in CSCwn63400. This fix is applicable only to cloud deployments. To fully apply the fix, you must synchronize all the nodes in your deployments with the PAN using one of these options:

- **Proceed with Auto Sync**: All nodes will be restarted to ensure immediate synchronization and application of the fix. You can verify the synchronization status of nodes in your deployment in the **Deployment Nodes** page (**Administration** > **System** > **Deployment**). We recommend this option to ensure automatic synchronization across all nodes.
- **Proceed with Manual Sync**: After the restart, you must manually synchronize all nodes as soon as possible to prevent desynchronization. If nodes are desynchronized, you must deregister, reset the configuration, and then register the nodes again to resolve the issue.



Attention Manual synchronization is critical to maintain deployment integrity after the mandatory restart. Without timely manual sync, key features such as endpoint database updates and certificate-based authentications will fail due to configuration mismatches.

- **Decide Later**: Options for fixing the vulnerability will be available to you at your next login.

Note This requirement does not apply if you have installed the latest Cisco ISE release 3.3 patch 7 AMI before upgrading to Cisco ISE release 3.3 patch 8 and later releases.

Known limitations in Cisco ISE release 3.3 cumulative patch 7

Log Analytics initialization issue after upgrade from Cisco ISE release 3.3 patch 7

After upgrading from Cisco ISE release 3.3 patch 7 to Cisco ISE release 3.4 patch 3, you may find the application server stuck in an "initializing" state. This occurs because the Kibana migration fails when it encounters unrecognized telemetry objects from previous releases. You can resolve this by manually deleting the problematic document and temporarily modifying the Kibana configuration to allow the migration to complete. Refer to the instructions in the workaround section of CSCwt07284.

Known limitations in Cisco ISE release 3.3 cumulative patch 4

Special character support for password repository

Special characters such as ?, /, ,, %, <, and > are not supported for repository passwords and are not accepted in the Cisco ISE GUI or CLI.

Usage of special characters in osquery visibility condition

When an equal-to operator is used with special characters for attribute values (for example, CPU @ 1.20GH), the osquery visibility condition fails. As a workaround, you can use the Like operator (is_containing) for configuring osquery visibility conditions with special characters.

Add posture remediation script to a requirement

To add a script condition to a client posture requirement, you must create the new script condition from the **Client Posture Requirements** page (**Policy > Policy Elements > Results > Posture > Requirements**) and use the **Save and Select** option to add the newly created script condition to the requirement.

Known limitations in Cisco ISE release 3.3 cumulative patch 1

Cisco ISE restart limitation with disabled pxGrid Direct connectors

Restarting Cisco ISE when there are disabled pxGrid Direct connectors causes problems with scheduling sync operations using pxGrid Direct connectors following the restart. We recommend that you to enable all disabled pxGrid Direct connectors before restarting Cisco ISE, and disable the connectors again following the restart. Alternatively, you could also edit the attributes of the disabled connector (making it an active connector) prior to the Cisco ISE restart as a workaround to this problem.

This problem has been resolved in Cisco ISE release 3.2 cumulative patch 5 and Cisco ISE release 3.3 cumulative patch 2.

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*.

Verified hardware

Cisco ISE 3.3 can be installed on the following Secure Network Server (SNS) hardware platforms:

Table 2: Verified platforms

Hardware Platform	Configuration
Cisco SNS-3615-K9 (small)	For appliance hardware specifications, see the *Cisco Secure Network Server Appliance Hardware Installation Guide*.
Cisco SNS-3655-K9 (medium)	
Cisco SNS-3695-K9 (large)	
Cisco SNS-3715-K9 (small)	
Cisco SNS-3755-K9 (medium)	
Cisco SNS-3795-K9 (large)	
Cisco SNS-3815-K9 (small)	
Cisco SNS-3855-K9 (medium)	
Cisco SNS-3895-K9 (large)	

Note

- Cisco SNS 3800 appliances are supported from Cisco ISE release 3.3 patch 7 onwards.
- Note that the filenames of the OVA templates have been changed in Cisco ISE Release 3.3.

The following OVA templates can be used for SNS 3600 series appliances:

OVA Template	ISE Node Size
Cisco-vISE-300-3.3.0.430.ova	Evaluation
	Extra Small
	Small
	Medium
Cisco-vISE-600-3.3.0.430.ova	Small
	Medium
Cisco-vISE-1200-3.3.0.430.ova	Medium
	Large

OVA Template	ISE Node Size
Cisco-vISE-1800-3.3.0.430.ova	Large
Cisco-vISE-2400-3.3.0.430.ova	Large

The following OVA templates can be used for both SNS 3600 and SNS 3700 series appliances:

OVA Template	ISE Node Size	
Cisco-vISE-300-3.3.0.430a.ova	Evaluation	300-Eval
	Extra Small	300-ExtraSmall
	Small	300-Small_36xx
		300-Small_37xx
	Medium	300-Medium_36xx
		300-Medium_37xx
Cisco-vISE-600-3.3.0.430a.ova	Small	600-Small_36xx
		600-Small_37xx
	Medium	600-Medium_36xx
		600-Medium_37xx
Cisco-vISE-1200-3.3.0.430a.ova	Medium	1200-Medium_36xx
		1200-Medium_37xx
	Large	1200-Large_36xx
		1200-Large_37xx
Cisco-vISE-2400-3.3.0.430a.ova	Large	2400-Large_36xx
		2400-Large_37xx

Cisco SNS 3595 is not supported for Cisco ISE 3.3 and later releases. For more information, see End-of-Life and End-of-Sale Notices.

You cannot install or upgrade to Cisco ISE 3.3 or later releases using a Cisco SNS 3595 appliance. Virtual appliances with Cisco SNS 3595 profile must be migrated to Cisco SNS 3655 profile. To migrate the profile, you must take the backup of the node, install Cisco ISE 3.3 using Cisco SNS 3655 profile, and then restore the backup of Cisco SNS 3595 profile on this node.

Note If you are upgrading from Cisco ISE 3.2 or earlier releases to Cisco ISE 3.3 using Cisco SNS 3595 profile, the node will be profiled as Cisco SNS 3615 in Cisco ISE 3.3. Hence, the performance of the node will be degraded.

Verified virtual environments

Cisco ISE supports these virtual environment platforms:

Table 3: Verified virtual environments

Virtual environment	Support details
VMware	• ISO files support ESXi 7.0, ESXi 8.0, and ESXi 9.0. • OVA templates support VMware version 14 or later on ESXi 7.0, ESXi 8.0, and ESXi 9.0. • In the case of vTPM devices, you must upgrade to VMware ESXi 7.0.3 or later releases. • You can use the VMware migration feature to migrate VM instances (running any persona) between hosts. Cisco ISE supports both hot and cold migration. Hot migration is also called live migration or **vMotion**. Cisco ISE need not be shut down or powered off during the hot migration. You can migrate the Cisco ISE VM without any interruption in its availability.
VMware Cloud Solutions on public cloud platforms	• AWS: Host Cisco ISE on a software-defined data center provided by VMware Cloud on AWS. • Azure VMware Solution: Runs VMware workloads natively on Microsoft Azure. • Google Cloud VMware Engine: Runs software-defined data center by VMware on Google Cloud.
Microsoft Hyper-V	• Supports Microsoft Windows Server 2012 R2 and later. • Supports Azure Stack HCI 23H2 and later. The virtual machine requirements and the installation procedure for the Cisco ISE VMs in the Azure Stack HCI are the same as that of Microsoft Hyper-V.
KVM on QEMU	• Supports QEMU 2.12.0-99 and later.
Nutanix	• Supported and verified Nutanix versions: AOS 7.3.1.7 AVH 10.3.1.7, AOS 7.5.1.2 AVH 11.0.1.1, AOS 7.5.0.6 AVH 11.0.0.2, AOS 7.0 AHV 10.0, AOS 6.8 AHV 20230302.100169, AOS 6.5.2.7 AHV 20220304.392.

Virtual environment	Support details
Public cloud platforms	• Native support for Amazon Web Services (AWS), Microsoft Azure Cloud, and Oracle Cloud Infrastructure (OCI).
Red Hat OpenShift	• Red Hat OpenShift container platform 4.19 and later. • Cisco ISE must be deployed on OpenShift platform using the standard Cisco ISE ISO image. Deploying Cisco ISE using OVA templates is not supported.

Verified and supported browsers

Cisco ISE release 3.3 is supported on these browsers:

- Mozilla Firefox versions 123, 125, 128, 136, 138, 139, 145, 146, and 147
- Google Chrome versions 126, 127, 134, 135, 137, 139, 140, 141, and 142
- Microsoft Edge versions 122, 124, 125, 128, 134, 135, 140, 141, and 142



Restriction Currently, you cannot access the Cisco ISE GUI on mobile devices.

Verified external identity sources

Table 4: Verified external identity sources

External identity source	Version
Active Directory The supported Active Directory versions are the same for both Cisco ISE and Cisco ISE-PIC.	
Microsoft Windows Active Directory 2016	Windows Server 2016
Microsoft Windows Active Directory 2019	Windows Server 2019
Microsoft Windows Active Directory 2022	Windows Server 2022 with Patch Windows10.0-KB5025230-x64-V1.006.msu
Microsoft Entra ID	—
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

External identity source	Version
AD as LDAP	Windows Server 2022 with Patch Windows10.0-KB5025230-x64-V1.006.msu
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

Verified antivirus and antimalware products

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

Verified OpenSSL version

Cisco ISE release 3.3 is verified with OpenSSL 1.1.1x and CiscoSSL 7.3.375.

OpenSSL update requires CA:True in CA certificates

For a certificate to be defined as a CA certificate, the certificate must contain the following property:

basicConstraints=CA:TRUE

This property is mandatory to comply with recent OpenSSL updates.

Upgrade information

Cisco ISE on cloud

Native cloud environments must use the Cisco ISE backup and restore method for upgrades. Upgrades cannot be performed on Cisco ISE nodes deployed in native cloud environments. You must deploy a new node with a newer version of Cisco ISE and restore the configuration of your older Cisco ISE deployment onto it. For more information, see Deploy Cisco Identity Services Engine Natively on Cloud Platforms.

Upgrading to Release 3.3

You can directly upgrade to Release 3.3 from the following Cisco ISE releases:

- 3.0
- 3.1
- 3.2

If you are on a version earlier than Cisco ISE Release 3.0, you must first upgrade to one of the releases listed above, and then upgrade to Release 3.3.

Cisco ISE patches are cumulative and we recommend that you upgrade to the latest patch in the existing release before starting the upgrade. We recommend that you install all the relevant patches before beginning the upgrade. For more information, see the Cisco Identity Services Engine Upgrade Guide.

Cisco SNS 37x5 appliance firmware upgrade

Before upgrading your Cisco SNS 37x5 appliance firmware from 4.x to 6.x, you must install the ise-apply-CSCwu00192_3.4_patchall-SPA.tar.gz hot patch if you are using Cisco ISE release 3.3 patch 11 or earlier versions. This step is mandatory and must be completed before starting the firmware upgrade process.

After the BIOS and HUU upgrades complete successfully, verify the TPM firmware as follows:

1. In the CIMC web UI, navigate to **Chassis > Inventory > TPM**.
2. If the TPM firmware version is 7.86 or later, no further action is required.

   If the version is 7.85 or earlier:

   a. Stop Cisco ISE services if the OS has booted.

   b. In the CIMC web UI, navigate to **Host Power > Power Cycle**.

   c. After the CIMC reboots, verify that the TPM firmware version is now 7.86 or later.

This issue is resolved in Cisco ISE release 3.3 patch 12. If you are running this patch or a later version, you do not need to install the hot patch. However, you must verify the TPM firmware and perform a reboot if the TPM firmware version is 7.85 or earlier.

Upgrade packages

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

Cisco ISE Release 3.3 upgrade bundle files have been replaced on the Cisco ISE Software Download site.

This entails:

- resolution of bugs CSCwj43362 and CSCwj55392.
- that the filenames of the new files will have "b" appended to the build number (for example, ise-upgradebundle-3.0.x-3.2.x-to-3.3.0.430b.SPA.x86_64.tar.gz).
- that existing Cisco ISE Release 3.3 cumulative patches will continue to work with this new upgrade bundle.

Cisco ISE integration with Cisco Catalyst Center

Cisco Catalyst Center

Cisco ISE can integrate with Cisco 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*.

Install a new patch

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*.

Changes in behavior

Changes in behavior in Cisco ISE release 3.3 cumulative patch 12

Table 5: Changes in behavior in Cisco ISE release 3.3 patch 12

Identifier	Description
CSCws89421	You may notice a change in how your policies are evaluated when using negation operators, such as "Not Equals." If either the left-hand side (LHS) or right-hand side (RHS) attribute resolves to a null value, Cisco ISE now returns false, whereas it previously returned true. You can verify this by checking your policy-engine debug logs for the message: "Either of LHS or RHS value is null (undefined), evaluation result = false." This change could cause your existing policies to be deselected or fail to match as they did previously. To restore the original behavior for these conditions, you can update your affected policy rule by changing the operator from "Not Equals" to "Equals" and selecting the "is-not" option in the Cisco ISE GUI. By making this adjustment, your policy continues to function as you intend, maintaining consistent evaluation logic despite the updated handling of null attributes in negation operations. Refer to CSCwo12680 for more information.
CSCwt68081	The **identity-store active-directory** command now supports an optional organizational-unit parameter when joining Cisco ISE to Active Directory. If provided, the Cisco ISE machine account is created in the specified organizational unit; otherwise, it is created in the default Computers organizational unit. The existing command can still be used without the optional parameter.
CSCws27786	Cisco ISE now supports joining Active Directory domains hosted on Windows Server 2025 and rotating the machine-account password by using the Kerberos Change Password protocol instead of legacy SAM RPC password-change methods.
OCSP validation for pxGrid client certificates	From Cisco ISE release 3.3 patch 12, Cisco ISE applies certificate status validation during pxGrid client authentication. Certificate status validation includes Online Certificate Status Protocol (OCSP) and certificate revocation list (CRL) validation. Cisco ISE first validates the certificate chain and then applies the existing validation policy for the issuing trusted certificate authority. Before this patch, Cisco ISE did not apply this policy during pxGrid client certificate authentication. This change does not require pxGrid-specific certificate status validation configuration. After the upgrade, a pxGrid integration might fail if its client certificate does not satisfy the configured certificate status validation policy. Before you upgrade, verify the certificate trust chain and certificate status validation settings for each certificate-based pxGrid integration. For configuration details, refer to Trusted Certificate Settings. Confirm that the OCSP or CRL responder reports each active pxGrid client certificate as GOOD. After the upgrade, reconnect each integration and use the pxGrid Live Log to verify successful certificate validation.

Identifier	Description
Stricter DNS SAN validation for node synchronization	From Cisco ISE release 3.3 patch 12, stricter DNS Subject Alternative Name (SAN) validation applies to bulk synchronization between nodes. After installing this patch in a multinode deployment, nodes might appear as 'Out of Sync' if the Admin certificate does not contain the node's fully qualified domain name (FQDN) as an exact DNS SAN entry or as a matching wildcard DNS SAN entry. To restore synchronization, deregister the affected nodes, update their Admin certificates, and replace the certificate on the Primary PAN first and then on each remaining node, one at a time. Confirm that synchronization is complete before proceeding to the next node. Refer to CSCww70696 for more information.

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 3.3. A caveat that is open for an earlier release and is still unresolved applies to all future releases until it is resolved.

Resolved caveats

Resolved caveats in Cisco ISE release 3.3 cumulative patch 12

Identifier	Headline
CSCwq91090	ERS NAD creation, update, or CSV import changes the identity store version.
CSCwt39843	Race condition triggers CoA when the MFC profiler is enabled.
CSCwu39084	Changes to the MTU configuration on GigabitEthernet are not applied at the OS level on an SNS device.
CSCwr39748	Cisco ISE scheduled and GUI backups stop working 5 to 6 days after a reload.
CSCwu65848	Monitoring database reset fails in Cisco ISE release 3.3 patch 11.
CSCws65812	PassiveID Agent fails to start on appliances with more than 25 CPU cores in Cisco ISE release 3.3 patch 8.
CSCwp63632	TACACS+ policy evaluation starts before all details are received.
CSCwv27442	Cisco ISE GUI remains on the loading page after session termination or a CoA request to a RADIUS DTLS device from CV.
CSCwu38974	Profiling fails for Cisco 8875 IP phones in Cisco ISE release 3.3 patch 6.

