



# Release Notes for Cisco Identity Services Engine, Release 3.3

---

**First Published:** 2023-07-05

**Last Modified:** 2024-08-12

## 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 the public cloud.

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

For detailed Cisco ISE ordering and licensing information, see the [Cisco Identity Services Engine Ordering Guide](#).

For information on monitoring and troubleshooting the system, see the "Monitoring and Troubleshooting Cisco ISE" section in the [Cisco Identity Services Engine Administrator Guide](#).

## What Is New In Cisco ISE, Release 3.3?

This section lists the new and changed features in Cisco ISE 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 Access > 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 the native IPSec configuration. You can use native IPSec 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 Probe
- 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 Visibility" 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 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*.

## System Requirements

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

For more details on hardware platforms and installation of this Cisco ISE release, see the [Cisco Identity Services Engine Hardware Installation Guide](#).

## Supported Hardware

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

**Table 1: Supported Platforms**

Hardware Platform	Configuration
Cisco SNS-3615-K9 (small)	For appliance hardware specifications, see the <a href="#">Cisco Secure Network Server Appliance Hardware Installation Guide</a> .
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)	



**Note** 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
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.

## Supported Virtual Environments

Cisco ISE supports the following virtual environment platforms:

- Cisco ISE Release 3.3 is the last release to support VMware ESXi 6.7.

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

In the case of vTPM devices, you must upgrade to VMware ESXi 7.0.3 or later releases.

- OVA templates: VMware version 14 or later on ESXi 6.7 ESXi 7.0, and ESXi 8.0.
- ISO file supports ESXi 6.7, ESXi 7.0, and ESXi 8.0.

You can deploy Cisco ISE on VMware cloud solutions on the following public cloud platforms:

- VMware cloud in Amazon Web Services (AWS): Host Cisco ISE on a software-defined data center provided by VMware Cloud on AWS.
- Azure VMware Solution: Azure VMware Solution runs VMware workloads natively on Microsoft Azure. You can host Cisco ISE as a VMware virtual machine.
- Google Cloud VMware Engine: Google Cloud VMware Engine runs software defined data center by VMware on the Google Cloud. You can host Cisco ISE as a VMware virtual machine on the software-defined data center provided by the VMware Engine.




---

**Note** From Cisco ISE 3.1, you can use the VMware migration feature to migrate virtual machine (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.

---

- Microsoft Hyper-V on Microsoft Windows Server 2012 R2 and later
- KVM on QEMU 2.12.0-99 and later




---

**Note** Cisco ISE cannot be installed on OpenStack.

---

- Nutanix AHV 20220304.392

You can deploy Cisco ISE natively on the following public cloud platforms:

- Amazon Web Services (AWS)
- Microsoft Azure Cloud
- Oracle Cloud Infrastructure (OCI)

For information about the virtual machine requirements, see the [Cisco Identity Services Engine Installation Guide](#) for your version of Cisco ISE.

## Validated Browsers

Cisco ISE 3.3 is supported on the following browsers:

- Mozilla Firefox versions 113, 114, 119, 123, 125, 127, and later

- Google Chrome versions 112, 114, 116, 117, 119, 122, 124, 126, and later
- Microsoft Edge version 112, 115, 117, 119, 122, 125, 126, and later
- Safari 18.0, and later



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

## Validated External Identity Sources



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

**Table 2: Validated External Identity Sources**

External Identity Source	Version
<b>Active Directory</b>	
Microsoft Windows Active Directory 2012	Windows Server 2012
Microsoft Windows Active Directory 2012 R2 <a href="#">1</a>	Windows Server 2012 R2
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 Windows Active Directory 2025	Windows Server 2025
<b>LDAP Servers</b>	
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
AD as LDAP	Windows Server 2022 with Patch Windows10.0-KB5025230-x64-V1.006.msu
<b>Token Servers</b>	
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

External Identity Source	Version
<b>Security Assertion Markup Language (SAML) Single Sign-On (SSO)</b>	
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
<b>Open Database Connectivity (ODBC) Identity Source</b>	
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
<b>Social Login (for Guest User Accounts)</b>	
Facebook	Latest

<sup>1</sup> Cisco ISE supports all the legacy features in Microsoft Windows Active Directory 2012 R2. However, the new features in Microsoft Windows Active Directory 2012 R2, such as Protected User Groups, are not supported.

## Supported Antivirus and Antimalware Products

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

## Validated OpenSSL Version

Cisco ISE 3.3 is validated with OpenSSL 1.1.1t and Cisco SSL 7.3.265.

## 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.

## Known Limitations and Workarounds

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

### 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.

## Upgrade Information




---

**Note** 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.

---

### 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.

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

### 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.

## Upgrade Procedure Prerequisites

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

For more information, see the [Cisco Identity Services Engine Upgrade Guide](#).

## Cisco ISE Integration with 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](#).




---

**Note** If you installed a hot patch on your previous Cisco ISE release, you must roll back the hot patch before installing a patch. Otherwise, the services might not be started due to an integrity check security issue.

---

## 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.

---

## 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*.

### Option to Add Identity Sync After Creating 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*.

## Resolved Caveats in Cisco ISE Release 3.3 - Cumulative Patch 3

Caveat ID Number	Description
<a href="#">CSCwi89720</a>	Microsoft Azure AD has been officially renamed as Microsoft Entra ID.
<a href="#">CSCwi67639</a>	Command show cpu usage does not display information on Cisco ISE Release 3.x.
<a href="#">CSCwi60778</a>	Endpoint loses static identity group assignment after reauthentication.
<a href="#">CSCwj43912</a>	Application remediation disappears after editing.
<a href="#">CSCwf24553</a>	Umbrella defect for providing information for terminologies used in licensing page.
<a href="#">CSCwj60692</a>	TLS is restricted to use only a few ciphers in Cisco ISE Release 3.3 but 8905, 9094, 9095 ports uses all ciphers.
<a href="#">CSCwi58699</a>	A guest flow triggers a CoA when Cisco Catalyst Centre or EA dictionary attributes are updated on Cisco ISE.
<a href="#">CSCwi62078</a>	[404] Resource Not Found error occurs when using the built-in authorization profile Block_Wireless_Access.
<a href="#">CSCwj48827</a>	Unable to add multiple tasks with quotes in launch program remediation.
<a href="#">CSCwj05508</a>	IP host <ip> <fqdn> command does not create IP-FQDN entry in Cisco ISE.
<a href="#">CSCwk00439</a>	The pxGrid direct service remains stuck in the initializing state as the lock file is not removed.
<a href="#">CSCwj35698</a>	Cisco ISE business logic issue in user dictionaries.
<a href="#">CSCwi94938</a>	The Cisco ISE Release 3.2 guest user API gives incorrect results when using a filter.