Identifier	Headline
CSCwk60765	High update volume from the AI Endpoint Analytics application on Cisco Catalyst Center causes high load on Cisco ISE nodes.
CSCwo84190	Allow configuration of accounting suppression behavior through the Cisco ISE GUI.
CSCwt93380	New connections cannot be established because 1,000 processes are in use.
CSCwt57041	Used Memory is calculated incorrectly after the change introduced in CSCwo71490.
CSCwq31233	Encrypt the shared secret key in network device exports from Cisco ISE.
CSCwt94400	Support new DISA DATT COAMS registry keys and legacy keys in Cisco ISE C2C reporting.
CSCws27786	Support Microsoft Active Directory domains hosted on Windows Server 2025.
CSCwr71709	New network devices cannot be added to Network Device conditions.
CSCwv00262	Installing patch 10 or patch 11 on Cisco ISE release 3.3 after encountering CSCwo80728 does not clear the MnT tablespace.
CSCws93917	“Admin thread pool reached threshold value” alerts appear on the Cisco ISE dashboard.
CSCwu96902	CA service remains in the Initializing state after restoring a backup from a SAN node in Cisco ISE release 3.5 patch 3.
CSCwu00192	Cisco ISE services do not start because TPM2ManagerServer initialization fails after a firmware upgrade.
CSCwu05826	Cisco Identity Services Engine Path Traversal Vulnerability.
CSCwu50515	MnT Collector NullPointerException causes “Log collection error: Log Type=Posture” alarms.
CSCwt76507	Upgrade staging times out after node reregistration and Admin or Portal certificate replacement in Cisco ISE release 3.4 patch 6.
CSCwu56865	Cisco ISE REST identity store user lookup does not return results when a group name contains “error” or a UPN contains an apostrophe.
CSCwu55972	Cisco ISE release 3.4 patch 5 stops sending logs to an external syslog server.
CSCwq70326	Admin Portal certificate changes do not take effect on the Primary PAN in Cisco ISE release 3.4.
CSCwk47648	Cisco ISE uses the hmac-sha2-256 and hmac-sha2-512 algorithms and fails to connect to an external device through SSH.
CSCwu17372	Patch installation hangs at “Applying database patch...” in Cisco ISE release 3.3 patch 10.
CSCwt81227	Cisco ISE release 3.x does not generate an alarm when the connection to the ODBC database fails.

Identifier	Headline
CSCwn53284	Admin certificate changes remain in the Saving state when a non-English browser is used.
CSCwu32618	CA service remains in the Initializing state because db_key.txt is not TPM-encrypted during patch installation in Cisco ISE release 3.4 patch 4 or later.
CSCwo53551	Cisco ISE swap space must be increased based on the available RAM.
CSCwt35322	IP-to-SGT binding deployment through SSH fails when Enable Mode Password is configured.
CSCwr03082	Cluster instability causes endpoint count discrepancies and shard failures.
CSCwt68081	Support organizational unit configuration in the Active Directory CLI.
CSCwu61717	MFC profiler service remains in the Not Running state on a PSN after an upgrade to Cisco ISE release 3.4 patch 6.
CSCws12274	Export of TrustSec-enabled network devices still fails after the CSCwk80440 fix.
CSCwt15886	KPM database query takes 19 minutes to complete.
CSCws89421	Block only null-to-null comparisons during policy evaluation.
CSCwp62979	Kong directory should be updated on every reload.
CSCwt96506	RevisedOUI.csv file is missing in Cisco ISE nodes when it is newly added or re-registered to the deployment.
CSCwv82427	Meraki connector integration is not successful.
CSCww16252	In Cisco ISE release 3.3 patch 12, ERS and OpenAPI endpoints fail when an external admin user invokes them.
CSCww39530	Cisco Identity Services Engine Authentication Bypass Vulnerability

Resolved caveats in Cisco ISE release 3.3 cumulative patch 11

Identifier	Headline
CSCwe48929	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerability.
CSCwp06144	Network device update API fails if previous shared secret expiry attribute is set to zero.
CSCwp98770	Cisco Identity Services Engine Authenticated Privilege Escalation Vulnerability.
CSCwr02280	When RMQ is not running or is initializing, the LSD queue increases in size.
CSCwr05052	Proxy bypass is not working for CRL retrieval in Cisco ISE release 3.4 patch 2 and patch 3.

Identifier	Headline
CSCwr49928	Unable to login to CLI post Cisco ISE release 3.5 installation with $ sign in admin SSH password.
CSCwr50566	The database server does not start after an Oracle crash.
CSCws25187	The system received a delayed CoA event that is not registered in the handlers.
CSCws33500	Telemetry queries cause high CPU or load on MnT nodes.
CSCws52717	Cisco Identity Services Engine Path Traversal Vulnerability.
CSCws52738	Cisco Identity Services Engine Remote Code Execution Vulnerability.
CSCws83036	Impact assessment of client authentication EKU enforcement in Cisco ISE.
CSCwt00836	Pre-checks fail with an error: "Error in triggering the Pre-checks: Please check connectivity between the specified nodes and PPAN.
CSCwt10926	The iPSK authorization profiles lose PSK value and duplicate psk-mode after editing.
CSCwt13149	NADs fail to load during service start up when a TrustSec HTTPS internal account is missing.

Resolved caveats in Cisco ISE release 3.3 cumulative patch 10

Identifier	Headline
CSCws76788	ConfD failed to start, which caused the node to become unavailable.
CSCws33285	The disabling and saving functionality for SMTP server settings is not handled correctly with the OAuth implementation.
CSCws61409	Live logs are not displayed in the graphical user interface due to rapid expansion of the MNT database.
CSCws65894	A warning should be displayed when enabling dynamic endpoint replication to inform users that manual synchronization is required.
CSCws33324	The nodes in the deployment are displayed as unreachable after configuring SMTP OAuth settings.
CSCwt23394	Unable to view posture reports after the upgrade due to a regression caused by the resolution of CSCwo80728.
CSCwt04886	Secondary PAN remains stuck in the synchronization stage during the split upgrade process.
CSCws52326	After patch installation, Cisco ISE fails to evaluate the custom attributes used in authorization rules.
CSCwt14016	CA service is unresponsive after you perform a rollback operation from the Cisco ISE CLI.

Resolved caveats in Cisco ISE release 3.3 cumulative patch 9

Identifier	Headline
CSCws51319	After upgrading to Cisco ISE release 3.3 patch 8, network access devices cannot download SGACLs from Cisco ISE.

Resolved caveats in Cisco ISE release 3.3 cumulative patch 8

Identifier	Headline
CSCvu20380	Add an option to set the DF bit to 0 on Cisco ISE, either through the CLI or the GUI.
CSCvv38637	Cisco ISE to use cisco.com hostnames for AMP services.
CSCvz00208	The wildcard domain list in proxy bypass does not work for CRL retrieval.
CSCvz86243	Change configuration audit detail report is empty.
CSCwe11092	MDM connection reset is reflecting false certificate alarm.
CSCwe48929	Cisco ISE sensitive information disclosure vulnerability.
CSCwf24983	In Cisco ISE release 3.3, the BH CLI banner remains present even after removal using admin access.
CSCwh61339	When you attempt to export more than 90,000 network devices, the operation times out.
CSCwh77618	Cisco ISE RMQ is full when high latency exists between Cisco ISE nodes and EPO is enabled.
CSCwi29623	Read-only users (local or AD) cannot view scheduled backup configuration details in Cisco ISE release 3.1 patch 7.
CSCwi57812	Cisco ISE release 3.2 is listening on TCP port 67.
CSCwi78093	The diagRunner processes are listening on Cisco ISE service ports.
CSCwj33565	Cisco ISE arbitrary file upload vulnerability.
CSCwj84894	Implement a custom 400 error message for Cisco ISE.
CSCwj94952	The prometheus.log file shows "Scrape failed" with "context deadline exceeded".
CSCwj97837	Oracle processes crash on MnT nodes due to long list of arguments.
CSCwk81421	Guest authentication fails due to delayed remote updates to the profiler Oracle database.
CSCwk89230	Users are unable to view IP addresses from access restrictions in Cisco ISE.
CSCwm00177	Unable to activate the log filter for the pxGrid component.
CSCwm26817	A duplicate FQDN entry appears after changing the IP address in reset-config.

Identifier	Headline
CSCwm41230	In Cisco ISE release 3.3 patch 3, resetting the MnT database corrupts all databases.
CSCwm42509	Unable to activate the Cisco AI Analytics engine due to restricted access to the AI agent container IP address.
CSCwm42629	In Cisco ISE release 3.2 patch 4, the PSN does not fully handle authentication after a reload or patch installation.
CSCwm43211	Cisco ISE reports incorrect latency for the RequestLatency and TotalAuthenLatency attributes in RADIUS accounting.
CSCwm56598	The Cisco ISE operational data purging Save button does not respond when selected.
CSCwm65380	Highload avarage alarm seen on MnT nodes.
CSCwm78749	Cisco ISE certificate authentication attributes are not propagated to the MDM compliance check flow.
CSCwm87014	Unable to delete identity groups, profiling policies, or conditions due to stale references.
CSCwn01410	Secondary Cisco ISE nodes cannot download files larger than 1 gigabyte (GB) through local disk management.
CSCwn06311	TrustSec HTTP credentials configuration is lost on a CoA NAK or timeout.
CSCwn09816	RADIUS shared secret masking after a switch reload causes authentication failures.
CSCwn15744	Audit log Jedis connection failures.
CSCwn46372	Log and dump files are unavailable during database export.
CSCwn46759	In Cisco ISE release 3.3, the profiler queue size limit is reached, preventing guest endpoints from being added to the identity group.
CSCwn51058	In Cisco ISE release 3.3, the rabbitmq log does not rotate and causes high disk space utilization.
CSCwn54934	Faulty behavior occurs when a Nonexistent per-user dACL is used in the VPN and posture flow.
CSCwn56909	Cisco ISE should send the FQDN in the SMTP EHLO message instead of the hostname.
CSCwn62873	Cisco ISE fails to join Microsoft Active Directory (AD) domains that are hosted on Windows Server 2025.
CSCwn63400	Cisco ISE on cloud installs contain a static internal-comm-user password.
CSCwn76571	Increase the timeout for scripts in posture conditions.
CSCwn76670	TrustSec does not send the CoA on the configured port. The guest password policy cannot be changed.

Identifier	Headline
CSCwn87051	The EventManager ExponentialRetryScheduler mechanism could lead to memory exhaustion.
CSCwn87602	The Cisco ISE ERS POST-create-internaluser operation using passwordIDStore fails intermittently.
CSCwn88214	Unable to update the 'Use Customization From' field in the guest type configuration in Cisco ISE.
CSCwn90693	In Cisco ISE release 3.2 patch 7, adding a sponsor group does not replicate the guest type.
CSCwn90896	The Network Access user's password is set to internal if the user is removed from the administrator list.
CSCwn93673	Disable DockerMetrics monitoring and logging.
CSCwn95991	Display a warning message when configuring the local log settings retention period in the Cisco ISE GUI.
CSCwn97429	Copying to or from SFTP fails with a timeout.
CSCwn99120	In Cisco ISE release 3.3, endpoint deletion fails when using the MyDevice portal.
CSCwo00935	The consumption count is not updated in the License_count table.
CSCwo01630	Cisco ISE AD (lwsmd) is stuck at "Updating" and consumes 90–100% CPU even after CSCwh72754 fix.
CSCwo02954	You cannot change the guest password policy.
CSCwo05386	Cisco ISE seeing alarms for the Baltimore CyberTrust Root internal certificate expiring.
CSCwo08869	The username suffix on the REST ID Store page does not accept special characters.
CSCwo09189	The SNMP service fails to start.
CSCwo11593	Unable to register the node when a hostname alias has an exaclamation mark.
CSCwo11599	The pxGrid Direct connector test connection fails with an invalid URL.
CSCwo11703	Cisco ISE disk fills up as the log rotation does not occur for the ctr.log file running in Podman containers.
CSCwo12471	The authentication or authorization policy is not visible under the policy set.
CSCwo12680	The system authenticates successfully even though both the LHS and RHS attributes are transformed to null values.
CSCwo14546	There is a limitation on creating more than 1,000 endpoint and user identity groups.
CSCwo16216	After you change the minimum length for the admin password policy, the page alternates between the Reset Password and Login screens after logout.

Identifier	Headline
CSCwo19583	High load caused by live log counter queries.
CSCwo22413	The guest flow with a grace period breaks when a customized portal is used.
CSCwo28647	Retained terminated sessions cause the publication of misinformation.
CSCwo30943	The pxGrid Direct connector URL escape needs to be changed.
CSCwo31020	RSA key fails to regenerate.
CSCwo32843	Duplicate custom field values are allowed in guest settings.
CSCwo34645	System 360 monitoring disk latency numbers are too high.
CSCwo35315	nslookup returns an invalid IP address for FQDNs starting with numbers.
CSCwo37181	Cisco ISE Cross-Site scripting vulnerabilities.
CSCwo37212	Cisco ISE EngineInformation disclosure vulnerability.
CSCwo37216	Cisco ISE Cross-Site scripting vulnerabilities.
CSCwo37218	Cisco ISE Cross-Site scripting vulnerabilities.
CSCwo37324	In Cisco ISE release 3.3 patch 4, child profiling policies are profiled incorrectly.
CSCwo40162	The integration between Catalyst Center and Cisco ISE fails with AD credentials.
CSCwo42592	Failed administration login attempts are not included in the Cisco ISE Administrator Login Audit Report.
CSCwo46656	Cisco ISE provisioning portal returns an HTTP 500 error or displays a white page due to the SAML certificate losing its usage attributes.
CSCwo48668	The GET_PRIMARYINTERFACE ORA-01427 error occurs during deregistration due to SXP and interface bonding.
CSCwo50986	An external user with multiple RBAC groups is unable to access the local disk under Local Disk Management.
CSCwo51755	A 12-digit phone number consumes an essential license, but a 13-digit phone number does not use a license.
CSCwo52494	Apply an individual grace period per posture policy.
CSCwo52568	Ensure that EndpointStopReplUpdateThread uses the pool.
CSCwo53162	After upgrading to Cisco ISE release 3.x, there is an issue with Permit_IP_Log or Deny_IP_Log showing empty ACL content.
CSCwo55134	Swapping MnT roles changes the default log targets in diagnostics.
CSCwo55160	The Cisco ISE posture client provisioning resource does not appear.

Identifier	Headline
CSCwo56110	Suppression of high load average alarms.
CSCwo56178	In Cisco ISE release 3.5, the reset to default option does not reset the maximum file size and maximum file count levels on secondary nodes in a deployment.
CSCwo57614	The Cisco ISE ERS API requires the changePassword attribute for internal users when using an external ID store.
CSCwo57716	The connected/disconnected filter in Cisco ISE Custom Views does not work.
CSCwo58974	The Identity Group ERS API call exhibits inconsistent behavior with the required parent attribute.
CSCwo59299	Cisco ISE RADIUS DTLS fails to accept an ECDHE client certificate with the KeyAgreement key usage for ECDHE-ECDSA.
CSCwo60932	Number formats greater than or equal to 15 characters will not be processed.
CSCwo61168	Creating or importing guest users in the Sponsor Portal fails when the start and end dates span a DST change.
CSCwo62522	The integrity check warining appears during Cisco ISE service restarts.
CSCwo67904	Cisco ISE ./oracle/base/diag/tnslsnr alert files are not cleared.
CSCwo68027	Need bad file names /var/log/confd/tmplocalhost/ are removed.
CSCwo68953	The OpenAPI patch installation fails with an HTTP or HTTPS repository.
CSCwo69066	Cisco ISE release 3.3 cannot schedule the customized report "Endpoint & Logical Profile Summary".
CSCwo69641	The posture lease timer does not update in Redis and the PAN Oracle database.
CSCwo70962	The Insufficient Virtual Machine Resources alarm is triggered when Cisco ISE is installed in Azure.
CSCwo73164	In the Cisco GUI dark theme mode, a few words are not clearly visible in the debug log wizard.
CSCwo75700	The dictionary password policy is not enforced on the SAN node.
CSCwo76265	Cisco ISE Passive ID Syslog out-of-memory issue.
CSCwo80728	Insertion of syslog data from the top 3 message code ranges through a CSV loader.
CSCwo80977	The "Unable to reach the internet" error appears when you re-enable PxGrid Cloud after deregistering pxGrid Cloud.
CSCwo82042	Access-Reject with no MAC address causes batch processing to fail.
CSCwo83076	The ReadOnlyAdmin user is granted ReadWrite admin access due to duplicate groups in the SAML response.