Caveat ID Number	Description
<a href="#">CSCwh33160</a>	Cisco ISE fails to send SNMPv3 disk traps to the configured SNMP server.
<a href="#">CSCwi15793</a>	Cisco ISE throws an error for iPSK custom attributes that start with special characters.
<a href="#">CSCwi59868</a>	The system extends sponsored guest accounts beyond the maximum number of days allowed.
<a href="#">CSCwi89082</a>	SAML default portal required to configure SAML in Cisco ISE is deleted from database.
<a href="#">CSCvy34255</a>	Extra popup screen appears while viewing RADIUS or TACACS key after enabling "require admin password" option.
<a href="#">CSCwi78164</a>	Cisco ISE DNS resolvability health check fails due to a duplicated entry of IP, name and FQDN on /etc/hosts.
<a href="#">CSCwi61950</a>	Cisco ISE reaches the context limit in proxy flow when it queries LDAP groups for authorization policy.
<a href="#">CSCwj14217</a>	Device network conditions GUI fails to load.
<a href="#">CSCwh67500</a>	Cisco ISE Release 3.2 could not find selected authorization profiles.
<a href="#">CSCwj97620</a>	The pxGrid direct sync is stuck in progress.
<a href="#">CSCwj12489</a>	Unable to delete network device group.
<a href="#">CSCwi57903</a>	A failed scheduled backup does not generate an alarm.
<a href="#">CSCwj21203</a>	The "Dashboard System Status" query exhausts 1000 database connections.
<a href="#">CSCwj03747</a>	Profiling does not suppress CoA although CoA is suppressed for specific logical groups.
<a href="#">CSCwh92366</a>	Insufficient virtual machine resource alarm is observed in Cisco ISE Release 3.1 Patch 8 longevity setup.
<a href="#">CSCwj06269</a>	Device administration setting changes record no report or alarm.
<a href="#">CSCwj51329</a>	MDM compliance check fails when there are multiple MAC addresses with VMware Workspace ONE as MDM.
<a href="#">CSCwj39533</a>	The RMQ forwarder causes high CPU or load average.
<a href="#">CSCwh01323</a>	Fix for using IPv6 with CoA requests.
<a href="#">CSCwj21403</a>	REST API authentication service does not enable when /etc/hosts has multiple entries.
<a href="#">CSCwj36716</a>	Cisco ISE self persistent Cross-Site Scripting (XSS) in my reports.
<a href="#">CSCwi59230</a>	Non super-admin users cannot edit or delete endpoints when Cisco ISE has more than 1000 identity groups.
<a href="#">CSCwd49321</a>	Cisco ISE integration fails with pxGrid is not enabled on Cisco ISE error message even when pxGrid is enabled in both nodes.
<a href="#">CSCwj43480</a>	Cisco ISE Release 3.3 does not invoke MFA for the user with User Principle Name (UPN).
<a href="#">CSCwh36667</a>	Cisco ISE monitoring GUI page stuck at "Welcome to Grafana".



Caveat ID Number	Description
<a href="#">CSCwi93050</a>	When using Azure SAML for admin access, RBAC causes endpoint import to fail.
<a href="#">CSCwh56565</a>	Primary PAN REST API call to MnT nodes should not be load balanced.
<a href="#">CSCwi74567</a>	Inconsistencies in the database cause corruption in the Cisco ISE portal.
<a href="#">CSCwa82035</a>	Cisco ISE support bundle must include garbage collector logs, thread dump, and heap dump.
<a href="#">CSCwj29392</a>	Cisco ISE cross-site request forgery.
<a href="#">CSCwi73981</a>	Cannot remove identity store from CLI that was added using uppercase FQDN.
<a href="#">CSCwf36985</a>	AD group retrieval fails while evaluating authorization policy.
<a href="#">CSCwi98793</a>	Profiler caches MDM attribute with wrong values.
<a href="#">CSCwj07319</a>	API ers/config/sessionsservice node returns an incorrect total.
<a href="#">CSCwi79159</a>	Cisco ISE Release 3.2 Patch 4: deleteCertFromStore fails to parse certificate.
<a href="#">CSCwi58421</a>	PSN node does not update the database with correct posture expiry time when posture lease is enabled.
<a href="#">CSCwi61491</a>	Application server crashes due to metaspace exhaustion.
<a href="#">CSCwi89689</a>	Invalid IP or hostname error.
<a href="#">CSCwi52041</a>	Changes in rank cause authorization rule to commit to the database table which triggers save call from UI.
<a href="#">CSCwh00060</a>	Cisco Identity Services Engine Code Injection Vulnerability.
<a href="#">CSCwj16540</a>	Cisco ISE Release 3.2 Patch 4 context visibility does not match live logs or sessions.
<a href="#">CSCwj06401</a>	Endpoints that have null key value pair in the attributes section interrupts the purge flow.
<a href="#">CSCwj72982</a>	No IPv4 or IPv6 selection is seen for passive ID reports for IP address column filter.
<a href="#">CSCvt75833</a>	Cisco ISE should do lookup again when the token server is FQDN.
<a href="#">CSCwh23986</a>	The pxGrid getUserGroups API request returns an empty response.
<a href="#">CSCwj32716</a>	The nsf should return index-0 SAN-URI to MDM, even when we have multiple SAN-URIs.
<a href="#">CSCvm56115</a>	Cisco ISE allows a policy to be saved when another browser tab deletes an ID Store.
<a href="#">CSCwi96581</a>	Upgrade CXF version as 3.4.2 is vulnerable.
<a href="#">CSCwj01310</a>	Intensive garbage collection is observed due to SXP component.
<a href="#">CSCwh69267</a>	After ADE-OS is restored, appserver is stuck at initializing state.
<a href="#">CSCwj07675</a>	Cisco ISE Release 3.2 sends outgoing RST packets with APIPA IP 169.254.4.x.
<a href="#">CSCwi67503</a>	Cisco ISE could not find selected authorization profile if created using API.