Identifier	Headline
CSCwo84374	Cisco ISE Improper User ID Updates.
CSCwo85071	Greenfield functionality does not work if the latest OS is not present in osgroup.xml.
CSCwo85102	The upgrade does not handle the session timeout dictionary attribute and updates the maximum value to 65,535 instead of 2,147,483,647 in the database.
CSCwo85633	The icon for the "Is-not" option in the policy set was difficult to identify
CSCwo90009	Endpoints are marked as disconnected on the Context Visibility page without an Accounting Stop from the NAD.
CSCwo90900	Cisco ISE Analytics license registration fails with a "Token Verification failed" error in Swagger UI.
CSCwo93801	The Qualys Scanner tool causes high CPU usage on Cisco ISE nodes.
CSCwo93825	Sorting network devices by the IP or MASK column does not work as expected and returns no data.
CSCwo93895	Optimisations to improve database performance.
CSCwo94849	CoA session reauthentication creates an SXP binding with the SXP domain set to default.
CSCwo97426	ScheduledExecutorService does not recover if an exception is encountered (LicensesTask is not running).
CSCwo97750	Export All (filtered NADs): Password is not encrypted.
CSCwo97767	Cisco ISE GUI sometimes displays inaccuarte dialog boxes.
CSCwo99449	Cisco ISE unauthenticated remote code execution vulnerability.
CSCwp00126	The Proxy Address field does not accept uppercase alphabetic characters.
CSCwp01022	Guest, sponsor, certificate, and posture portals do not load after an upgrade to Cisco ISE release 3.3 patch 5.
CSCwp01113	Multiple portals are not accessible due to a file descriptor leak in the Infra API.
CSCwp01790	When interface tables are empty, information pop-up with no information on registration failure.
CSCwp02104	SLR code generation failed: agent already registered
CSCwp02806	Cisco ISE authenticated remote code execution vulnerability.
CSCwp02819	Cisco ISE Authenticated Remote Code Execution vulnerability.
CSCwp03118	In Cisco ISE release 3.3 patch 5, the error "Failed to create endpoint. ORA-00001: Unique constraint (CEPM.EPMACADDINDX) violated" was encountered.
CSCwp04508	RADIUS shared secret characters are converted to HTML code when saved.
CSCwp04663	Creating a VN does not always create an SGT domain filter for that VN.
CSCwp05894	Cosmetic external MDM server connection failure alarm.
CSCwp06144	ERS API update fails after the previous TACACS shared secret expires.

Identifier	Headline
CSCwp06928	In Cisco ISE release 3.3 patch 5, changing the network device settings changes the RADIUS shared secret.
CSCwp09651	Cisco ISE IP filter bypass vulnerability.
CSCwp09671	The UI pages backed by OpenAPIs fail to load data when an IP access list is configured for admin services.
CSCwp09983	Incomplete or partial message codes in Cisco ISE can cause issues such as the endpoint state appearing blank on the Context Visibility page.
CSCwp10018	Cisco ISE CoAHandler received a duplicate CoA event; the event was ignored for the MAC address.
CSCwp11396	OpenAPI or Duo Identity Sync status updates can cause 'No data available' to appear for external identity sources.
CSCwp14719	Cisco ISE pxGrid Direct service runs after renewing the certificate on the PSN.
CSCwp18000	Identity Sync for native Cisco ISE-DUO integration fails when the username in the Active Directory group contains a space.
CSCwp21830	Cisco ISE Admin WebUI SAML SSO does not work after CSCwh49351 until a manual sync is performed.
CSCwp23104	Cisco ISE reports remain stuck in the 'In Progress' status if the time between the 'In Progress' and 'Completed' updates is too short.
CSCwp23760	Cisco ISE incorrectly shares internal CoA MAR cache logs with FMC over pxGrid.
CSCwp26752	After updating SAML, an error occurs stating Signing certificate validation failed.
CSCwp27799	Cisco ISE triggering false positive alarm for Operational Backup Failure.
CSCwp27887	Null Injection into RBACGROUPIDSASSTRING column observed.
CSCwp28026	DUO IDsync queries to AD need better error handling.
CSCwp33924	The isecfgrestore is stuck at 40% due to Crypt$EncryptionException error.
CSCwp60343	The ERS POST operation for an internal user on port 9060 fails due to client validation failure during certificate-based authentication.
CSCwp63251	Replication fails when the mnt.properties file does not contain the attribute key dedicatedMnT.replication.exception.
CSCwp63601	The non-owner Cisco ISE node has stale information in its Redis entry, which requires regular cleanup.
CSCwp64033	Cisco ISE sends NTP traffic using an incorrect protocol version when configured with SHA-256 authentication.
CSCwp66324	Catalyst Center integration fails when the Cisco ISE hostname contains the string 'admin'.
CSCwp67296	Cisco ISE policy XML export file shows incorrect data for authorization policy security groups for custom-made SGT.

Identifier	Headline
CSCwp80392	Some ciphers are flagged as 'should not use' by Cisco SSL.
CSCwp85879	Guest registration fails for emails containing apostrophes in the 'Person Being Visited (email)' field.
CSCwp90808	TLS security settings should be used to control Cisco ISE release 3.3 Data Connect.
CSCwp91413	When editing an endpoint in Context Visibility for the first time, it may be displayed as "unknown" even if assigned to a static policy and identity group, but refreshing and reopening it displays the correct value.
CSCwp97893	Cisco ISE guest portal Input validation.
CSCwp98652	An out-of-bounds write vulnerability.
CSCwq00041	Exception in the time and date condition does not work.
CSCwq10479	Cisco ISE does not encrypt the empty password field in the RADIUS proxy flow.
CSCwq14266	Cisco ISE firewall rules are not cleared after an administration node swap for port 9002.
CSCwq15847	Duplicating a policy set and changing from Allowed Protocols to a RADIUS sequence are not allowed in the same transaction.
CSCwq17908	LDAP Server Root CA became corrupted after importing the Cisco ISE admin or EAP certificate issued by the same Root CA, causing the application to crash.
CSCwq20539	A CoA is initiated by the PAN when the PAN and the PSN are in different domains, and NIC bonding is configured.
CSCwq20752	CSCwn63400 HP causes OPS DB purge with Export-to-Repository and Encryption Key to fail.
CSCwq21509	Cisco ISE creates additional SXP mappings for the same endpoint in dual-stack environments.
CSCwq22423	The unbound-anchor is not disabled in Cisco ISE release 3.3 patch 6.
CSCwq36692	Cisco ISE images are not available on the AWS Marketplace.
CSCwq53192	Importing a new certificate for the Cisco ISE portal fails with an unsupported protocol (regression CSCwc64480).
CSCwq56216	High CPU and memory leak observed in Cisco ISE during guest 802.1X authentications.
CSCwq56241	TACACS sub-queries do not return the correct or intended details.
CSCwq58770	Stale entries for guest portals are inserted into the database after the application server restarts.
CSCwq58902	Unable to edit users through the sponsor portal results in this error: “An unexpected error occurred. Please contact the help desk for assistance.”

Identifier	Headline
CSCwq68468	In Cisco ISE command set, regex special functionality and escape characters does not work.
CSCwq70418	In Cisco ISE release 3.3 patch 7, Intune MDM based GUID check fails when SAN_URI field contains comma separated entity values.
CSCwq85092	PSN is unable to download the CSC package from PAN.
CSCwq86093	You cannot integrate Cisco ISE with Cisco Meraki if the Meraki Organization name contains special characters that are not part of the English alphabet.
CSCwq96860	Portals displays Ukrainian language when browser language is set to Russian language.
CSCwr10806	Cisco ISE release 3.4 patch 2 and patch 3 fail to update endpoint attribute staticGroupAssignment to 'true' or 'false' when updated using PUT API.
CSCwr19678	ERS API call /ers/config/endpoint with filter does not return description.
CSCwr24232	Cisco ISE release patch 7 rollback issue with IRF_LIVE_LOG & IRF_TEMP_LIVE_LOG.
CSCwr46685	In Cisco ISE release 3.2 patch 7, NMAP scan is not working.
CSCwr70499	Get session bindings count from timesten DB for the telemetry.
CSCwq37845	RADIUS Message-Authenticator must be the first attribute in the packet.
CSCwo26071	Remove Endpoint Replication Issues - Consolidated Changes.

Resolved caveats in Cisco ISE release 3.3 cumulative patch 7

Identifier	Headline
CSCwo99449	Cisco Identity Services Engine Unauthenticated Remote Code Execution Vulnerability
CSCwn11566	Admin access IP address restrictions are enforced only on the login page.
CSCwp02806	Cisco Identity Services Engine Authenticated Remote Code Execution Vulnerability
CSCwp02811	Cisco Identity Services Engine IP Access Restriction for Admin Access Bypass Vulnerability
CSCwp02819	Cisco Identity Services Engine Authenticated Remote Code Execution Vulnerability

Resolved caveats in Cisco ISE release 3.3 cumulative patch 6

Identifier	Headline
CSCwp01022	The Guest, Sponsor, Certificate, and Posture portals do not load after upgrading to Cisco ISE Release 3.3 patch 5.
CSCwp17745	'Message Authenticator Required on Response' is enabled by default in Cisco ISE Release 3.3 patch 5.

Resolved caveats in Cisco ISE release 3.3 cumulative patch 5

Identifier	Headline
CSCwm12300	Unable to change the password policy in Cisco ISE under internal identity user authentication settings.
CSCwm05739	A blank screen is seen through the CIMC KVM in SNS-3755 PID after POST in the customer unit.
CSCwn82191	Password policy with dictionary words is not functioning as expected on Cisco ISE Release 3.3.
CSCwn46575	Need Lower Interface MTU Than 1280.
CSCwk98617	A black line is visible when expanding the menu in Cisco ISE Release 3.3 Patch 3 in Firefox version 128.
CSCwm48850	Unable to retrieve Endpoint Identity Groups using ERS starting from Cisco ISE Release 3.3 Patch 3.
CSCwn12582	Script condition is not displayed on the requirements page.
CSCwe09140	Development bug related to the implementation of the 'CA Diagnostic Tool'.
CSCwj48353	The Cisco ISE hourly cron page cache cleanup needs to be adjusted based on the percentage of memory occupied.
CSCwn81215	Unable to profile devices using LLDP during onboarding because Cisco ISE does not process the LLDP attributes.
CSCwn17599	The SFTP server validation fails with Cisco ISE Release 3.3 Patch 3.
CSCwf23271	The deployment SEC_TRNREP_STATUS is not updated from the "In Progress" state.
CSCwn50257	MDM server-related attributes are missing in the pxGrid session published data.
CSCwk45576	Unable to save the UI for NAD with IPv6 when TrustSec sends configuration changes to the device.
CSCwn09816	The RADIUS shared secret masking after switch reload causes authentication failures.
CSCwm05976	RPC calls are made through Active Directory probe for ODBC authentications.
CSCwm00336	The domain name is not updated in the system file (etc/hosts) during bond configuraton.

Identifier	Headline
CSCwk24032	Not all Cisco ISE SRV records have IP address due to UDP size limit (length = 548).
CSCwn52291	The integrity check file must be included in the support bundle.
CSCwn44838	Egress (SGACL) Policy: The command 'show cts role-based policy' is incorrect.
CSCwm36268	In Cisco ISE Release 3.3 Patch 2, endpoints are incorrectly displayed as rejected endpoints even after they are released from the network.
CSCwn92051	In Cisco ISE Release 3.3, a blank TACACS authorization report is restored if the operational backup is obtained from an older Cisco ISE release (below Cisco ISE Release 3.3).
CSCwj04839	Cisco ISE Azure REST ID Store - Lifetime validation failed; the token is expired.
CSCwm52140	Cisco ISE Release 3.3 Patch 2: DACL parse failure.
CSCwm66426	Cisco ISE is inaccessible from both the GUI and the CLI.
CSCwj38688	When using an expired license, the error "Host not found in the identity group due to a profiler null pointer exception" is displayed.
CSCwn21374	In Cisco ISE Release 3.3, there's a delay when logging into an asynchronous PAN due to lack of response to TCP 443.
CSCwm33559	GET requests to the Policy API may fail on non-primary PAN.
CSCwn30743	Custom endpoint attribute format error in Cisco ISE Release 3.2 Patch 6.
CSCwi51182	Cisco ISE, as an OCSP client, needs to be more tolerant of current time differences from those of OCSP responders.
CSCwm72853	Cisco ISE-PIC: The MFC Profiler service on Cisco ISE must be disabled.
CSCwm60820	Scheduled restart does not work as expected when Cisco ISE nodes are in different domains.
CSCwn30984	Administration thread pool reached threshold value alarm.
CSCwn03702	Cisco ISE: SAML: Multi-Application Support.
CSCwm65550	The endpoint static identity group is changed due to duplicate EPIDs and stale RCM EPIDs across nodes.
CSCwi01581	SXP binding is stuck on Cisco ISE during re-authentication of endpoints between multiple VNs.
CSCwj04202	Cisco Identity Services Engine Stored Cross-Site Scripting vulnerability.
CSCwn26742	Cisco ISE is missing rate limiting protection for the Local Disk Management page.
CSCwm63134	In Cisco ISE Release 3.2 Patch 6, Cisco ISE does not query MDM intermittently if it receives a 404 response from the MDM server.

Identifier	Headline
CSCwm91602	Modifying the TACACS shared secret in limited admin groups alters the 'VPN Servers' attribute.
CSCwd96743	Log Collection Error warning: Log collection error - Server=xxxx; Log Type=RadiusAuthenticationPassed.
CSCwm59541	Relocate sensitive API gateway data to an encrypted partition.
CSCwm59423	Unable to retrieve the Evaluated System Admin and Super Admin groups permissions for SAML authentication.
CSCwn92534	Serviceability: Context visibility does not work when the Stunnel service is not running.
CSCwn77322	Context visibility blurs device information and MFC information.
CSCwn11732	The Cisco ISE GUI login page loads for a long time and the URL changes to /admin/login.jsp?mid=auth_failed.
CSCwj81776	Unable to use the advanced filter in Cisco ISE Release 3.2 for "Empty" and "Not Empty" filters.
CSCwm43231	Previews of custom portal files do not load properly.
CSCwn94797	The RADIUS token configuration does not work after installing Cisco ISE Release 3.1 Patch 10 in the deployment.
CSCwm65529	The static identity group cannot be changed for endpoints.
CSCwh92320	There is a memory allocation limit for Oracle PGA and Oracle SGA processes.
CSCwm07116	The URL mapping for SMS gateway GET requests is not visible in the guest.log.
CSCwm84363	Using 'Network Device Profile = ANY' and 'Advanced Attribute' breaks the GET all authorization profile API call.
CSCwk67747	RADIUS protocol spoofing vulnerability (Blast-RADIUS).
CSCwm95060	Context visibility reset fails when Cisco ISE is dual-stacked.
CSCwn54212	Unable to remove the identity-store CLI configuration due to case-sensitive mismatches.
CSCwm99057	The agentless posture is stuck in pending state due to an unsupported OS.
CSCwk91347	Enable PAP when FIPS is enabled for RADIUS DTLS compatibility.
CSCwm90962	Unable to filter data using the advanced filter on the Context Visibility page after creating a new dashlet.
CSCwn60000	In Cisco ISE Release 3.4, group retrieval fails in Secure LDAP due to the offered cipher suite in 'Client-Hello'.
CSCwf09393	In Cisco ISE Release 3.1, services fail to start after restoring a backup from Cisco ISE Release 2.7.

Identifier	Headline
CSCwm26992	An IllegalStateException occurs when querying external groups from Azure.
CSCwm10884	LDAP groups on Cisco ISE cannot be saved if the CN contains parentheses.
CSCwm04552	Uploaded CSS files do not reflect changes on the portal.
CSCwj91517	You need to disable the unbound-anchor when starting Cisco ISE.
CSCwm50409	The ERS API endpoint call is slow.
CSCwm53340	The PSN node running TACACS crashes - regression CSCwe82004.
CSCwm99047	The agentless posture troubleshooting tool is failing with a 'RequiredFieldNotExist' error.
CSCwm88516	The option 'The Enable Password for TACACS access will never expire' is ineffective.
CSCwm18037	OCSP is unreachable due to the use of HTTP 1.0 by Cisco ISE.
CSCwn51058	In Cisco ISE Release 3.3, the RabbitMQ log does not rotate, causing high disk space utilization.
CSCwn34778	The authentication session does not match the MDM policy despite having MDM attributes.
CSCvy74903	The IP address 169.254.4.3 is seen when using certificate-based authentication for Cisco ISE administration.
CSCwm88519	Sending a certificate with incorrect SAN values will bring down the tunnel.
CSCwn52227	MDM VPN endpoint reauthentication flows do not hit the authorization policy due to a null value.
CSCwm37824	The download button for the proposed profiled rule throws a 400 error.
CSCwm71222	The /opt directory in Cisco ISE is full because alarm files are not automatically deleted.
CSCwn96913	The incremental scheduler is not functioning, resulting in a 401 unauthorized error.
CSCwm40047	Misleading error prompt: 'Unable to send email.'
CSCwm91931	In Cisco ISE Release 3.4 Patch 1, the scheduled export fails, and data does not appear in the Health Summary in a longevity setup.
CSCwk63893	UDP syslog DNS name resolution must be performed in a single function call rather than two separate calls for IPv6 and IPv4.
CSCwm53456	In Cisco ISE Release 3.3 Patch 2, an error occurs while retrieving certificate details.
CSCwk51948	In Cisco ISE Release 3.2, MNT cannot connect to its own database.
CSCwn66616	Predefined alarms with restricted special characters cannot be edited.

Identifier	Headline
CSCwm80276	Authentication against the ROPC identity store failed due to an RSA key generation error in the asynchronous flow.
CSCwn63678	RADIUS accounting reports cannot be exported to the repository in Cisco ISE Release 3.3.
CSCwn47652	Endpoint attributes are not reflected in the Oracle database during the MDM flow when EPOD is disabled.
CSCwn17160	Clarify EAP-TLS (TLS 1.2) authentication failures when using an elliptic curve that is not in the supported groups.
CSCwm47768	Cisco ISE portals display Ukrainian when the browser language is set to Russian.
CSCwk56154	An RBAC admin user can add a user without a static assignment group.
CSCwm36039	In Cisco ISE Release 3.4, the GuestAPI query fails when using an admin account with sponsor privileges.
CSCwm67082	Cisco ISE Release 3.2 and later should not allow updates to the hostname, IP, or domain name for Cisco ISE nodes in deployments.
CSCwn09009	Local and global exception policies exhibit unexpected behavior when the 'Default' policy is configured.
CSCwm87358	Delete the endpoint purge rule.
CSCwm44513	System 360 permission issues occur when using PIV or CAC authentication for Cisco ISE admin access.
CSCwn27059	Exporting a filtered NAD causes infinite loading in Cisco ISE Release 3.2.
CSCwn50479	In Cisco ISE Release 3.2 Patch 7, the sponsor view (SAML Sponsor) cannot be limited.
CSCwm67805	BYOD devices remain in WebAuth Pending status even after registration due to CoA reauthentication being stuck.
CSCwi61222	Perform a spell check for 'Reassessment' on the page below.
CSCwn97014	The scanDirectory method causes a memory leak when a large number of Cisco ISE localStore logs are present.
CSCwf60994	Vulnerabilities in high charts version 6.1.0.
CSCwk97061	Creating a new profiling policy updates the inactive days for all endpoints.
CSCwm03837	In Cisco ISE Release 3.2 Patch 6, the health check for I/O bandwidth fails even when it is within the supported guidelines.
CSCwh27101	IPv6 static routes are removed after performing shut and no shut on the interface.
CSCwm88083	In Cisco ISE Release 3.3, the Smart License registration fails with the error message: 'Unable to perform Smart Licensing operation.'

Identifier	Headline
CSCwm42509	Activation of the Cisco AI Analytics engine is not possible due to restricted access to the AI agent container's IP address.
CSCwn07856	Vulnerabilities in RabbitMQ version 3.6.5.
CSCvg54133	The hostname changes when printed in the CLI during a 'show tech' command.
CSCwm13073	Error: 'This custom view has exceeded the maximum number of SGTs (3000),' despite having fewer than 3000 SGTs.
CSCwm68670	The import of guest users fails when adding Username and Password columns to the Sponsor Portal template.
CSCwm51099	Sponsors from different GROUP_ACCOUNTS can see all users if they are in the same OWN_ACCOUNTS group.
CSCwm85239	Cannot delete User Identity Groups: <>java.lang.NullPointerException.
CSCwn15744	Serviceability improvement: Audit log the Jedis connection failure.
CSCwn27953	In the Italian Sponsor Portal, the calendar should not show Dom, Lun, Mar, Mer, MAR, Ven, DOM.
CSCwn07375	The '\' character is being interpreted as an escape sequence during admin login.
CSCwn96558	Authentication latency is observed while checking for MDM.OS version.
CSCwj45793	In Cisco ISE Release 3.2, the `catalina.out` file is flooded with application logs when endpoint debugs are running.
CSCwn22572	Cisco ISE is stuck at the saving changes stage when duplicating and editing a CPP portal.
CSCwk80409	The disk is full due to the `ctr.log` file growing exponentially.
CSCwm26245	Secondary PAN and PSN nodes cannot upload files larger than 14GB via Local Disk Management.
CSCwn84705	The import of guest users fails when using a CSV template in Firefox.
CSCwn24592	Scroller issue under SAML group.
CSCwm60638	Unable to start or stop an existing TCP dump capture.
CSCwj52266	The endpoint description in Context Visibility is updated with the Static Identity Group description.
CSCwn43818	There is a mismatch between the username and calling station ID when calling the ODBC stored procedure for attribute retrieval.
CSCwm32937	Cisco ISE is not responding to specific accounting packets, which has led to incorrect IP addresses being updated in Cisco ISE.

Identifier	Headline
CSCwn57286	In Cisco ISE Release 3.3, the "Security Settings" section incorrectly shows a TLS warning when the user modifies other settings.
CSCwk59325	Cisco ISE services are initializing due to a dangling LOCK_FILE.
CSCwk30242	Cisco ISE is not updating the NAS when a client performs Fast-Roaming.

Resolved caveats in Cisco ISE release 3.3 cumulative patch 4

Identifier	Headline
CSCwj57697	Data mismatch while opening live logs or live session details in Cisco ISE.
CSCwh01906	Deleted MDM server is still listed in MDMServerName attribute allowed values.
CSCwm13930	Agentless posture endpoint logs are exported as HTM instead of a zip file.
CSCwk45395	When a previous mandatory policy fails, the audit policy fails and shows skipped conditions.
CSCwk07593	The Get-All Guest User API does not retrieve all accounts, specifically those created by other sponsor users.
CSCwj82278	Stale lock files blocks API gateway and context visibility.
CSCwk76790	When you try to edit or add a description for network access users, the description field closes.
CSCwj76445	Cisco ISE ERS guest documentation should be updated to exclude portal ID from the Get calls.
CSCwk71111	Backup restoration is stuck at 75 percent.
CSCwj54376	Evaluate configuration validator does not parse all the NAD interfaces.
CSCwk25206	Empty GPG files are exported if there is no data to purge.
CSCwj68795	Replication Error "Error synchronizing object: EDF2EndPoint: Operation: Update".
CSCwm10693	Cisco ISE internal users account disable policy feature does not work after one day of inactivity.
CSCwk13234	Old Cisco ISE nodes are shown in TCP dump and debug profile configuration after restore.
CSCwh54899	Unable to log in to Cisco ISE GUI. After entering the credentials, it hangs on checking the credentials screen.
CSCwj83460	Discrepancy in the count of identity groups between the CV and Oracle database.
CSCwf69715	After patch install TC-NAC adapters will be not reachable and new adapters cannot be configured.
CSCwi58421	When posture lease is enabled, the PSN node does not update the database with the correct posture expiry time.
CSCwj58727	Cisco ISE does not allow saving allowed protocols with no protocols checked.
CSCwh49351	SAML request PSN exclusion.

Identifier	Headline
CSCwj44649	TACACS data is not retained and everything gets purged.
CSCwj82240	Cisco ISE counters reports are empty for secondary nodes.
CSCwf11926	Repository password accepts %,<,>,? characters from CLI but not from GUI.
CSCwk74103	Cisco ISE EAP-FAST PAC-less session timeout, value does not get saved.
CSCwj09219	Update OpenSSL library to OpenSSL 1.1.1x (CiscoSSL 7.3.375 with FOM 7.3a).
CSCwk07454	PSN does not update the database with the correct posture lease expiry time.
CSCwk46855	Users pending account is not displayed in the Sponsor Manage Account page.
CSCwk30610	TACACS+ endstation network condition high step latency while accessing the NAD through console.
CSCwk04493	From Cisco ISE 3.1 Patch 6, the method used to retreive policy details calls the internal method and is not cached.
CSCwk15719	Cisco ISE profiler unable to read the MAC from the LLDP port ID subtype 7 received through SNMP probe response.
CSCwi20027	TrustSec deploy request failed and CoA request got stuck while fetching NADs.
CSCwj94294	Cisco ISE REST API Blind SQL Injection Vulnerabilities.
CSCwj94297	Cisco ISE REST API Blind SQL Injection Vulnerabilities.
CSCvy30859	From Cisco ISE Release 2.6, it is not possible to create static IP-SGT mapping for EPGs imported from ACI.
CSCwj94305	Cisco ISE REST API Blind SQL Injection Vulnerabilities.
CSCwk38279	The ea.log file should be included in support bundle.
CSCwk87768	Authentication using the name of the profile fails when the default device is used.
CSCwj84815	"No session available" error is displayed when tried to rename guest type in the policy set.
CSCwk67197	Cisco ISE does not connect with external RADUIS server when proxy-state attribute is missing.
CSCwj97724	Cisco ISE should not allow updating existing library conditions with conditions that are not allowed in the policy set.
CSCwk31930	Cisco ISE skips authentication against the child domain controller when the AD Forest is marked offline.
CSCwk06043	Binding with SGT assigned through MAB policy is not seen in SGT bindings table.
CSCwm00197	Numeric overflow exception encountered during restart of replication client.
CSCwk88239	MDM significant attributes causing database persistent events during authentication flow.
CSCwk35573	Vulnerable JS Library issue found while executing ZAP in Cisco ISE Release 3.3.

Identifier	Headline
CSCwj97491	Cisco ISE Command Injection Vulnerability.
CSCwk93711	Cybervision receives DDOS getAssets calls post Cisco ISE integration.
CSCwj67089	Cisco ISE app server crashes while importing large files to secondary node through local disk management.
CSCwk07483	Profiler network device event handler failed to add device for input string 0-255.
CSCwj23933	AD connector is not in joined status.
CSCwk55333	The ise.psc.log does not print the incoming API request's URI in DEBUG mode.
CSCwi86762	Right CoA to be triggered in VPN flow when posture and MDM flow are configured together.
CSCwk36095	The pxGrid live log serviceability.
CSCwj85626	Unable to retrieve Endpoint IP address through API calls.
CSCwf79582	AD credentials fail to integrate Cisco ISE with Cisco Catalyst Center 2.2.1.x and above.
CSCwk13244	The ise.messaging.log is not visible on GUI to download.
CSCwj95818	Maximum concurrent CLI sessions does not work.
CSCwk32078	Endpoint check result remains unreachable after passive ID login event.
CSCwj35581	Cisco ISE missing rate limiting protection.
CSCwh39213	Unable to replace SSH key for Cisco ISE AWS Ec2 instances.
CSCwk25839	Getting higher counts on external active directory logs on syslog server.
CSCwk64227	ODBC query in authorization policy does not return result with postgres.
CSCwk40725	ConfD generates endless localhost:9888.access.1.1.1.1...and so on.
CSCwk79546	In Cisco ISE Release 3.3 Patch3, DUO MFA authentication fails instantly with "22076 MFA authentication failed" in live logs.
CSCwk59176	The graph is not shown when you click on Cisco ISE report in launchpad from prime infrastructure.
CSCwj80616	Endpoint details in Cisco ISE context visibility does not match with RADIUS live logs or sessions during MDM flow.
CSCwj48625	Agentless posture fails for EAP-TLS flows with multiple domains configured for endpoint login.
CSCwj35698	Cisco ISE Business Logic Issue - User Dictionaries.
CSCwk04644	From Cisco ISE Release 3.2, the System 360 Monitoring debug log rotation does not work.
CSCwk14636	In Cisco ISE 3.2 Patch 6, insufficient virtual machine resources alarm triggers on AWS.
CSCwk40233	Posture state synchronization feature use cases and validation steps need to be documented.
CSCwk21895	Cisco ISE says CLI maximum password size is 127.

Identifier	Headline
CSCwk32677	The ise-duo.log is not collected at the time of support bundle creation.
CSCwk09094	Misleading pop-up is seen while password lifetime is set for more than 365 days.
CSCwk38828	In API NBAR application management setting, PUT option shows an error in swagger tool.
CSCwk06817	Known OS bug causes swap to increase on Cisco ISE nodes.
CSCwj29473	Cisco ISE Formula Injection.
CSCwk91976	The GUI does not ask confirmation of old password for password change.
CSCwk32104	OOM heap files must be deleted for agentprobeoom.sh and restprobeoom.
CSCwk38327	Health check fails for MDM flow.
CSCwj66951	When creating network access user, the system does not allow to create the user with the first name or last name including combinations of "OR".
CSCwc64144	Total authentication latency and client latency does not work for TACACS+.
CSCwk20019	Attribute name in SMS HTTP URL causes issues with URL updates on editing.
CSCwk35172	The "DumpClearOnExceed" files filling up the disk on Cisco ISE PSN nodes.
CSCwj35576	Cisco ISE Server-Side Validation Missing.
CSCwk07789	Invalid IP or hostname error when using "_" as first character in the nslookup request.
CSCwi72309	Cisco ISE stuck in a profiling loop which causes slow replication errors.
CSCwm29900	Imported endpoints shows incorrect endpoint IDs causing data mismatch.
CSCwj77501	ODBC advanced attributes does not work if two or more in-bound attributes are selected.
CSCwe54931	System 360 does not show Cisco ISE nodes with different DNS domain names other than primary Cisco ISE.
CSCwk75775	The health check fails on input or output bandwidth performance check and returns a NULL result.
CSCwj82298	Assigned logical profile is repeated in context visbility endpoint attributes and reports.
CSCwj83459	Unable to create new internal user due to "could not execute statement; SQL [n/a]; constraint" error.
CSCwj72680	The HS_err files gets generated on MnT nodes.
CSCwk73315	Cisco ISE 360 Monitoring dashboard displays average CPU time percentage instead of summing the rate.
CSCwj72117	Operational data purging shows only primary monitoring node name in a two deployment node.
CSCwk25064	SXP threads storing NULL objects in the Java heap causes high CPU load and utilization.
CSCwk53171	Cisco ISE /ers/config/endpoint/getrejectedendpoints does not have pagination and returns only 100 endpoints.

Identifier	Headline
CSCwj97449	SNMP v3 config does not alert the admin when engineID format is incorrect for snmp-server host.
CSCwj38485	High memory usage observed in <getAllTrustCerts> class in eight-node deployment.
CSCwj94315	Cisco ISE REST API Blind SQL Injection Vulnerabilities.
CSCwj52362	Primary admin node stuck at disk corruption check stage during split upgrade from Cisco ISE Release 3.3 Patch 1 to Cisco ISE Release 3.4.
CSCwj33906	IP-SXP mapping is not created for VPN clients.
CSCwk34825	Cisco ISE internal users lock or suspend on incorrect attempts counter does not work as expected.
CSCwk69424	ODBC advanced setting sent in procedure call should be logged.
CSCwj17975	Could not assign EAP role on certificate with IMS role.
CSCwj89479	When joining multiple Cisco ISE nodes to the domain controller simultaneously, duplicate accounts are created.
CSCwk75761	High CPU on admin node post accessing "Endpoint Identity Groups" page on Cisco ISE.
CSCwk66013	Change in local log settings does not trigger old files deletion.
CSCwi66105	In Cisco ISE Release 3.1 Patch 7, When the endpoint attribute filter is disabled, custom attributes are not retained.
CSCwj40026	Backup details are showing scheduled status as "no" and "triggered from CLI", when they are scheduled from GUI.
CSCwk38245	In Cisco ISE Release 3.2 Patch 6, Cisco ISE_Internal_Operations_Diagnostics triggers FATAL logging message stating system has reached low disk space limit due to localstore directory size issue.
CSCwc62131	Cisco ISE is not able to query MySQL 8.x as mysql.proc table is not implemented.
CSCwm00497	Cisco ISE passiveid-agent.log should include information about the user when logon event is shared.
CSCwk45006	Device admin license does not allow Cisco ISE admin user to reset first login password.
CSCwj74175	Compress restprobeOOMHeap dumps.
CSCwk90681	From Cisco ISE Release 3.3 Patch 3, multiple options have been removed or do not work work in application configure ise command.
CSCwj80950	Cisco ISE does not share posture compliant session properly over pxGrid.
CSCwj77067	Better description for error while editing internal users
CSCwk29799	List of installed patches does not show under patch management page due to admin certificate issue.
CSCwd61906	Sysaux tablespace allocation should be done based on the profile of the node.
CSCwk69537	Cisco ISE Release 3.2 API does not validate if a join point is being used when deleting it over the ERS API.