Caveat ID Number	Description
<a href="#">CSCwj47769</a>	Invalid request page in Cisco ISE Release 3.2 Patch 5.
<a href="#">CSCwi63725</a>	SNMPD process causes memory leak on Cisco ISE.
<a href="#">CSCwi57761</a>	In Cisco ISE, the vulnerabilities identified by the Common Vulnerability and Exposures (CVE) ID, CVE-2023-48795 affect third-party software in open SSH.
<a href="#">CSCwh25160</a>	Swap cleanup script to drop the swap area and program the cron.
<a href="#">CSCwh95587</a>	Cisco ISE Release 3.2 Patch 2 is intermittently not unmounting NFS repositories.
<a href="#">CSCwd14523</a>	The 'accountEnabled' attribute in Azure AD causes authentication issues for EAP-TLS.
<a href="#">CSCwh61339</a>	Export of more than 90,000 network devices times out.
<a href="#">CSCwj07717</a>	Cisco ISE audit reports log APIPA addresses as the source of API requests.
<a href="#">CSCwa32407</a>	Resend the user account details for all or specific guest users to the sponsor.
<a href="#">CSCwf56826</a>	Primary PAN nodes show cores related to jstack.
<a href="#">CSCwj66777</a>	Cisco ISE Release 3.3 ECDSA Explicit Curve test fails for EAP, secure syslog, and secure LDAP.
<a href="#">CSCwj60125</a>	Enhance guest user account search functionality.
<a href="#">CSCwk18638</a>	TrustSec CoA is not sent from the primary PAN when it does not have a policy role.
<a href="#">CSCwi61950</a>	Cisco ISE reaches the context limit in the proxy flow while querying LDAP groups for authorization policy.
<a href="#">CSCwi38377</a>	Unable to trigger CoA that is stuck at dispatcher queue.
<a href="#">CSCwk07324</a>	Cisco ISE main ThreadPool is stuck due to ACE 3rd party library causing contextN leak.
<a href="#">CSCwk61938</a>	Cisco ISE Evaluate OpenSSH CVE-2024-6387 "regreSSHion".
<a href="#">CSCwj44649</a>	In Cisco ISE 3.3, TACACS data is not retained and everything gets purged.

## Open Caveats in Cisco ISE Release 3.3 - Cumulative Patch 3

Caveat ID Number	Description
<a href="#">CSCwf79582</a>	AD credentials fail to integrate Cisco ISE with Cisco Catalyst Center 2.2.1.x and later.
<a href="#">CSCwk67747</a>	RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS).
<a href="#">CSCwk79546</a>	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

## New Features in Cisco ISE Release 3.3 - Cumulative Patch 2

### Configure Virtual Tunnel Interfaces (VTI) with Native IPsec

From Cisco ISE Release 3.3 Patch 2, you can configure VTIs using the native IPsec configuration. You can use native IPsec to establish security associations between Cisco ISE PSNs and NADs across an IPsec tunnel using IKEv1 and IKEv2 protocols. The 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*.

## 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*.

### Resolved Caveats in Cisco ISE Release 3.3 - Cumulative Patch 2

Caveat ID Number	Description
<a href="#">CSCwf47838</a>	Space characters in command arguments are not preserved after CSV Export of TACACS + command set.
<a href="#">CSCwi48806</a>	Authorization policy takes time to load, causing delays in Duo portal entries.
<a href="#">CSCwf24554</a>	SR-Insights identifies an Umbrella defect that displays more information on SL registration failure.
<a href="#">CSCwf93165</a>	In Cisco ISE 3.3, enabling the "always show invalid usernames" option does not work.
<a href="#">CSCwh99534</a>	Endpoint probe does not clean up SGT Exchange Protocol mappings.
<a href="#">CSCwh24823</a>	Updating internal users through ERS need to retain values of Non-Mandatory Attributes.
<a href="#">CSCwi53104</a>	Exporting the report beyond one-month period yields no data.
<a href="#">CSCwd67833</a>	ERS API takes several seconds to update single endpoint.

Caveat ID Number	Description
<a href="#">CSCwh83323</a>	In Cisco ISE 3.2: SMS is not sent in the "Reset Password" flow when using a custom SMTP API Destination Address.
<a href="#">CSCwe25050</a>	A wildcard certificate imported on PSPAN is not replicated to other nodes in deployment.
<a href="#">CSCwi69659</a>	TrustSec deploy verification - policy difference alarm while policy identical on Cisco ISE and NAD.
<a href="#">CSCwh74135</a>	Unable to integrate with Prime Infrastructure due to a wrong password error.
<a href="#">CSCwi29253</a>	The Cisco ISE AD Diagnostic Tool stops working upon upgrade, making it impossible to retrieve the list of available tests.
<a href="#">CSCvj75157</a>	Cisco ISE API   Does not recognize identity groups while creating user accounts.
<a href="#">CSCwf61673</a>	Cisco ISE CLI Read only users cannot run show CPU usage command.
<a href="#">CSCwi61491</a>	Application server crashes due to metaspace exhaustion.
<a href="#">CSCwi54722</a>	In redirect URLs that use FQDN that end with IP, IP is replaced by Cisco ISE hostname.
<a href="#">CSCwa15336</a>	In Cisco ISE PIC 3.1, the Live Session feature does not show terminated sessions.
<a href="#">CSCwi30707</a>	Cisco ISE 3.1 patch 7: Removed Device Types remain selectable in policy set.
<a href="#">CSCwi45090</a>	Cisco ISE: REST API ERS: downloadableacl: The filter field 'name' is not supported.
<a href="#">CSCwi42628</a>	MAR Cache replication fails between peer nodes for both NIC and NON-NIC bonding interfaces.
<a href="#">CSCwh81035</a>	The PAN is missing non-significant attribute updates of endpoints from PSNs.
<a href="#">CSCwi21020</a>	Cisco ISE Messaging Certificate generation does not replicate full certificate chain on secondary nodes.
<a href="#">CSCwi04514</a>	Posture Client Provisioning Resources HTTP Error when dictionary attribute contains "-".
<a href="#">CSCwi36040</a>	IP access list control in Cisco ISE 3.2 is not visible.
<a href="#">CSCwi15914</a>	Additional IPv6-SGT session binding created for IPv6 link local address from SXP ADD operation.
<a href="#">CSCwi66126</a>	Cisco ISE ERS API - Updating DACL does not modify last update timestamp.
<a href="#">CSCwh87732</a>	Vulnerabilities in antisamy 1.5.9.
<a href="#">CSCvs77939</a>	There are errors when editing AnyConnect configuration and Posture Agent profiles.
<a href="#">CSCwh21038</a>	Session info not stored in timed session cache during third party posture flow.
<a href="#">CSCwh83482</a>	Cisco ISE Database does not update the email field for Sponsor Accounts.