Identifier	Headline
CSCwj12359	Interrupting execution of "show tech-support" causes services to stop on Cisco ISE.
CSCwh50924	Unable to delete the IPv6 route after performing the modification.
CSCwk05023	Undefined data in information page of identities.
CSCwj71638	Policy hit count shows zero when fetched by open API GET call.
CSCwk70500	From Cisco ISE Release 3.2 and later, bond interfaces need MTU as configured on primary interfaces.
CSCwk80923	Cisco ISE CLI or SSH user does not follow password policy.
CSCwm30212	The pxGrid direct triggers sync at last restart time instead of scheduled time.
CSCwm48867	The swapon or swapoff cron should be removed as it causes high load every six hours.
CSCwm35851	If PAN failover is enabled in deployment page PAN-HA precheck fails.
CSCwj75183	In Cisco ISE Release 3.2 Patch 5, documentation correction for guest.
CSCwj87344	Cannot delete a capture following a hostname change.
CSCwm41230	In Cisco ISE Release 3.3 Patch 3, MnT database reset causes all database to corrupt.
CSCwk02837	High memory utilization causes the app server to restart after 12 hours of passive traffic.
CSCwm53627	Optimize the indexing for 'EDF_MDM_GUID' lookups for 'EDF_MDM_GUID' to eliminate full table scans.
CSCwk63923	DNS cache timeout is not honored.
CSCwm33110	Heap space is fully utilized by RMQ Consumer.
CSCwm72206	In Cisco ISE Release 3.3 Patch 3, the external identity sources show "no data available" after Cisco ISE Release 3.3 Patch 3 installation.
CSCwm58686	Passive session is not published to FMC as Cisco ISE tries to stitch the session.
CSCwj72586	OOM killer alerts Cisco ISE Admin CLI due to API-gateway memory limitation.
CSCwm02519	Additional fix to LSD class.
CSCwm61668	TC-NAC_Tenable throws "Scan Failed: Error in connecting to host: 403 Forbidden" error.
CSCwm44693	Cisco ISE reverts to the old CLI password after shutting down and powering on the VM or SNS appliance.
CSCwi89923	GigabitEthernet or Bond Interfaces with link-local IPv6 addresses after IPv6 is disabled.
CSCwm46079	SXP mappings is not learned for VPN users private IP.

Resolved caveats in Cisco ISE release 3.3 cumulative patch 3

Caveat ID Number	Description
CSCwi89720	Microsoft Azure AD has been officially renamed as Microsoft Entra ID.
CSCwi67639	Command show cpu usage does not display information on Cisco ISE Release 3.x.
CSCwi60778	Endpoint loses static identity group assignment after reauthentication.
CSCwj43912	Application remediation disappears after editing.
CSCwf24553	Umbrella defect for providing information for terminologies used in licensing page.
CSCwj60692	TLS is restricted to use only a few ciphers in Cisco ISE Release 3.3 but 8905, 9094, 9095 ports uses all ciphers.
CSCwi58699	A guest flow triggers a CoA when Cisco Catalyst Centre or EA dictionary attributes are updated on Cisco ISE.
CSCwi62078	[404] Resource Not Found error occurs when using the built-in authorization profile Block_Wireless_Access.
CSCwj48827	Unable to add multiple tasks with quotes in launch program remediation.
CSCwj05508	IP host <ip> <fqdn> command does not create IP-FQDN entry in Cisco ISE.
CSCwk00439	The pxGrid direct service remains stuck in the initializing state as the lock file is not removed.
CSCwj35698	Cisco ISE business logic issue in user dictionaries.
CSCwi94938	The Cisco ISE Release 3.2 guest user API gives incorrect results when using a filter.
CSCwh33160	Cisco ISE fails to send SNMPv3 disk traps to the configured SNMP server.
CSCwi15793	Cisco ISE throws an error for iPSK custom attributes that start with special characters.
CSCwi59868	The system extends sponsored guest accounts beyond the maximum number of days allowed.
CSCwi89082	SAML default portal required to configure SAML in Cisco ISE is deleted from database.
CSCvy34255	Extra popup screen appears while viewing RADIUS or TACACS key after enabling "require admin password" option.
CSCwi78164	Cisco ISE DNS resolvability health check fails due to a duplicated entry of IP, name and FQDN on /etc/hosts.
CSCwi61950	Cisco ISE reaches the context limit in proxy flow when it queries LDAP groups for authorization policy.
CSCwj14217	Device network conditions GUI fails to load.
CSCwh67500	Cisco ISE Release 3.2 could not find selected authorization profiles.
CSCwj97620	The pxGrid direct sync is stuck in progress.
CSCwj12489	Unable to delete network device group.

Caveat ID Number	Description
CSCwi57903	A failed scheduled backup does not generate an alarm.
CSCwj21203	The "Dashboard System Status" query exhausts 1000 database connections.
CSCwj03747	Profiling does not suppress CoA although CoA is suppressed for specific logical groups.
CSCwh92366	Insufficient virtual machine resource alarm is observed in Cisco ISE Release 3.1 Patch 8 longevity setup.
CSCwj06269	Device administration setting changes record no report or alarm.
CSCwj51329	MDM compliance check fails when there are multiple MAC addresses with VMware Workspace ONE as MDM.
CSCwj39533	The RMQ forwarder causes high CPU or load average.
CSCwh01323	Fix for using IPv6 with CoA requests.
CSCwj21403	REST API authentication service does not enable when /etc/hosts has multiple entries.
CSCwj36716	Cisco ISE self persistent Cross-Site Scripting (XSS) in my reports.
CSCwi59230	Non super-admin users cannot edit or delete endpoints when Cisco ISE has more than 1000 identity groups.
CSCwd49321	Cisco ISE integration fails with pxGrid is not enabled on Cisco ISE error message even when pxGrid is enabled in both nodes.
CSCwj43480	Cisco ISE Release 3.3 does not invoke MFA for the user with User Principle Name (UPN).
CSCwh36667	Cisco ISE monitoring GUI page stuck at "Welcome to Grafana".
CSCwi93050	When using Azure SAML for admin access, RBAC causes endpoint import to fail.
CSCwh56565	Primary PAN REST API call to MnT nodes should not be load balanced.
CSCwi74567	Inconsistencies in the database cause corruption in the Cisco ISE portal.
CSCwa82035	Cisco ISE support bundle must include garbage collector logs, thread dump, and heap dump.
CSCwj29392	Cisco ISE cross-site request forgery.
CSCwi73981	Cannot remove identity store from CLI that was added using uppercase FQDN.
CSCwf36985	AD group retrieval fails while evaluating authorization policy.
CSCwi98793	Profiler caches MDM attribute with wrong values.
CSCwj07319	API ers/config/sessionservice node returns an incorrect total.
CSCwi79159	Cisco ISE Release 3.2 Patch 4: deleteCertFromStore fails to parse certificate.
CSCwi61491	Application server crashes due to metaspace exhaustion.
CSCwi89689	Invalid IP or hostname error.

Caveat ID Number	Description
CSCwi52041	Changes in rank cause authorization rule to commit to the database table which triggers save call from UI.
CSCwh00060	Cisco Identity Services Engine Code Injection Vulnerability.
CSCwj16540	Cisco ISE Release 3.2 Patch 4 context visibility does not match live logs or sessions.
CSCwj06401	Endpoints that have null key value pair in the attributes section interrupts the purge flow.
CSCwj72982	No IPv4 or IPv6 selection is seen for passive ID reports for IP address column filter.
CSCvt75833	Cisco ISE should do lookup again when the token server is FQDN.
CSCwh23986	The pxGrid getUserGroups API request returns an empty response.
CSCwj32716	The nsf should return index-0 SAN-URI to MDM, even when we have multiple SAN-URIs.
CSCvm56115	Cisco ISE allows a policy to be saved when another browser tab deletes an ID Store.
CSCwi96581	Upgrade CXF version as 3.4.2 is vulnerable.
CSCwj01310	Intensive garbage collection is observed due to SXP component.
CSCwh69267	After ADE-OS is restored, appserver is stuck at initializing state.
CSCwj07675	Cisco ISE Release 3.2 sends outgoing RST packets with APIPA IP 169.254.4.x.
CSCwi67503	Cisco ISE could not find selected authorization profile if created using API.
CSCwj47769	Invalid request page in Cisco ISE Release 3.2 Patch 5.
CSCwi63725	SNMPD process causes memory leak on Cisco ISE.
CSCwi57761	In Cisco ISE, the vulnerabilities identified by the Common Vulnerability and Exposures (CVE) ID, CVE-2023-48795 affect third-party software in open SSH.
CSCwh25160	Swap cleanup script to drop the swap area and program the cron.
CSCwh95587	Cisco ISE Release 3.2 Patch 2 is intermittently not unmounting NFS repositories.
CSCwd14523	The 'accountEnabled' attribute in Azure AD causes authentication issues for EAP-TLS.
CSCwh61339	Export of more than 90,000 network devices times out.
CSCwj07717	Cisco ISE audit reports log APIPA addresses as the source of API requests.
CSCwa32407	Resend the user account details for all or specific guest users to the sponsor.
CSCwf56826	Primary PAN nodes show cores related to jstack.
CSCwj66777	Cisco ISE Release 3.3 ECDSA Explicit Curve test fails for EAP, secure syslog, and secure LDAP.
CSCwj60125	Enhance guest user account search functionality.
CSCwk18638	TrustSec CoA is not sent from the primary PAN when it does not have a policy role.

Caveat ID Number	Description
CSCwi61950	Cisco ISE reaches the context limit in the proxy flow while querying LDAP groups for authorization policy.
CSCwi38377	Unable to trigger CoA that is stuck at dispatcher queue.
CSCwk07324	Cisco ISE main ThreadPool is stuck due to ACE 3rd party library causing contextN leak.
CSCwk61938	Cisco ISE Evaluate OpenSSH CVE-2024-6387 "regreSSHion".
CSCwj44649	In Cisco ISE 3.3, TACACS data is not retained and everything gets purged.

Resolved caveats in Cisco ISE release 3.3 cumulative patch 2

Caveat ID Number	Description
CSCwf47838	Space characters in command arguments are not preserved after CSV Export of TACACS + command set.
CSCwi48806	Authorization policy takes time to load, causing delays in Duo portal entries.
CSCwf24554	SR-Insights identifies an Umbrella defect that displays more information on SL registration failure.
CSCwf93165	In Cisco ISE 3.3, enabling the "always show invalid usernames" option does not work.
CSCwh99534	Endpoint probe does not clean up SGT Exchange Protocol mappings.
CSCwh24823	Updating internal users through ERS need to retain values of Non-Mandatory Attributes.
CSCwi53104	Exporting the report beyond one-month period yields no data.
CSCwd67833	ERS API takes several seconds to update single endpoint.
CSCwh83323	In Cisco ISE 3.2: SMS is not sent in the "Reset Password" flow when using a custom SMTP API Destination Address.
CSCwe25050	A wildcard certificate imported on PPAN is not replicated to other nodes in deployment.
CSCwi69659	TrustSec deploy verification - policy difference alarm while policy identical on Cisco ISE and NAD.
CSCwh74135	Unable to integrate with Prime Infrastructure due to a wrong password error.
CSCwi29253	The Cisco ISE AD Diagnostic Tool stops working upon upgrade, making it impossible to retrieve the list of available tests.
CSCvj75157	Cisco ISE API | Does not recognize identity groups while creating user accounts.
CSCwf61673	Cisco ISE CLI Read only users cannot run show CPU usage command.
CSCwi61491	Application server crashes due to metaspace exhaustion.
CSCwi54722	In redirect URLs that use FQDN that end with IP, IP is replaced by Cisco ISE hostname.
CSCwa15336	In Cisco ISE PIC 3.1, the Live Session feature does not show terminated sessions.

Caveat ID Number	Description
CSCwi30707	Cisco ISE 3.1 patch 7: Removed Device Types remain selectable in policy set.
CSCwi45090	Cisco ISE: REST API ERS: downloadableacl: The filter field 'name' is not supported.
CSCwi42628	MAR Cache replication fails between peer nodes for both NIC and NON-NIC bonding interfaces.
CSCwh81035	The PAN is missing non-significant attribute updates of endpoints from PSNs.
CSCwi21020	Cisco ISE Messaging Certificate generation does not replicate full certificate chain on secondary nodes.
CSCwi04514	Posture Client Provisioning Resources HTTP Error when dictionary attribute contains "-".
CSCwi36040	IP access list control in Cisco ISE 3.2 is not visible.
CSCwi15914	Additional IPv6-SGT session binding created for IPv6 link local address from SXP ADD operation.
CSCwi66126	Cisco ISE ERS API - Updating DACL does not modify last update timestamp.
CSCwh87732	Vulnerabilities in antisamy 1.5.9.
CSCvs77939	There are errors when editing AnyConnect configuration and Posture Agent profiles.
CSCwh21038	Session info not stored in timed session cache during third party posture flow.
CSCwh83482	Cisco ISE Database does not update the email field for Sponsor Accounts.
CSCwh96018	Failure due to case sensitive check when new MDMs are created with the same name but different case.
CSCwi54325	LINUX ISSUE - PRA fails if end point is within posture lease.
CSCwi53915	Advanced Filter "Save" option does not work for Client Provisioning Resources filtering.
CSCwf89224	Session ticket received from NAD decrypt fails when OU has & and @ characters in it.
CSCwh99772	All network device groups are deleted after removing a child item from any group.
CSCwh93498	Cisco ISE 3.1 endpoints purging rule is created automatically when My Devices portal is duplicated.
CSCwh90610	Cisco ISE - Abandoned Jedis connections are not being sent back to the threadPool.
CSCwh41977	Cisco ISE 3.2: Verify existence of Per-User dACL in the Cisco ISE configuration.
CSCwi40089	Allow pxGrid session update publishing without IP Address.
CSCwi45879	Unable to select hotspot portal if an existent or duplicated authorization profile is selected.
CSCwh84446	Guest type save does not work when account expiration notification has special or newline character.
CSCwh71117	Cisco ISE Admin Access: Enabling only "User Services" enables Admin GUI Access as well.
CSCwi33361	Cisco ISE CLI access problems: Failed to connect to server.
CSCwi34117	Grafana UI and Kibana should have RBAC implemented in Identity Services Engine.
CSCwh55667	Cisco ISE Posture Failure: Internal System Error when premier license is disabled.

Caveat ID Number	Description
CSCwi59555	Cisco ISE 3.2 patch 4: ODBC: Search for MAC address in format is ignored.
CSCwi18005	External Radius server list does not show up after upgrading to 3.2.
CSCwi17694	Cisco ISE: synflood-limit does not take effect if configured with more than 10000.
CSCwf34596	User Custom Attributes stuck on rendering.
CSCwe92640	In Cisco ISE 3.1/3.2, the validation for existing routes is missing during CLI configuration.
CSCwi03961	Location group information is missing from policy sets.
CSCwf61657	Gig0 always participates on TCP handshake of sponsor FQDN.
CSCwh77574	Cisco ISE doesn't allow special characters for the password while importing the certificate.
CSCwi59312	Cisco ISE Authorization Profile does not persist data with "Security Group" and "Reauthentication" common tasks.
CSCwh90691	Show CLI command throws exception after configuring log level to 5.
CSCwi59216	Sponsor Portal returns 400 Bad Request when clicking (Contact Support).
CSCwi45131	Apache Struts Vulnerability affecting Cisco Products: December 2023.
CSCwh95022	Sponsor portal shows wrong days of week information from [Setting date] tab when using Japanese UI.
CSCwi52264	Cisco ISE SAML ID provider Configuration Attributes are deleted though they are referenced.
CSCwf31073	Cisco ISE: Error 400 when fetching device admin network conditions through OpenAPI.
CSCwh92117	Sysaux tablespace full due to AUD$ table size growth.
CSCwi25755	Cannot add SAML provider into Cisco ISE 3.2 or higher.
CSCwi23166	Unable to save changes in the patch management condition.
CSCuz65708	FireFox 45+ or Chrome 72: Incorrect line numbering for DACL.
CSCwi34405	Unable to enforce the IdentityAccesssRestricted attribute during authorization.
CSCwi05905	Cisco ISE ERS API /ers/config/deploymentinfo/getAllInfo returns different data on multi-node deployments.
CSCwf80386	Current value of Disable_RSA_PSS environmental value is not preserved upon patch installation.
CSCwi27497	Cisco ISE REST Authentication Service does not run due to iptables error.
CSCwi57950	Cisco ISE 3.2: Nexpose Rapid 7: Strict-Transport-Security malformed.
CSCwc85211	Cisco ISE Passive ID Agent error "id to load is required for loading".
CSCwh93925	When multiple static default routes are present Cisco ISE incorrectly routes RADIUS Traffic.
CSCwi28131	A custom attribute used in a 'never purge' rule is still purges endpoints.

Caveat ID Number	Description
CSCwi59567	Issues with updating the CoA retry count to "0".
CSCwh92185	Radius Authentication reports exported from the Operational Data Purging pages are empty.
CSCwi73984	Cisco ISE 3.1p8 Installed Patches menu does not list all the patches.
CSCwi78722	Azure VM: Not able to register node to deployment.
CSCwh72754	Cisco ISE Active Directory process (lwsmd) is stuck at "Updating" and consumes 90-100% CPU.
CSCwi32576	PSN node crashes while assigning the CPMSessionID.
CSCwi19099	Issue while inserting the data to the config folder if any of the connector is disabled.
CSCwj27469	Cisco ISE 3.3 on Cloud (Azure, AWS, OCI) doesn't read the disk size properly; the size always defaults to 300 GB.

Resolved caveats in Cisco ISE release 3.3 cumulative patch 1

Identifier	Headline
CSCwf80509	Cisco ISE Passive ID sessions are always cleared after an hour.
CSCwh42683	Read-only admin group users have full access when logging into Cisco ISE GUI through SAML authentication.
CSCwh64195	Data corruption is causing an authentication failure with the error messages: FailureReason=11007 or FailureReason=15022.
CSCwf37679	Sponsor permissions are disabled on sponsor portal when accessed from the primary PAN persona.
CSCwf78003	In the pxGrid Endpoints page, the endpoint details are not displayed accurately.
CSCwh17386	The dedicated MnT nodes in a Cisco ISE deployment do not replicate the SMTP configuration.
CSCwe89459	Cisco ISE REST API documentation provides incorrect script while creating endpoint group.
CSCwf25955	A match authorization profile with SGT, VN name, VLAN fields empty causes port to crash.
CSCwh18487	Expired guest accounts don't receive SMS when they try to reactivate account.
CSCwh71273	Disabled essential license leads to limited Cisco ISE GUI page access and inability to regenerate root CA.
CSCwh52589	Acs.Username is not being updated with guest username in first device connection.
CSCwd82539	Local or global exception rules are not matched for authorization policy.
CSCwh06338	GUI doesn't load when trying to edit Client Provisioning Portal config.
CSCwf68108	The OpenAPIs for endpoints are not working for the existing IOT asset attributes.

Identifier	Headline
CSCwd79277	The sync status is displayed as failed when the maximum number of TrustSec objects are selected for syncing.
CSCwh79938	The PreferredDCs registry value cannot be set during advanced tuning.
CSCwe07822	Date of last purge has a wrong timestamp.
CSCwb63834	MNT log processor is enabled on non-MNT admin Cisco ISE node.
CSCwe95624	In Cisco ISE Release 3.2, the SNMP is not working following a node restart.
CSCvz48764	Allow launch program remediation to have a set order.
CSCwh95022	The Sponsor portal shows the wrong days of week information from the [Setting date] tab when using the Japanese Cisco ISE GUI.
CSCwf22794	Inconsistency in VLAN ID results in erorr message: Not a valid ODBC dictionary.
CSCwh69045	In Cisco ISE Release 3.1 Patch 5: Some internal users passwords are not expiring after the configured global password expiry dates.
CSCwe74135	In Cisco ISE Release 3.1 Patch 5: An attempt to remove the guest portal after a PAN failure leads to a ORA-02292 integrity constraint.
CSCwd28431	Removal of EPS from the Cisco ISE code.
CSCvq79397	Cisco ISE GUI pages are not loading properly with custom admin menu workcenter permissions.
CSCwh51156	Cisco ISE cannot load corrupted NAD profiles causing authorization failures with the following reasons: failureReasons 11007 and 15022.
CSCwh47299	Cisco ISE Alarm and Dashboard Summary does not load.
CSCwh51548	Cisco ISE 3.2.0.542: The hot patches are not getting installed when both the patch and hot patches are in ZTP configuration.
CSCwc26835	RADIUS server sequence configuration gets corrupted.
CSCwf44906	Reconfiguring repository with credentials is required following the restoration of a configuration backup.
CSCwf72037	Cisco ISE Release 3.1: Administrator Login Report shows 'Administrator authentication failed' every 5 minutes.
CSCwh36544	pxGrid does not show the topic registration details.
CSCwf39620	Agentless posture is not working in Windows if the username starts with the special character '$'.
CSCwd36753	The AnyConnect posture script does not run when the script condition name contains a period.
CSCwh17448	Cisco ISE Release 3.1: Agentless posture flows fail when the domain user is configured for an endpoint login.
CSCwf72918	In Cisco ISE Release 3.2, the order of the IP name-servers in the running configuration is fallible.

Identifier	Headline
CSCvj75157	Cisco ISE API desn't recognize the identity groups while creating user accounts.
CSCwh63501	Vulnerabilities in log4net 2.0.8.0.
CSCwh47601	Cisco ISE Release 3.2 Patches 2 and 3: Unable to create a user with authorization and privacy password that is equal to 40 characters.
CSCwh58768	Unable to delete existing devices in My Device Portal following a restoration from Cisco ISE Release 2.7.
CSCwd57628	NAD RADIUS shared secret key is incorrect when it starts with an apostrophe on Cisco ISE Release 3.1 Patches 1, 2, 3, 4, and 5.
CSCwh46669	After an admin certificate change, Cisco ISE is not restarting services if the bond interface is configured.
CSCwh17285	Cisco ISE Release 3.2 Patch 3 and Cisco ISE Release 3.3: The initialization of portals fail if *IPV6 enable* is the only IPV6 command on the interface.
CSCwe10898	An endpoint's MAC address is not added to the endpoint identity group when using grace access in the guest portal.
CSCwf07855	Cisco ISE SXP bindings API call returns 2xx response when the call fails.
CSCwh42009	Cisco ISE Release 3.2 Patch 3: The adapter.log remains in the INFO state even if the Cisco ISE GUI configuration is set to TRACE or DEBUG.
CSCwh03740	CRL retrieval is failing.
CSCwf22527	Context visibility: Endpoint custom attributes cannot be filtered with special characters.
CSCwf10516	In Cisco ISE Release 3.2, the authorization policy search feature is not working.
CSCwh05599	Cisco ISE Sponsor Portal is displaying an invalid input error when special characters are used in the guest type.
CSCwh18899	Cisco ISE Open API: /certs/system-certificate/import must support multi-node deployment.
CSCwf88944	Guest portal FQDN is mapped with IP address of the node in the database.
CSCwh23367	In Cisco ISE Release 3.2, the self-registered email subject line truncates everything after the equal (=) sign on the sponsor guest portal.
CSCwf72123	In pxGrid direct, if the user data information is stored in a nested object within the data array, Cisco ISE is unable to process it.
CSCwf80292	Cisco ISE cannot retrieve a peer certificate during EAP-TLS authentication.
CSCvo60450	Cisco ISE: Enhancement for the encryption to only send AES256 for MS-RPC calls.
CSCwf10773	Removing one of multiple DNS servers using "no ip name-server <IP_of_DNS_server>" command restarts Cisco ISE services without a restart prompt.
CSCvw81130	Cisco ISE Release 2.7: Unable to disable the scheduled Active Directory Diagnostic Tool tests.

Identifier	Headline
CSCwh26288	pxGrid Direct: Premier license is required to add a connector. To use the feature, you need the Advantage license.
CSCwf30570	Agentless posture script does not run when the endpoint is not connected to an AC power source.
CSCwf24158	Terms and Conditions check box disappears when Portal Builder is used for Cisco ISE Release 3.0 and later releases.
CSCwf94289	Cisco ISE Release 3.0 Patch 6: Policy export fails to export the policies.
CSCwc39545	DockerMetrics - Report needs to be changed.
CSCwa08802	Cisco ISE Release 3.1 on AWS gives a false negative on the DNS check for Health Checks.
CSCwf09393	Cisco ISE Release 3.1: Services failed to start after restoring a backup from Cisco ISE Release 2.7.
CSCwe15945	Guest account cannot be seen by sponsors in a specific sponsor group.
CSCwf34391	Cisco ISE EasyConnect stitching does not happen when the PassiveID syslog is received by MnT before the active authentication syslog.
CSCwh42442	Cisco ISE Release 3.2 Patch 3: CRL Download failure.
CSCwf79582	The certificates API - /admin/API/PKI/TrustCertificates is not exposed but breaks Cisco DNA Center integration with AD username.
CSCwf14365	"Configuration Missing" warning is seen when navigating to the Log Analytics page.
CSCwh24823	Updates to the internal users using ERS APIs must retain the values of non-mandatory attributes.
CSCwh90691	The Show CLI command throws an exception after configuring the log level to 5.
CSCwf66934	Cisco ISE Release 3.2: GUI issues are noticed in Windows when adding a new context visibility dashboard.
CSCwh14249	Cisco ISE 3.x: There is a spelling mistake in the API gateway settings.
CSCvz86688	Aruba-MPSK-Passphrase needs encryption support.
CSCwf09364	The user identity group and endpoint identity group description fields have a character limit of 1199.
CSCwc04447	Cisco ISE Release 2.7 Patch 6 is unable to filter TACACS live logs by network device IP.
CSCwh30893	Profiling is not processing calling station ID values with the following format: XXXXXXXXXXXX.
CSCwh10401	Cisco ISE Release 3.1 Patch 5: Cannot generate pxGrid client certificate leveraging the CSR option.
CSCwh70275	While registering node with left over certificates from deregistration, the certificates that are currently in use get deleted.
CSCwf47038	Trash all or selected option at pxGrid policy should not touch entries for internal group.
CSCwf07444	Cisco ISE patch GUI installation is stuck on a specific Cisco ISE node in deployment.
CSCwh04251	Cisco ISE agentless posture does not support password containing a colon.

Identifier	Headline
CSCvu56500	An export of all the network devices on Cisco ISE results in an empty file.
CSCwf66237	Cisco ISE: Get All Endpoints request takes a longer time to execute from Cisco ISE Release 2.7.
CSCwf59058	RBAC policy with custom permissions is not working when the administration menu is hidden.
CSCwd97984	Meraki Sync service not running immediately after a Cisco ISE application server restart.
CSCwf66880	Endpoint .csv file import displays "no file chosen" after selecting the file.
CSCwh08408	Cisco ISE Release 3.3 cannot register new nodes to the deployment post upgrade due to the node exporter password not being found.
CSCwf26951	Profiler CoA sent with the wrong session ID.
CSCwh45472	Operational backups from the Cisco ISE GUI to the SFTP repositories fail if the PKI key pair passphrase contains a plus (+) symbol.
CSCwh28528	TopN device admin reports do not work when incoming TACACS exceeds 40M records per day.
CSCwf40265	Cisco ISE Max Session Counter time limit is not working.
CSCwf97173	Asynchronous policy engine affecting CoA for ANC quarantine of active VPN clients.
CSCwh48026	pxgriddirect-connector.log shows a discrepancy between the actual clock time and the time it prints the logs.
CSCwf83193	Unable to login to secondary admin node's GUI using AD credentials.
CSCwf96294	Cisco ISE Release 3.0: A connection attempt to not allowed on the domains.
CSCwd34467	Cisco ISE authorization rule evaluation is broken for attempts using EAP-chaining and Azure AD groups.
CSCwf98849	A critical error seen in Client Provisioning Portal customization.
CSCwf61939	Using an apostrophe in the First Name and/or Last name field presents an invalid name error.
CSCwf64662	SXP can create inconsistent mapping between IP address and SGT.
CSCwc36589	Cisco ISE Intune MDM integration may be disrupted due to end of support for MAC address-based APIs from Intune.
CSCwh18731	Upgrade to Cisco ISE Release 3.2 with LSD disabled prior to the upgrade is causing EP profiler exception.
CSCwc53824	Cisco ISE limits connection to AMP AMQP service to TLSv1.0.
CSCwe53550	Cisco ISE and CVE-2023-24998.
CSCwf82055	Cisco ISE - Unable to disable SHA1 for ports associated with Passive ID agents.
CSCwh53159	Cisco ISE Release 3.1 Patch 7: Unable to change admin password if it contains special character '$'.
CSCwf62744	Add the "disable EDR internet check" tag.

Identifier	Headline
CSCwh26698	Add a mechanism to fetch user data for pxGrid connector.
CSCwh28098	Cisco ISE Release 3.2 Patch 3: CoA disconnect is sent instead of CoA push during posture assessment with the RSD disabled.
CSCwb57672	GCMP256 auth with SHA384withRSA4096 certificate (Android 12 requirement) failing authorization.
CSCwe82004	TCP Socket Exhaustion.
CSCwf98944	Vulnerabilities in axios 0.21.1.
CSCwh38464	Cisco ISE CLI user is unable login after about 2 months of not using the Cisco ISE CLI.
CSCwd21798	Cisco ISE-PIC license expiration alarms.
CSCwf71870	TACACS deployment with 0 days evaluation will not work after registering to smart licensing.
CSCwh46877	Need CoA port-bounce while removing ANC policy with PORT_BOUNCE.
CSCwf62987	Vulnerabilities in AntiSamy 1.5.9.
CSCwh32290	After performing a reset configuration, there is a mismatch in the FQDN value in the GUI and CLI.
CSCwh60726	The Cisco ISE automatic crash decoder is faulty.
CSCwf31477	Profiler is triggering a port bounce when multiple sessions exist on a switch port.
CSCwh71435	Enable password of the internal users is created when it has not been specified through the ERS API.
CSCwf55641	German and Italian emails cannot be saved under Account Expiration Notification in Guest Types.
CSCwf28452	The other conditions are reordered after saving in Client Provisioning Policy.
CSCwh41693	ISEaaS: AWS - Support IMDS v2.
CSCwh05647	Static IPV6 routes are removed after a reload in Cisco ISE Release 3.2.
CSCwh44407	Cisco ISE Release 3.2 API: System certificate import does not work for Cisco ISE node in deployment.
CSCwf27484	Unable to match Azure AD group if the user belongs to more than 99 groups.
CSCwe03624	Smart license registration fails with "communication send error" alarms occur intermittently.
CSCwf81550	Cisco ISE is changing the MAC address format according to the selected MAC Address Format even when it is not a MAC.
CSCwf54680	Unable to edit or delete authorization profiles with parentheses in their names.
CSCwh38484	Manual deletion of the static route will cause Cisco ISE to send a packet with wrong MAC addresses in Cisco ISE Release 3.0 Patch 7.
CSCwf35760	ct_engine is using 100% CPU.
CSCwh39008	Not able to schedule or edit schedule for configuration backup.

Identifier	Headline
CSCwf60904	ANC remediation is not functioning with AnyConnect VPN.
CSCwh03227	Cisco ISE does not consume license when authorization with no authorization profile rule.
CSCwf80951	Cannot edit or create admin user due to "xwt.widget.repeater.DataRepeater" error.
CSCwh51136	Cisco ISE drops RADIUS request with the message "Request from a non-wireless device was dropped".
CSCwh30723	Cisco ISE context visibility does not validate static MAC entries if they miss a separator like colon.
CSCwf59310	Cisco ISE Release 3.1 Patch 7: Context Visibility and pxGrid ContextIn are missing custom attributes.
CSCwf38083	Cisco ISE services are stuck in the initializing state with secure syslogs.
CSCwh35713	ERS SDK developer resources on use cases are not loading properly.
CSCwh03306	Threads get blocked on primary PAN if port 1521 is not available.

Resolved caveats in Cisco ISE release 3.3

The resolved caveats in Cisco ISE Release 3.3, have parity with these Cisco ISE patch releases: 3.2 Patch 2, 3.1 Patch 7, and 3.0 Patch 7.

The following table lists the resolved caveats in Cisco ISE Release 3.3.

Caveat ID Number	Description
CSCwe34204	The Upgrade tab in Cisco ISE shows that the upgrade is in progress after installing a patch.
CSCwd07345	Cisco ISE privilege escalation vulnerability.
CSCwc50392	The *fetch* command of ROPC groups with nearly 53k groups is not working in the Cisco ISE GUI.
CSCwf15717	In Cisco ISE Release 3.2, the System 360 feature is not available with the Device Admin license.
CSCwe37377	The Cisco ISE CRL Retrieval Failed alarm needs to display the server on which the CRL download failed.
CSCwc33290	Unable to delete custom endpoint attribute in Cisco ISE.
CSCvr79992	The Session.CurrentDate attribute is not calculated correctly during authentication of endpoints in Cisco ISE.
CSCwd48787	The Cisco ISE - SSL buffer is causing problems with PAC decryption. This is affecting the EAP-FAST flows in Cisco ISE.
CSCwe68336	Posture assessment by condition generates the following invalid identifier: ORA-00904: "SYSTEM_NAME" in the Cisco ISE GUI.
CSCwd07349	Cisco ISE command injection vulnerability.
CSCwd27865	The Configuration Changed field is not working when assigning an endpoint to a group in Cisco ISE.
CSCwf14957	The TrustSec status cannot be changed if you are using the Japanese Cisco ISE GUI.