Caveat ID Number	Description
<a href="#">CSCwh96018</a>	Failure due to case sensitive check when new MDMs are created with the same name but different case.
<a href="#">CSCwi54325</a>	LINUX ISSUE - PRA fails if end point is within posture lease.
<a href="#">CSCwi53915</a>	Advanced Filter "Save" option does not work for Client Provisioning Resources filtering.
<a href="#">CSCwf89224</a>	Session ticket received from NAD decrypt fails when OU has & and @ characters in it.
<a href="#">CSCwh99772</a>	All network device groups are deleted after removing a child item from any group.
<a href="#">CSCwh93498</a>	Cisco ISE 3.1 endpoints purging rule is created automatically when My Devices portal is duplicated.
<a href="#">CSCwh90610</a>	Cisco ISE - Abandoned Jedis connections are not being sent back to the threadPool.
<a href="#">CSCwh41977</a>	Cisco ISE 3.2: Verify existence of Per-User dACL in the Cisco ISE configuration.
<a href="#">CSCwi40089</a>	Allow pxGrid session update publishing without IP Address.
<a href="#">CSCwi45879</a>	Unable to select hotspot portal if an existent or duplicated authorization profile is selected.
<a href="#">CSCwh84446</a>	Guest type save does not work when account expiration notification has special or newline character.
<a href="#">CSCwh71117</a>	Cisco ISE Admin Access: Enabling only "User Services" enables Admin GUI Access as well.
<a href="#">CSCwi33361</a>	Cisco ISE CLI access problems: Failed to connect to server.
<a href="#">CSCwi34117</a>	Grafana UI and Kibana should have RBAC implemented in Identity Services Engine.
<a href="#">CSCwh55667</a>	Cisco ISE Posture Failure: Internal System Error when premier license is disabled.
<a href="#">CSCwi59555</a>	Cisco ISE 3.2 patch 4: ODBC: Search for MAC address in format is ignored.
<a href="#">CSCwi18005</a>	External Radius server list does not show up after upgrading to 3.2.
<a href="#">CSCwi17694</a>	Cisco ISE: synflood-limit does not take effect if configured with more than 10000.
<a href="#">CSCwf34596</a>	User Custom Attributes stuck on rendering.
<a href="#">CSCwe92640</a>	In Cisco ISE 3.1/3.2, the validation for existing routes is missing during CLI configuration.
<a href="#">CSCwi03961</a>	Location group information is missing from policy sets.
<a href="#">CSCwf61657</a>	Gig0 always participates on TCP handshake of sponsor FQDN.
<a href="#">CSCwh77574</a>	Cisco ISE doesn't allow special characters for the password while importing the certificate.

Caveat ID Number	Description
<a href="#">CSCwi59312</a>	Cisco ISE Authorization Profile does not persist data with "Security Group" and "Reauthentication" common tasks.
<a href="#">CSCwh90691</a>	Show CLI command throws exception after configuring log level to 5.
<a href="#">CSCwi59216</a>	Sponsor Portal returns 400 Bad Request when clicking (Contact Support).
<a href="#">CSCwi45131</a>	Apache Struts Vulnerability affecting Cisco Products: December 2023.
<a href="#">CSCwh95022</a>	Sponsor portal shows wrong days of week information from [Setting date] tab when using Japanese UI.
<a href="#">CSCwi52264</a>	Cisco ISE SAML ID provider Configuration Attributes are deleted though they are referenced.
<a href="#">CSCwf31073</a>	Cisco ISE: Error 400 when fetching device admin network conditions through OpenAPI.
<a href="#">CSCwh92117</a>	Sysaux tablespace full due to AUD\$ table size growth.
<a href="#">CSCwi25755</a>	Cannot add SAML provider into Cisco ISE 3.2 or higher.
<a href="#">CSCwi23166</a>	Unable to save changes in the patch management condition.
<a href="#">CSCuz65708</a>	FireFox 45+ or Chrome 72: Incorrect line numbering for DACL.
<a href="#">CSCwi34405</a>	Unable to enforce the IdentityAccessRestricted attribute during authorization.
<a href="#">CSCwi05905</a>	Cisco ISE ERS API /ers/config/deploymentinfo/getAllInfo returns different data on multi-node deployments.
<a href="#">CSCwf80386</a>	Current value of Disable_RSA_PSS environmental value is not preserved upon patch installation.
<a href="#">CSCwi27497</a>	Cisco ISE REST Authentication Service does not run due to iptables error.
<a href="#">CSCwi57950</a>	Cisco ISE 3.2: Nexpose Rapid 7: Strict-Transport-Security malformed.
<a href="#">CSCwc85211</a>	Cisco ISE Passive ID Agent error "id to load is required for loading".
<a href="#">CSCwh93925</a>	When multiple static default routes are present Cisco ISE incorrectly routes RADIUS Traffic.
<a href="#">CSCwi28131</a>	A custom attribute used in a 'never purge' rule is still purges endpoints.
<a href="#">CSCwi59567</a>	Issues with updating the CoA retry count to "0".
<a href="#">CSCwh92185</a>	Radius Authentication reports exported from the Operational Data Purging pages are empty.
<a href="#">CSCwi73984</a>	Cisco ISE 3.1p8 Installed Patches menu does not list all the patches.
<a href="#">CSCwi78722</a>	Azure VM: Not able to register node to deployment.