Caveat ID Number	Description
CSCwe69085	The Policy Service Node is not accessible in the Cisco ISE GUI when the Device Administration license is enabled.
CSCwc33751	In Cisco ISE Release 3.1, the copy command using the TFTP protocol times out.
CSCwd97022	In Cisco ISE Release 3.2 patch 3, the disabled Cisco ISE-PIC smart license is being used erroneously for upgrade.
CSCwd46505	The queue link error alarms are not displayed in Cisco ISE-PIC nodes.
CSCwd07340	Cisco ISE privilege escalation vulnerability.
CSCwc39320	Cisco ISE nodes upgraded using the CLI do not progress beyond the "Upgrading" status in the Cisco ISE GUI.
CSCwd93719	Cisco ISE XML external entity injection vulnerability.
CSCwe18359	Vulnerabilities in Sudo 1.8.29 (a third-party software) have been fixed.
CSCwd63749	In Cisco ISE Release 3.1, the Active Directory Retrieve Groups window displays a blank screen when loading a large number of Active Directory groups.
CSCwd24089	Unable to launch Cisco ISE Release 3.2 in Safe Mode.
CSCwb92655	Common Policy (CDP) is not enabled by default in Cisco ISE Releases 3.1 and 3.2.
CSCwb77915	Use the toggle button to enable or disable RSA PSS ciphers based on policy under Allowed Protocols in the Cisco ISE GUI.
CSCwd30994	When a default static route is configured with an interface's subnet gateway excluding Giganet 0, the network connectivity to Cisco ISE is lost.
CSCwe55215	Cisco ISE smart licensing now uses smart transport.
CSCwd35608	The CoA is failing in Cisco ISE due to usage of old and stale audit session IDs.
CSCwc61320	Users may experience some slowness on Support Bundle page because of the Download Logs page loading in the background.
CSCwc58608	Cisco ISE Release 3.2 is cashing as soon as a RADIUS request is received with EAP-FAST and EAP Chaining.
CSCvt62460	Unable to retrieve groups from different LDAPs when nodes are using servers that are undefined.
CSCwd70902	PRRT should be sending unfragmented messages to the monitoring node if IMS is enabled.
CSCwe49261	Cisco ISE PassiveID agent probes the status of all domains (including domains that do not have a PassiveID configuration).
CSCwc95878	There are intermittent issues with app activation.
CSCwd13201	The Cisco ISE GUI crashes while loading the authorization policy on Google Chrome and Microsoft Edge browsers.

Caveat ID Number	Description
CSCwc57294	The duplicate manager doesn't remove relevant packets when there is an exception in the reading configuration.
CSCwe07354	The RADIUS token server configuration accepts empty host IP address for secondary server.
CSCwd57071	The self registration portal does not support the FQDNs of the nodes for the Approve/Deny links sent to the sponsors.
CSCwf26973	Network Device Group information missing when a Cisco ISE admin account has only read access.
CSCwd27506	In Cisco ISE Release 3.0 patch 6, the scheduled reports created by external admins are missing.
CSCwc79321	Unable to change the identity source from internal source to external source in the RSA/RADIUS-token server.
CSCwd41773	In Cisco ISE Release 3.1, the application server crashes if CRL of 5 MB or more is downloaded frequently.
CSCwd97606	Multiple requests for the same IP, VN, and VPN combinations with different session IDs is creating duplicate records in Cisco ISE.
CSCwe63320	Cisco ISE Releases 3.2, 3.1, and 3.0 display mismatched information on the "Get All Endpoints" report.
CSCwe54466	A sponsor portal print issue in Cisco ISE displays guest user settings based on From-First-Login guest account setting instead of the configured purge settings.
CSCwc62419	Cisco ISE insufficient access control vulnerability.
CSCwe33360	The anomalous behavior detection is not working as expected in Cisco ISE.
CSCwe69179	The latest IP access restriction configuration removes the previous configuration in Cisco ISE.
CSCwd90613	The RADIUS server sequence page displays "no data available".
CSCwd30433	The email notification when a guest account creation is denied is not sent to the admin.
CSCwc86067	Cisco ISE authorization bypass vulnerability.
CSCwd31524	Cisco ISE Release 3.2 does not support 16-character passwords for SFTP configuration.
CSCwd12357	The SXP service gets stuck in the initial setup due to an exception on 9644.
CSCwd41219	Cisco ISE command injection vulnerability.
CSCwf19811	In Cisco ISE Release 3.1, the SXP Bindings report displays the "No data found" error.
CSCwe70402	Cisco ISE 3.2 does not support portal customization scripts that include single-line JavaScript comments.
CSCwe15315	The TrustSec PAC Information Field attribute values are lost when importing a network device CSV template file.
CSCwe37978	Scheduled reports with large data sizes are displayed as "empty" in the Cisco ISE repository.
CSCwd87161	In Cisco ISE Release 3.1, the certificate-based login asks for license files only if the Device Admin license is enabled.

Caveat ID Number	Description
CSCwe22934	Cisco ISE authentication latency is observed because of devices with no MAC addresses.
CSCwe43002	"Read-only Admin" not available for Cisco ISE admin SAML authentication.
CSCwe64558	The Cisco ISE admin account created from network access users can't change dark mode settings in the Cisco ISE GUI.
CSCwd30038	Cisco ISE command injection vulnerability.
CSCwd30039	Cisco ISE command injection vulnerability.
CSCwd07350	Cisco ISE path traversal vulnerability.
CSCwd28431	Endpoint Protection Service has been removed from the Cisco ISE code.
CSCwc93253	The Cisco ISE network device captcha is prompted only when the filter matches a single network device.
CSCwd51812	Certificate authentication permissions in the Cisco ISE GUI have been modified for Cisco ISE Release 3.1 patch 4.
CSCwc64346	The Cisco ISE ERS SDK documentation for network device bulk requests is incorrect.
CSCwd31137	Scheduled RADIUS authentication reports in Cisco ISE fail while exporting them to the SFTP repository.
CSCwc48509	Windows server 2022 is working as the target domain controller and should be monitored.
CSCwc47015	The resolution for CSCvz85074 breaks AD group retrieval in Cisco ISE.
CSCwe52296	The Cisco ISE MNT authentication status API query should be optimized.
CSCvg66764	The Cisco ISE-PIC agent provides session stitching support.
CSCwf33128	The RADIUS used space in Cisco ISE reports incorrect usage. This is because it also takes TACACS tables into account for the final report.
CSCwf02093	In Cisco ISE Release 3.2, hyper-V installations have DHCP enabled.
CSCwb83304	Cisco ISE upgrade is failing because of custom security groups.
CSCwc47799	Cisco ISE does not display an error message when importing a certificate and private key that contains "%" in the password.
CSCwd32591	In Cisco ISE Release 3.2, the SFTP repositories are not operational from the Cisco ISE GUI even after clicking the "generate key pairs" option.
CSCwd42311	Unable to download REST-ID stores from Download Logs on the Cisco ISE GUI.
CSCwd48000	Vulnerabilities in TomCat 9.0.14.
CSCwc31482	The NetworkSetupAssistance.exe digital signature certificate is expired in the BYOD flow when using Sierra Pacific Windows (SPW windows in Microsoft Windows).
CSCwd92324	Cisco ISE Release 3.2 ROPC basic serviceability improvements.

Caveat ID Number	Description
CSCwe12098	In Cisco ISE Release 3.2, the ports for Guest Portal configuration do not open on Cisco ISE nodes that are installed on AWS.
CSCwf21585	Using potentially insecure methods - HTTP PUT method accepted.
CSCwe49422	From Cisco ISE Release 3.2, text passwords must be entered in the identity-store command.
CSCwe96633	The support bundle does not contain tterrors.log and times.log.
CSCwd19529	Cisco ISE stored cross-site scripting vulnerability.
CSCwf22799	The deferrred update condition will not work if the compliance module is not compatible with Cisco Secure client.
CSCwc91917	Users cannot add the quotation character in a TACACS authorization profile.
CSCwc85920	Cisco ISE TrustSec Logging: The SGT create event is not logged to ise-psc.log file.
CSCwd97353	Automatic backup stops working after 3 to 5 days.
CSCwd71574	High CPU utilization due to agentless posture configured in Cisco ISE.
CSCwe27146	Unable to parse CLI Username with '-' (hyphen/dash) in Cisco ISE Release 3.2 Patch 1.
CSCwc69492	Metaspace exhaustion causes crashes on the Cisco ISE node in Cisco ISE Release 3.1.
CSCwe97989	Cisco ISE Release 3.2 crashing with VN in authorization profile.
CSCwd24304	Cisco ISE Release 3.2 ERS POST /ers/config/networkdevicegroup fails has the broken attribute othername/type/ndgtype.
CSCvz68091	Configuration changes to guest types are not updated in the audit reports.
CSCwe70889	Full upgrade from Cisco ISE Release 3.0 to Cisco ISE Release 3.1 failed due to DB service timeout.
CSCwd92835	Network Device Profile shows HTML code as name.
CSCwe50710	In Cisco ISE Release 3.2, an error is displayed when entering the DNS domain in the Cisco ISE deploy instance on cloud.
CSCwe49167	In Cisco ISE Release 3.2, the SAML sign authentication request setting is getting unchecked upon saving the setting.
CSCwf33881	In Cisco ISE Release 3.2 Patch 1, connections are established to servers not listed in the Cisco ISE ports, resources, or the reference guide.
CSCwc44580	Cisco ISE Release 3.1 creates cni-podman0 interface with IP 10.88.0.1 and IP route for 10.88.0.0/16.
CSCwe14808	Cisco ISE fails to translate AD attribute of msRASSavedFramedIPAddress.
CSCwe57764	The MDM connection to Microsoft SCCM fails after Windows DCOM Server Hardening for CVE-2021-26414.

Caveat ID Number	Description
CSCwf17490	Post service licensing update, the Cisco ISE Licensing page shows Evaluation compliance status for consumed licenses.
CSCwd78306	The ROPC authentication functionality is broken in Cisco ISE Release 3.2.
CSCwf13630	The monitoring log processor service stops every night.
CSCwd38766	Deleting SNMPv3 username with "-" or "_" character doesn't delete the hexadecimal username from Cisco ISE.
CSCvy69943	Allow Guest Portal HTTP requests containing content-headers with {} characters.
CSCwe78540	IotAsset information is missing when using Get All Endpoints.
CSCwd07351	Cisco ISE command injection vulnerability.
CSCwd05697	The guest locations do not load in the Cisco ISE Guest Portal.
CSCwd03009	RMQForwarder thread to control platform properties in the hardware appliance in Cisco ISE Release 2.7 patch 7.
CSCwc74531	The Cisco ISE hourly cleanup should clean the cached buffers instead of the 95% memory usage.
CSCwd41018	Cisco ISE command injection vulnerability.
CSCwd16837	Cisco ISE OpenAPI HTTP repo patch install fails when direct listing is disabled.
CSCwa62202	Cisco ISE with two interfaces configured for portal access is broken.
CSCwe24932	Agentless posture fails when using multiple domain users in the endpoint login configuration.
CSCwc48311	Cisco ISE vPSN with IMS performance degrades by 30-40% compared to UDP syslog.
CSCwa55233	Queue link errors "Unknown CA" when utilizing third-party signed certificate for IMS.
CSCwf42496	Attempt to delete "Is IPSEC Device" NDG causes all subsequent RADIUS/TACACS+ authentications to fail.
CSCwd41651	The vertical scroll bar is missing in RBAC Data and Menu Permissions window in Cisco ISE Release 3.1.
CSCwe86793	Cisco ISE filter of REST ID Store Groups displays "Error processing this request."
CSCwe40577	Failed to handle API resource request: Failed to convert condition.
CSCwd16657	Cisco ISE arbitrary file download vulnerability.
CSCwf10004	ISE IP SGT static mapping is not sent to SXP Domain upon moving it to another mapping group.
CSCwc75572	Primary administration node application server remains stuck at the initializing stage.
CSCvv90394	Cisco ISE Release 2.6 patch 7 is unable to match "identityaccessrestricted equals true" in the authorization policy.

Caveat ID Number	Description
CSCwe11676	Data is lost when accessing Total Compromised Endpoints in the Cisco ISE dashboard Threat for TC-NAC.
CSCwe13780	Cisco ISE is unable to join node to AD by REST API.
CSCwd45843	Authentication step latency for policy evaluation due to garbage collection activity in Cisco ISE.
CSCwd78028	Cisco ISE - Apache TomCat vulnerability CVE-2022-25762.
CSCwc74206	Cisco ISE 3.0 is not saving SCCM MDM server objects with new password but works when a new instance is in use.
CSCwe07406	Error loading page error is the output when creating a guest account in the Self-Registered Guest Portal in Cisco ISE.
CSCwe38610	Make MDM API V3 certificate string case insensitive.
CSCwc44614	Using "Export Selected" under Network Devices leads to the login screen with more selections.
CSCwe24589	Cisco ISE Release 3.2 URT fails with "Failed (Import into cloned database failed)" on Cisco ISE Release 3.1.
CSCwe92624	Cisco ISE Africa or Cairo timezone DST.
CSCwd26845	APIC integration in Cisco ISE Release 3.2 is missing fvIP subscription.
CSCwc70197	Cisco ISE Certificate API fails to return Trusted Certificate with hash character in the Friendly Name field.
CSCwe12618	APIC integration in Cisco ISE Release 3.2 fails to get EPs null (com.cisco.cpm.apic.ConfImporter:521).
CSCwc98828	Cisco ISE interface feature insufficient access control vulnerability.
CSCwc98824	Posture Requirements only show the default entry in Cisco ISE.
CSCwe41824	Cisco ISE Release 3.2 is missing secondary policy administration node key for PKI-based SFTP.
CSCvo61351	Cisco ISE Live Session gets stuck at "Authenticated" state.
CSCwc88848	Cisco ISE Release 3.1 Patch 1 does not create the Rest ID or ROPC folder logs.
CSCvy69539	CIAM: openjdk - multiple versions.
CSCwc57240	Cisco ISE GUI is not validating the default value while adding custom attributes.
CSCvy88380	Unable to select ISE Messaging usage (appears grayed out) for an existing certificate in the Cisco ISE GUI.
CSCwf05309	Cisco ISE SAML certificate is not replicating to other nodes.
CSCwe94012	Evaluate Configuration Validator gets stuck when using a password with special characters in Cisco ISE.
CSCwa52678	Cisco ISE GUI TCP DUMP gets stuck in the "Stop_In_Progress" state.
CSCwc62716	IndexRebuild.sql script ran over the monitoring node in Cisco ISE.

Caveat ID Number	Description
CSCwd63661	Entering the incorrect password in the Cisco ISE GUI shows the end user agreement in Cisco ISE Release 3.1 patch 1.
CSCwc65802	Save button for SAML configuration is grayed out in the Cisco ISE GUI.
CSCwe17953	Cisco ISE path traversal vulnerability.
CSCwe17338	Hostnames on Cisco ISE should not exceed 19 characters when deployed via AWS.
CSCwc65711	MAC - CSC 5.0554 web deployment packages failed to upload.
CSCwc62415	Cisco ISE unauthorized file access vulnerability.
CSCwe43468	Static IP-SGT mapping with VN reference causes Cisco DNA Center Group-Based Policy sync to fail.
CSCwd71496	Cisco ISE is not deleting all the sessions from the SXP mapping table.
CSCvv10712	The transaction table should be truncated after a 2 million record count.
CSCwc62413	Cisco ISE cross-site scripting vulnerability.
CSCwc13859	Unable to create a scheduled backup with the admin user from "System Admin" AdminGroup in Cisco ISE.
CSCwf26226	CPU spike due to memory leak with EP purge call.
CSCwf40128	Accept client certificate without KU purpose validation per CiscoSSL rules.
CSCwc20314	PIC license consumption in Cisco ISE-PIC Release 3.1.
CSCwe00424	Cisco ISE- SQLException sent to the Collection Failure Alarm caused by NAS-Port-ID length.
CSCwc98833	Cisco ISE cross-site scripting vulnerability.
CSCwc98831	Cisco ISE stored cross-site scripting vulnerability.
CSCwe86494	Cisco ISE displaying Tomcat stacktrace when using a specific URL.
CSCwd97582	Cisco ISE Release 3.1 patch 5 verifies CA certificate EKU causing the "unsupported certificate" error.
CSCwe37041	Internal CA certificate chain becomes invalid if the original primary administration node is removed.
CSCwe52461	Unable to enable the firewall condition in Cisco ISE Release 3.1.
CSCwa82521	There are issues in the Trusted Certificates menu in Cisco ISE Release 3.1.
CSCwd41098	Getting pxGrid error logs in ise-psc.log after disabling pxGrid.
CSCwd24286	Cisco ISE is not sending the hostname attribute to Cisco DNA Center.
CSCwd74898	"Posture Configuration detection" alarms should be at the "INFO" level and must be reworded.
CSCwe36788	In Cisco ISE Release 3.2, users are not able to delete the rules that were added during IP access rule addition.