Caveat ID Number	Description
<a href="#">CSCwh72754</a>	Cisco ISE Active Directory process (lwsmd) is stuck at "Updating" and consumes 90-100% CPU.
<a href="#">CSCwi32576</a>	PSN node crashes while assigning the CPMSessionID.
<a href="#">CSCwi19099</a>	Issue while inserting the data to the config folder if any of the connector is disabled.
<a href="#">CSCwj27469</a>	Cisco ISE 3.3 on Cloud (Azure, AWS, OCI) doesn't read the disk size properly; the size always defaults to 300 GB.

## Open Caveats in Cisco ISE Release 3.3 - Cumulative Patch 2

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

## 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](#).

## Resolved Caveats in Cisco ISE Release 3.3 - Cumulative Patch 1

Identifier	Headline
<a href="#">CSCwf80509</a>	Cisco ISE Passive ID sessions are always cleared after an hour.
<a href="#">CSCwh42683</a>	Read-only admin group users have full access when logging into Cisco ISE GUI through SAML authentication.
<a href="#">CSCwh64195</a>	Data corruption is causing an authentication failure with the error messages: FailureReason=11007 or FailureReason=15022.
<a href="#">CSCwf37679</a>	Sponsor permissions are disabled on sponsor portal when accessed from the primary PAN persona.
<a href="#">CSCwf78003</a>	In the pxGrid Endpoints page, the endpoint details are not displayed accurately.
<a href="#">CSCwh17386</a>	The dedicated MnT nodes in a Cisco ISE deployment do not replicate the SMTP configuration.
<a href="#">CSCwe89459</a>	Cisco ISE REST API documentation provides incorrect script while creating endpoint group.

Identifier	Headline
<a href="#">CSCwf25955</a>	A match authorization profile with SGT, VN name, VLAN fields empty causes port to crash.
<a href="#">CSCwh18487</a>	Expired guest accounts don't receive SMS when they try to reactivate account.
<a href="#">CSCwh71273</a>	Disabled essential license leads to limited Cisco ISE GUI page access and inability to regenerate root CA.
<a href="#">CSCwh52589</a>	Acs.Username is not being updated with guest username in first device connection.
<a href="#">CSCwd82539</a>	Local or global exception rules are not matched for authorization policy.
<a href="#">CSCwh06338</a>	GUI doesn't load when trying to edit Client Provisioning Portal config.
<a href="#">CSCwf68108</a>	The OpenAPIs for endpoints are not working for the existing IOT asset attributes.
<a href="#">CSCwd79277</a>	The sync status is displayed as failed when the maximum number of TrustSec objects are selected for syncing.
<a href="#">CSCwh79938</a>	The PreferredDCs registry value cannot be set during advanced tuning.
<a href="#">CSCwe07822</a>	Date of last purge has a wrong timestamp.
<a href="#">CSCwb63834</a>	MNT log processor is enabled on non-MNT admin Cisco ISE node.
<a href="#">CSCwe95624</a>	In Cisco ISE Release 3.2, the SNMP is not working following a node restart.
<a href="#">CSCvz48764</a>	Allow launch program remediation to have a set order.
<a href="#">CSCwh95022</a>	The Sponsor portal shows the wrong days of week information from the [Setting date] tab when using the Japanese Cisco ISE GUI.
<a href="#">CSCwf22794</a>	Inconsistency in VLAN ID results in error message: Not a valid ODBC dictionary.
<a href="#">CSCwh69045</a>	In Cisco ISE Release 3.1 Patch 5: Some internal users passwords are not expiring after the configured global password expiry dates.
<a href="#">CSCwe74135</a>	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.
<a href="#">CSCwd28431</a>	Removal of EPS from the Cisco ISE code.
<a href="#">CSCvq79397</a>	Cisco ISE GUI pages are not loading properly with custom admin menu workcenter permissions.
<a href="#">CSCwh51156</a>	Cisco ISE cannot load corrupted NAD profiles causing authorization failures with the following reasons: failureReasons 11007 and 15022.
<a href="#">CSCwh47299</a>	Cisco ISE Alarm and Dashboard Summary does not load.
<a href="#">CSCwh51548</a>	Cisco ISE 3.2.0.542: The hot patches are not getting installed when both the patch and hot patches are in ZTP configuration.
<a href="#">CSCwc26835</a>	RADIUS server sequence configuration gets corrupted.

Identifier	Headline
<a href="#">CSCwf44906</a>	Reconfiguring repository with credentials is required following the restoration of a configuration backup.
<a href="#">CSCwf72037</a>	Cisco ISE Release 3.1: Administrator Login Report shows 'Administrator authentication failed' every 5 minutes.
<a href="#">CSCwh36544</a>	pxGrid does not show the topic registration details.
<a href="#">CSCwf39620</a>	Agentless posture is not working in Windows if the username starts with the special character '\$'.
<a href="#">CSCwd36753</a>	The AnyConnect posture script does not run when the script condition name contains a period.
<a href="#">CSCwh17448</a>	Cisco ISE Release 3.1: Agentless posture flows fail when the domain user is configured for an endpoint login.
<a href="#">CSCwf72918</a>	In Cisco ISE Release 3.2, the order of the IP name-servers in the running configuration is fallible.
<a href="#">CSCvj75157</a>	Cisco ISE API doesn't recognize the identity groups while creating user accounts.
<a href="#">CSCwh63501</a>	Vulnerabilities in log4net 2.0.8.0.
<a href="#">CSCwh47601</a>	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.
<a href="#">CSCwh58768</a>	Unable to delete existing devices in My Device Portal following a restoration from Cisco ISE Release 2.7.
<a href="#">CSCwd57628</a>	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.
<a href="#">CSCwh46669</a>	After an admin certificate change, Cisco ISE is not restarting services if the bond interface is configured.
<a href="#">CSCwh17285</a>	Cisco ISE Release 3.2 Patch 3 and Cisco ISE Release 3.3: The initialization of portals fail if <i>IPV6 enable</i> is the only IPV6 command on the interface.
<a href="#">CSCwe10898</a>	An endpoint's MAC address is not added to the endpoint identity group when using grace access in the guest portal.
<a href="#">CSCwf07855</a>	Cisco ISE SXP bindings API call returns 2xx response when the call fails.
<a href="#">CSCwh42009</a>	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.
<a href="#">CSCwh03740</a>	CRL retrieval is failing.
<a href="#">CSCwf22527</a>	Context visibility: Endpoint custom attributes cannot be filtered with special characters.
<a href="#">CSCwf10516</a>	In Cisco ISE Release 3.2, the authorization policy search feature is not working.

Identifier	Headline
<a href="#">CSCwh05599</a>	Cisco ISE Sponsor Portal is displaying an invalid input error when special characters are used in the guest type.
<a href="#">CSCwh18899</a>	Cisco ISE Open API: /certs/system-certificate/import must support multi-node deployment.
<a href="#">CSCwf88944</a>	Guest portal FQDN is mapped with IP address of the node in the database.
<a href="#">CSCwh23367</a>	In Cisco ISE Release 3.2, the self-registered email subject line truncates everything after the equal (=) sign on the sponsor guest portal.
<a href="#">CSCwf72123</a>	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.
<a href="#">CSCwf80292</a>	Cisco ISE cannot retrieve a peer certificate during EAP-TLS authentication.
<a href="#">CSCvo60450</a>	Cisco ISE: Enhancement for the encryption to only send AES256 for MS-RPC calls.
<a href="#">CSCwf10773</a>	Removing one of multiple DNS servers using "no ip name-server <IP_of_DNS_server>" command restarts Cisco ISE services without a restart prompt.
<a href="#">CSCvw81130</a>	Cisco ISE Release 2.7: Unable to disable the scheduled Active Directory Diagnostic Tool tests.
<a href="#">CSCwh26288</a>	pxGrid Direct: Premier license is required to add a connector. To use the feature, you need the Advantage license.
<a href="#">CSCwf30570</a>	Agentless posture script does not run when the endpoint is not connected to an AC power source.
<a href="#">CSCwf24158</a>	Terms and Conditions check box disappears when Portal Builder is used for Cisco ISE Release 3.0 and later releases.
<a href="#">CSCwf94289</a>	Cisco ISE Release 3.0 Patch 6: Policy export fails to export the policies.
<a href="#">CSCwc39545</a>	DockerMetrics - Report needs to be changed.
<a href="#">CSCwa08802</a>	Cisco ISE Release 3.1 on AWS gives a false negative on the DNS check for Health Checks.
<a href="#">CSCwf09393</a>	Cisco ISE Release 3.1: Services failed to start after restoring a backup from Cisco ISE Release 2.7.
<a href="#">CSCwe15945</a>	Guest account cannot be seen by sponsors in a specific sponsor group.
<a href="#">CSCwf34391</a>	Cisco ISE EasyConnect stitching does not happen when the PassiveID syslog is received by MnT before the active authentication syslog.
<a href="#">CSCwh42442</a>	Cisco ISE Release 3.2 Patch 3: CRL Download failure.
<a href="#">CSCwf79582</a>	The certificates API - /admin/API/PKI/TrustCertificates is not exposed but breaks Cisco DNA Center integration with AD username.

Identifier	Headline
<a href="#">CSCwf14365</a>	"Configuration Missing" warning is seen when navigating to the Log Analytics page.
<a href="#">CSCwh24823</a>	Updates to the internal users using ERS APIs must retain the values of non-mandatory attributes.
<a href="#">CSCwh90691</a>	The Show CLI command throws an exception after configuring the log level to 5.
<a href="#">CSCwf66934</a>	Cisco ISE Release 3.2: GUI issues are noticed in Windows when adding a new context visibility dashboard.
<a href="#">CSCwh14249</a>	Cisco ISE 3.x: There is a spelling mistake in the API gateway settings.
<a href="#">CSCvz86688</a>	Aruba-MPSK-Passphrase needs encryption support.
<a href="#">CSCwf09364</a>	The user identity group and endpoint identity group description fields have a character limit of 1199.
<a href="#">CSCwc04447</a>	Cisco ISE Release 2.7 Patch 6 is unable to filter TACACS live logs by network device IP.
<a href="#">CSCwh30893</a>	Profiling is not processing calling station ID values with the following format: XXXXXXXXXXXXX.
<a href="#">CSCwh10401</a>	Cisco ISE Release 3.1 Patch 5: Cannot generate pxGrid client certificate leveraging the CSR option.
<a href="#">CSCwh70275</a>	While registering node with left over certificates from deregistration, the certificates that are currently in use get deleted.
<a href="#">CSCwf47038</a>	Trash all or selected option at pxGrid policy should not touch entries for internal group.
<a href="#">CSCwf07444</a>	Cisco ISE patch GUI installation is stuck on a specific Cisco ISE node in deployment.
<a href="#">CSCwh04251</a>	Cisco ISE agentless posture does not support password containing a colon.
<a href="#">CSCvu56500</a>	An export of all the network devices on Cisco ISE results in an empty file.
<a href="#">CSCwf66237</a>	Cisco ISE: Get All Endpoints request takes a longer time to execute from Cisco ISE Release 2.7.
<a href="#">CSCwf59058</a>	RBAC policy with custom permissions is not working when the administration menu is hidden.
<a href="#">CSCwd97984</a>	Meraki Sync service not running immediately after a Cisco ISE application server restart.
<a href="#">CSCwf66880</a>	Endpoint .csv file import displays "no file chosen" after selecting the file.
<a href="#">CSCwh08408</a>	Cisco ISE Release 3.3 cannot register new nodes to the deployment post upgrade due to the node exporter password not being found.
<a href="#">CSCwf26951</a>	Profiler CoA sent with the wrong session ID.