Caveat ID Number	Description
CSCwc81729	"All devices were successfully deleted" error after trying to delete one particular network access device by filtering.
CSCwd74560	PUT operation failing with payload via Cisco DNA Center to Cisco ISE (ERS).
CSCwc42712	Cisco ISE RADIUS and PassiveID session merging.
CSCwd15888	Not able to access Time Settings Configuration Export on Cisco ISE ERS API.
CSCwc15013	Add serviceability & fix "Could not get a resource since the pool is exhausted" Error in Cisco ISE Release 3.0.
CSCwf26482	REST AUTH services not running after upgrading from Cisco ISE Release 3.1 to Cisco ISE Release 3.2.
CSCwe37018	Cisco ISE integration with Cisco DNA Center fails if there are invalid certificates in the Cisco ISE trusted store.
CSCwd05040	Unable to import certificates on Secondary node post registration to the deployment.
CSCwd31405	Latency is observed during query of Session.PostureStatus.
CSCwe36242	TACACS Command Accounting report export is not working.
CSCwe15576	Not able to configure KRON job.
CSCwb18744	SG and contracts with multiple backslash characters in a row in the description cannot sync to Cisco ISE.
CSCwe70975	In Cisco ISE, the SMS Javascript customization is not working for SMS email gateway.
CSCwc85867	Cisco ISE Change Configuration Audit Report does not clearly indicate the SGT creation and deletion events.
CSCwc66841	CIAM: openjdk - multiple versions.
CSCwd51409	Cisco ISE cannot retrieve repositories and scan policies of Tenable Security Center.
CSCwd79921	Cisco ISE arbitrary file download vulnerability.
CSCwd13555	Cisco ISE abruptly stops consuming passive-id session from a third-party syslog server.
CSCwe13110	Cisco ISE Release 3.1 configuration backup is executed on the primary monitoring node.
CSCwd70658	Unable to add Network Access Device due to the error: "There is an overlapping IP Address in your device".
CSCwd63717	PKI-enabled SFTP Repositories not working in Cisco ISE Release 3.2.
CSCwe45245	Smart license registration is not working.
CSCwe99961	Sponsored Portal in Germany - Calendar shows Thursday (Donnerstag) as Di not Do.
CSCwf23981	Cisco ISE Authorization Profile displays wrong Security Group or VN value.
CSCwd73282	In Cisco ISE Release 3.1 Patch 3, the Sponsor Portal - Session Cookie SameSite value set to none.

Caveat ID Number	Description
CSCwc80243	Cisco ISE TCP DUMP stuck at the error "COPY_REPO_FAILED" state when no repository is selected.
CSCwe54318	SXP service gets stuck at initializing due to H2 DB delay in querying bindings.
CSCwc23593	LSD is causing high CPU usage.
CSCwf09674	Registered Endpoint Report shows unregistered guest devices.
CSCwc93451	Profiler should ignore non-positive RADIUS syslog messages while forwarding the messages from the default RADIUS probe.
CSCwc85546	In Cisco ISE Release 3.1, the error "Illegal hex characters in escape (%) pattern ? For input string: ^F" is displayed.
CSCwf40861	The Cisco ISE GUI shows HTML hexadecimal code for the characters in the command set.
CSCwf36285	The row of "Manage SXP Domain filters" only displays maximum 25.
CSCwe53550	Cisco ISE and CVE-2023-24998.
CSCwe30235	Vulnerabilities in jszip 3.0.0.
CSCwf44942	Cisco ISE TACACS primary service node crashed during maximum user session authentication flow.
CSCwc80844	Cisco ISE VMSA-2022-0024 - VMware Tools update addresses a local privilege escalation vulnerability.
CSCwe84210	Authorization policy evaluation failing due to NullPointerException in LicenseConsumptionUtil.java.
CSCwd10864	Cisco ISE XML external entity injection vulnerability.
CSCwe36063	No validation of PBIS registration key configuration on the advance tuning page.
CSCwe25138	Identity user cannot be created if the user custom attribute includes $ or ++.
CSCwd13425	Patch install from the Cisco ISE GUI fails.
CSCwe69189	LSD is causing high bandwidth utilization.
CSCwd98296	Network Device Port Conditions: IP Addresses or Device Groups don't accept valid port strings.
CSCwc36987	Cisco ISE BETA certificate is shown as stale certificate and must be cleaned up.
CSCwd31414	The Guest portal page displays "Error Loading Page" when the reason for the visit field contains special characters.
CSCwd39056	Cisco ISE Release 3.1 Patch 4 Passive DC configuration is not saving the username correctly.
CSCwd45783	pxGrid session publishing stops when reintegrating FMC while P-PIC is down.
CSCwf21960	During upgrade the deregister call fails to remove all the nodes from the database.
CSCwd82119	EAP-TLS authentication with ECDSA certificate fails on Cisco ISE Release 3.1.
CSCwc53895	In Cisco ISE Release 3.1 Patch 3, SAML SSO does not work if the active policy service node goes down.

Caveat ID Number	Description
CSCwe61215	SFTP and FTP validation is failing through CLI when 16+ characters in the password is configured.
CSCvz08319	Cisco ISE's Application Server process is restarting during Dot1X due to buffer length = 0 for eapTLS.
CSCwc99178	Unable to add many authorization profiles with the active sessions alarm setting.
CSCwd10997	Node syncup fails to replicate wildcard certificate with the portal role.
CSCwe63873	Qualys adapter is unable to download the knowledge base: Stuck with the error "knowledge download in progress".
CSCwc65821	Cisco ISE ERS API doesn't allow for use of minus character in "Network Device Group" name.
CSCwd12453	Cisco ISE Release 3.1 portal tag has an issue with special character validation.
CSCwa37580	Cisco ISE Release 3.0 NFS share stuck.
CSCwe53921	Support for concatenating AD group attributes when they exceed the length of the RADIUS attribute.
CSCwc44622	The session gets stuck indefinitely until Cisco ISE is restarted.
CSCwd84055	Cisco ISE Release 3.1 Azure AD autodiscovery for MDM API V3 is incorrect.
CSCwe92177	In Cisco ISE, the Mexico time zone incorrectly changes to Daylight Saving Time.
CSCwd68070	Import of SAML metadata fails.
CSCwe71804	In Cisco ISE Release 3.1, certain key attributes in the SessionCache are missing when a third-party network device profile is in use.
CSCwc76720	Cisco ISE Release 3.1 displays an error when using the SNMPv3 privacy password.
CSCvx15522	The command to enable DNSCache in FQDN syslog popup needs correction.
CSCwc99664	Support for macOS 12.6.
CSCwe71729	In Cisco ISE Release 3.2, the Data Connect password expiry alarm is consistently visible even when the Data Connect feature is disabled.
CSCwd57978	All network access devices are deleted while filtering based on NDG location and IP address.
CSCwe39781	Cisco ISE does not remove SXP mapping when the SGT changes after CoA.
CSCwc64480	Cisco ISE fails to establish a secure connection when new certificates are imported for the guest portal.
CSCwd38137	Cisco ISE XML external entity injection vulnerability.
CSCwf28229	VLAN detection interval should not be more than 30 seconds.
CSCwc26482	The Replogns table space on the primary administration node increases when there are replication issues in the deployment.
CSCwf19039	Agentless posture failures cause the TMP folder to increase in size in Cisco ISE Release 3.1 Patch 5.

Caveat ID Number	Description
CSCwd57752	DB Connections are increasing in longevity and the maximum DB connections are 994 in Cisco ISE Release 3.1 Patch 5.
CSCwe44750	The reprofiling result is not updated to Oracle/VCS after a feed incremental update.
CSCwd54844	Cisco ISE ERS API schema for network device group creation.
CSCwe49183	Cisco ISE SAML Destination attribute is missing for signed authorization requests.
CSCwd39746	MSAL support is needed for SCCM integration with Cisco ISE as MS is deprecating ADAL.
CSCwc87670	In Cisco ISE Release 3.1 patch 3, users are unable to import endpoints from .csv file if SAML is used.
CSCwd82134	Incorrect SLR out of compliance error reported in Cisco ISE.
CSCwe80760	Unable to save the launch program remediation when the parameter contains a double quote ("").
CSCwd64649	Cisco DNA Center integration issue due to more internal CA certificates.
CSCwd69072	Session directory write failed alarm with Cisco NAD using "user defined" NAD profile.
CSCvz86446	SyncRequest timeout monitor thread does not terminate the file transfer after timeout during Cisco ISE replication.
CSCwc55529	Authentication failed due to missing certificate private key.
CSCwc07082	"The phone number is invalid" error is displayed when trying to import users from .csv file.
CSCwe37826	Users cannot change the condition operator from AND to OR in posture policy conditions.
CSCwe34566	Authentication against ROPC identity store fails with RSA key generation error.
CSCwf22816	Authorization policy failing due to wrong condition evaluation.
CSCwc91923	Uploading the AnyConnect agent from the Cisco ISE GUI triggered high CPU utilization on the primary administration node and took nearly 7 hours to complete.
CSCvw59025	Misspelled PassiveID errors seen in logs and reports.
CSCwc60997	The SAML flow with load balancer is failing due to incorrect token handling on Cisco ISE.
CSCwc49580	The Adaptive Network Control (ANC) CoA is sent to the NAS IP address instead of the Device IP address.
CSCwe87660	In Cisco ISE Release 3.1, the previous version of the hot patch is still visible in the DB.
CSCwe49504	Cisco ISE Release 3.2 does not support passwords with more than 16 characters for the identity-store configuration command.
CSCwb72948	Unable to access the system certificates page for the registered node in Cisco ISE Release 3.0 patch 4.
CSCwf32255	No response received from SNMP server when the "snmp-server host" is configured in Cisco ISE Release 3.2 patch 2.
CSCwe96739	TLS 1.0/1.1 is accepted in the Cisco ISE Release 3.0 admin portal.

Caveat ID Number	Description
CSCwe98676	Vulnerable JS library issue found while executing ZAP.
CSCwe39262	Passive ID agent sending incorrect time format events.
CSCwf15130	Permission for collector.log file is set to root automatically.
CSCwe30606	Unable to download the support bundle of size greater than 1 GB from the Cisco ISE GUI.
CSCvv99093	Cisco ISE nodes intermittently trigger the queue link alarms.
CSCwd61906	Sysaux tablespace allocation should be done based on the profile of the node.
CSCwf16165	An NTP authentication key with more than 15 characters is getting the error "% ERROR: Bad hashed key".
CSCwc98823	Cisco ISE command injection vulnerability.
CSCwf19463	Layering of drag and drop action in the Conditions Studio.
CSCwc03220	Removing an IP access list from Cisco ISE destroys the distributed deployment.
CSCwe59587	Some items are displayed as [Test] in the Japanese Cisco ISE GUI.

Open caveats

Open caveats in Cisco ISE release 3.3 cumulative patch 12

Any unresolved issue from a previous release remains applicable to subsequent releases until it is resolved.

Caveat ID Number	Description
CSCwt34939	Extracting the GUID from the SAN URI causes an incorrect epid assignment.
CSCwv09701	Creating an endpoint statically or through import is not allowed because of the RCM flow.
CSCwu54421	An unvalidated endpoint owner lookup causes a `NullPointerException` when endpoint ownership is transferred in the RCM state machine.
CSCww18723	An epid is not generated when RCM merge is disabled.
CSCww19459	Endpoint purge VCS evaluation skips all endpoints when RCM is disabled.

Open caveats in Cisco ISE release 3.3 cumulative patch 11

Caveat ID Number	Description
CSCwt99926	When upgrading from Cisco ISE release 3.3 patch 11 split upgrade to Cisco ISE release 3.4 patch 6, the former PPAN (second iteration) is getting stuck at app server start.

Open caveats in Cisco ISE release 3.3 cumulative patch 10

Any unresolved issue from a previous release remains applicable to subsequent releases until it is resolved.

Open caveats in Cisco ISE release 3.3 cumulative patch 9

Any unresolved issue from a previous release remains applicable to subsequent releases until it is resolved.

Open caveats in Cisco ISE release 3.3 cumulative patch 8

Caveat ID Number	Description
CSCws51319	After upgrading to Cisco ISE release 3.3 patch 8, network access devices cannot download SGACLs from Cisco ISE.
CSCws52326	After installing Cisco ISE release 3.3 patch 8, Cisco ISE does not correctly evaluate custom attributes for endpoints shown on the Context Visibility page. As a result, authorization rules that use custom attributes may be matched inaccurately, causing incorrect authorization profiles to be assigned.

Open caveats in Cisco ISE release 3.3 cumulative patch 7

Any unresolved issue from a previous release remains applicable to subsequent releases until it is resolved.

Open caveats in Cisco ISE release 3.3 cumulative patch 6

Any unresolved issue from a previous release remains applicable to subsequent releases until it is resolved.

Open caveats in Cisco ISE release 3.3 cumulative patch 5

Caveat ID Number	Description
CSCwo33728	Scheduled exports are failing on the Cisco ISE Release 3.3 Patch 5 Longevity setup.
CSCwp01022	Guest, Sponsor, Certificate, and Posture portals do not load after upgrading to Cisco ISE release 3.3 patch 5 version.
CSCwo56178	Cisco ISE Release 3.5 - The 'Resettodefault' command does not reset the max file size and count levels in secondary nodes in a deployment.
CSCwn09515	PnS Longevity: High allocations in the Profiler are causing high GC activity, and HAL is also observed.
CSCwh77618	ISE RMQ full: High latency exists between ISE nodes with EPO enabled.
CSCwo37235	Not all nodes are listed on the Grafana Monitoring dashboard.
CSCwo59299	ISE RADIUS DTLS fails to accept an ECDHE client certificate that has the KeyAgreement key usage for ECDHE-ECDSA.

Open caveats in Cisco ISE release 3.3 cumulative patch 4

Caveat ID Number	Description
CSCwn34778	Authentication session does not match with an MDM policy despite having the MDM attributes.

Open caveats in Cisco ISE release 3.3 cumulative patch 3

Caveat ID Number	Description
CSCwf79582	AD credentials fail to integrate Cisco ISE with Cisco Catalyst Center 2.2.1.x and later.
CSCwk67747	RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS).
CSCwk79546	Cisco ISE 3.3 Patch 3 DUO MFA authentication fails instantly with a "22076 MFA Authentication failure" message in Live Logs. You must install the following hot patch to fix this issue: HP_3.3P3.zip

Open caveats in Cisco ISE release 3.3 cumulative patch 2

Caveat ID Number	Description
CSCwf36985	AD group retrieval fails while evaluating authorization policy.
CSCwh25160	Swap cleanup script to drop the swap area and program the cron.
CSCwh69267	Post Adeos restore, appserver stuck at initializing.
CSCwh92366	In Cisco ISE 3.1 Patch 8, observing insufficient virtual machine resource alarm in 3.1 Patch 8 longevity setup.
CSCwi61950	Cisco ISE is running out of Context N.
CSCwi89725	Make the PAN to honor the endpoint from DB when purging by purge routine on PAN only.
CSCwj12359	Interrupting execution of "show tech-support" causes services to stop on Cisco ISE.
CSCwj38688	Host not found in identity group due to profiler null pointer exception.
CSCwj44649	In Cisco ISE 3.3, TACACS data is not retained and everything gets purged.

Open caveats in Cisco ISE release 3.3 cumulative patch 1

Caveat ID Number	Description
CSCwe92640	Cisco ISE Releases 3.1 and 3.2: Missing validation for existing routes during CLI configuration.
CSCwf55795	In Cisco ISE Release 3.2 Patch 1, the Cisco ISE GUI and CLI are inaccessible following a configuration restoration with ADE-OS.

Caveat ID Number	Description
CSCwh92366	In 3.1 Patch 8: Observing Insufficient Virtual Machine Resource Alarm in 3.1Patch 8 Longevity setup.

Open caveats in Cisco ISE release 3.3

The following table lists the open caveats in Release 3.3.

Caveat ID Number	Description
CSCwf78050	Enabling log analytics in lower models 3615/3715 may cause Cisco ISE to become unresponsive.
CSCwf02597	Cisco ISE Release 3.3: ML on Cisco ISE: Cisco ISE cluster will not be able to connect to ML cloud if clock diff is more than 5 minutes.
CSCwf49520	Cisco ISE Release 3.3: Labelling ML-proposed rule has issues with special character and overlapping.
CSCwf76160	MFC profiler shows "No data" for all the metrics in grafana dashboard.
CSCwf69829	Cisco ISE Release 3.3: MFC_EPType isn't showing as Phone for iPhone in case of Wi-Fi analytics.
CSCwf14365	"Configuration Missing" warning seen when browsing to log analytics page.
CSCwh36667	Cisco ISE monitoring GUI page stuck at "Welcome to Grafana".
CSCwh08408	Cisco ISE Release 3.3 cannot register new nodes to deployment post upgrade due to node exporter password not found.
CSCwh92366	In 3.1 Patch 8: Observing Insufficient Virtual Machine Resource Alarm in 3.1Patch 8 Longevity setup
CSCwm05210	Getting '500 internal error' when sending ISE 9060/ers/config/endpoint/{MAC address}/releaserejectedendpoint
CSCwn62873	Known issue with Cisco ISE integration with Active Directory on Windows server 2025.

Additional references

Refer to Cisco ISE collection pages for additional resources that you can use when working with Cisco ISE.

Communications, services, and additional information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

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)

© 2024–2026 Cisco Systems, Inc. All rights reserved.