Identifier	Headline
<a href="#">CSCwh45472</a>	Operational backups from the Cisco ISE GUI to the SFTP repositories fail if the PKI key pair passphrase contains a plus (+) symbol.
<a href="#">CSCwh28528</a>	TopN device admin reports do not work when incoming TACACS exceeds 40M records per day.
<a href="#">CSCwf40265</a>	Cisco ISE Max Session Counter time limit is not working.
<a href="#">CSCwf97173</a>	Asynchronous policy engine affecting CoA for ANC quarantine of active VPN clients.
<a href="#">CSCwh48026</a>	pxgriddirect-connector.log shows a discrepancy between the actual clock time and the time it prints the logs.
<a href="#">CSCwf83193</a>	Unable to login to secondary admin node's GUI using AD credentials.
<a href="#">CSCwf96294</a>	Cisco ISE Release 3.0: A connection attempt to not allowed on the domains.
<a href="#">CSCwd34467</a>	Cisco ISE authorization rule evaluation is broken for attempts using EAP-chaining and Azure AD groups.
<a href="#">CSCwf98849</a>	A critical error seen in Client Provisioning Portal customization.
<a href="#">CSCwf61939</a>	Using an apostrophe in the First Name and/or Last name field presents an invalid name error.
<a href="#">CSCwf64662</a>	SXP can create inconsistent mapping between IP address and SGT.
<a href="#">CSCwc36589</a>	Cisco ISE Intune MDM integration may be disrupted due to end of support for MAC address-based APIs from Intune.
<a href="#">CSCwh18731</a>	Upgrade to Cisco ISE Release 3.2 with LSD disabled prior to the upgrade is causing EP profiler exception.
<a href="#">CSCwc53824</a>	Cisco ISE limits connection to AMP AMQP service to TLSv1.0.
<a href="#">CSCwe53550</a>	Cisco ISE and CVE-2023-24998.
<a href="#">CSCwf82055</a>	Cisco ISE - Unable to disable SHA1 for ports associated with Passive ID agents.
<a href="#">CSCwh53159</a>	Cisco ISE Release 3.1 Patch 7: Unable to change admin password if it contains special character '\$'.
<a href="#">CSCwf62744</a>	Add the "disable EDR internet check" tag.
<a href="#">CSCwh26698</a>	Add a mechanism to fetch user data for pxGrid connector.
<a href="#">CSCwh28098</a>	Cisco ISE Release 3.2 Patch 3: CoA disconnect is sent instead of CoA push during posture assessment with the RSD disabled.
<a href="#">CSCwb57672</a>	GCMP256 auth with SHA384withRSA4096 certificate (Android 12 requirement) failing authorization.
<a href="#">CSCwe82004</a>	TCP Socket Exhaustion.

Identifier	Headline
<a href="#">CSCwf98944</a>	Vulnerabilities in axios 0.21.1.
<a href="#">CSCwh38464</a>	Cisco ISE CLI user is unable login after about 2 months of not using the Cisco ISE CLI.
<a href="#">CSCwd21798</a>	Cisco ISE-PIC license expiration alarms.
<a href="#">CSCwf71870</a>	TACACS deployment with 0 days evaluation will not work after registering to smart licensing.
<a href="#">CSCwh46877</a>	Need CoA port-bounce while removing ANC policy with PORT_BOUNCE.
<a href="#">CSCwf62987</a>	Vulnerabilities in AntiSamy 1.5.9.
<a href="#">CSCwh32290</a>	After performing a reset configuration, there is a mismatch in the FQDN value in the GUI and CLI.
<a href="#">CSCwh60726</a>	The Cisco ISE automatic crash decoder is faulty.
<a href="#">CSCwf31477</a>	Profiler is triggering a port bounce when multiple sessions exist on a switch port.
<a href="#">CSCwh71435</a>	Enable password of the internal users is created when it has not been specified through the ERS API.
<a href="#">CSCwf55641</a>	German and Italian emails cannot be saved under Account Expiration Notification in Guest Types.
<a href="#">CSCwf28452</a>	The other conditions are reordered after saving in Client Provisioning Policy.
<a href="#">CSCwh41693</a>	ISEaaS: AWS - Support IMDS v2.
<a href="#">CSCwh05647</a>	Static IPV6 routes are removed after a reload in Cisco ISE Release 3.2.
<a href="#">CSCwh44407</a>	Cisco ISE Release 3.2 API: System certificate import does not work for Cisco ISE node in deployment.
<a href="#">CSCwf27484</a>	Unable to match Azure AD group if the user belongs to more than 99 groups.
<a href="#">CSCwe03624</a>	Smart license registration fails with "communication send error" alarms occur intermittently.
<a href="#">CSCwf81550</a>	Cisco ISE is changing the MAC address format according to the selected MAC Address Format even when it is not a MAC.
<a href="#">CSCwf54680</a>	Unable to edit or delete authorization profiles with parentheses in their names.
<a href="#">CSCwh38484</a>	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.
<a href="#">CSCwf35760</a>	ct_engine is using 100% CPU.
<a href="#">CSCwh39008</a>	Not able to schedule or edit schedule for configuration backup.
<a href="#">CSCwf60904</a>	ANC remediation is not functioning with AnyConnect VPN.



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

## Open Caveats in Cisco ISE Release 3.3 - Cumulative Patch 1

Caveat ID Number	Description
<a href="#">CSCwe92640</a>	Cisco ISE Releases 3.1 and 3.2: Missing validation for existing routes during CLI configuration.
<a href="#">CSCwf55795</a>	In Cisco ISE Release 3.2 Patch 1, the Cisco ISE GUI and CLI are inaccessible following a configuration restoration with ADE-OS.
<a href="#">CSCwh92366</a>	In 3.1 Patch 8: Observing Insufficient Virtual Machine Resource Alarm in 3.1Patch 8 Longevity setup.

## 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 Release 3.3.

Caveat ID Number	Description
<a href="#">CSCwe34204</a>	The Upgrade tab in Cisco ISE shows that the upgrade is in progress after installing a patch.
<a href="#">CSCwd07345</a>	Cisco ISE privilege escalation vulnerability.
<a href="#">CSCwe50392</a>	The <i>fetch</i> command of ROPC groups with nearly 53k groups is not working in the Cisco ISE GUI.

Caveat ID Number	Description
<a href="#">CSCwf15717</a>	In Cisco ISE Release 3.2, the System 360 feature is not available with the Device Admin license.
<a href="#">CSCwe37377</a>	The Cisco ISE CRL Retrieval Failed alarm needs to display the server on which the CRL download failed.
<a href="#">CSCwc33290</a>	Unable to delete custom endpoint attribute in Cisco ISE.
<a href="#">CSCvr79992</a>	The Session.CurrentDate attribute is not calculated correctly during authentication of endpoints in Cisco ISE.
<a href="#">CSCwd48787</a>	The Cisco ISE - SSL buffer is causing problems with PAC decryption. This is affecting the EAP-FAST flows in Cisco ISE.
<a href="#">CSCwe68336</a>	Posture assessment by condition generates the following invalid identifier: ORA-00904: "SYSTEM_NAME" in the Cisco ISE GUI.
<a href="#">CSCwd07349</a>	Cisco ISE command injection vulnerability.
<a href="#">CSCwd27865</a>	The Configuration Changed field is not working when assigning an endpoint to a group in Cisco ISE.
<a href="#">CSCwf14957</a>	The TrustSec status cannot be changed if you are using the Japanese Cisco ISE GUI.
<a href="#">CSCwe69085</a>	The Policy Service Node is not accessible in the Cisco ISE GUI when the Device Administration license is enabled.
<a href="#">CSCwc33751</a>	In Cisco ISE Release 3.1, the copy command using the TFTP protocol times out.
<a href="#">CSCwd97022</a>	In Cisco ISE Release 3.2 patch 3, the disabled Cisco ISE-PIC smart license is being used erroneously for upgrade.
<a href="#">CSCwd46505</a>	The queue link error alarms are not displayed in Cisco ISE-PIC nodes.
<a href="#">CSCwd07340</a>	Cisco ISE privilege escalation vulnerability.
<a href="#">CSCwc39320</a>	Cisco ISE nodes upgraded using the CLI do not progress beyond the "Upgrading" status in the Cisco ISE GUI.
<a href="#">CSCwd93719</a>	Cisco ISE XML external entity injection vulnerability.
<a href="#">CSCwe18359</a>	Vulnerabilities in Sudo 1.8.29 (a third-party software) have been fixed.
<a href="#">CSCwd63749</a>	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.
<a href="#">CSCwd24089</a>	Unable to launch Cisco ISE Release 3.2 in Safe Mode.
<a href="#">CSCwb92655</a>	Common Policy (CDP) is not enabled by default in Cisco ISE Releases 3.1 and 3.2.
<a href="#">CSCwb77915</a>	Use the toggle button to enable or disable RSA PSS ciphers based on policy under Allowed Protocols in the Cisco ISE GUI.

Caveat ID Number	Description
<a href="#">CSCwd30994</a>	When a default static route is configured with an interface's subnet gateway excluding Gigaset 0, the network connectivity to Cisco ISE is lost.
<a href="#">CSCwe55215</a>	Cisco ISE smart licensing now uses smart transport.
<a href="#">CSCwd35608</a>	The CoA is failing in Cisco ISE due to usage of old and stale audit session IDs.
<a href="#">CSCwc61320</a>	Users may experience some slowness on Support Bundle page because of the Download Logs page loading in the background.
<a href="#">CSCwc58608</a>	Cisco ISE Release 3.2 is caching as soon as a RADIUS request is received with EAP-FAST and EAP Chaining.
<a href="#">CSCvt62460</a>	Unable to retrieve groups from different LDAPs when nodes are using servers that are undefined.
<a href="#">CSCwd70902</a>	PRRT should be sending unfragmented messages to the monitoring node if IMS is enabled.
<a href="#">CSCwe49261</a>	Cisco ISE PassiveID agent probes the status of all domains (including domains that do not have a PassiveID configuration).
<a href="#">CSCwc95878</a>	There are intermittent issues with app activation.
<a href="#">CSCwd13201</a>	The Cisco ISE GUI crashes while loading the authorization policy on Google Chrome and Microsoft Edge browsers.
<a href="#">CSCwc57294</a>	The duplicate manager doesn't remove relevant packets when there is an exception in the reading configuration.
<a href="#">CSCwe07354</a>	The RADIUS token server configuration accepts empty host IP address for secondary server.
<a href="#">CSCwd57071</a>	The self registration portal does not support the FQDNs of the nodes for the Approve/Deny links sent to the sponsors.
<a href="#">CSCwf26973</a>	Network Device Group information missing when a Cisco ISE admin account has only read access.
<a href="#">CSCwd27506</a>	In Cisco ISE Release 3.0 patch 6, the scheduled reports created by external admins are missing.
<a href="#">CSCwc79321</a>	Unable to change the identity source from internal source to external source in the RSA/RADIUS-token server.
<a href="#">CSCwd41773</a>	In Cisco ISE Release 3.1, the application server crashes if CRL of 5 MB or more is downloaded frequently.
<a href="#">CSCwd97606</a>	Multiple requests for the same IP, VN, and VPN combinations with different session IDs is creating duplicate records in Cisco ISE.
<a href="#">CSCwe63320</a>	Cisco ISE Releases 3.2, 3.1, and 3.0 display mismatched information on the "Get All Endpoints" report.

Caveat ID Number	Description
<a href="#">CSCwe54466</a>	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.
<a href="#">CSCwc62419</a>	Cisco ISE insufficient access control vulnerability.
<a href="#">CSCwe33360</a>	The anomalous behavior detection is not working as expected in Cisco ISE.
<a href="#">CSCwe69179</a>	The latest IP access restriction configuration removes the previous configuration in Cisco ISE.
<a href="#">CSCwd90613</a>	The RADIUS server sequence page displays "no data available".
<a href="#">CSCwd30433</a>	The email notification when a guest account creation is denied is not sent to the admin.
<a href="#">CSCwc86067</a>	Cisco ISE authorization bypass vulnerability.
<a href="#">CSCwd31524</a>	Cisco ISE Release 3.2 does not support 16-character passwords for SFTP configuration.
<a href="#">CSCwd12357</a>	The SXP service gets stuck in the initial setup due to an exception on 9644.
<a href="#">CSCwd41219</a>	Cisco ISE command injection vulnerability.
<a href="#">CSCwf19811</a>	In Cisco ISE Release 3.1, the SXP Bindings report displays the "No data found" error.
<a href="#">CSCwe70402</a>	Cisco ISE 3.2 does not support portal customization scripts that include single-line JavaScript comments.
<a href="#">CSCwe15315</a>	The TrustSec PAC Information Field attribute values are lost when importing a network device CSV template file.
<a href="#">CSCwe37978</a>	Scheduled reports with large data sizes are displayed as "empty" in the Cisco ISE repository.
<a href="#">CSCwd87161</a>	In Cisco ISE Release 3.1, the certificate-based login asks for license files only if the Device Admin license is enabled.
<a href="#">CSCwe22934</a>	Cisco ISE authentication latency is observed because of devices with no MAC addresses.
<a href="#">CSCwe43002</a>	"Read-only Admin" not available for Cisco ISE admin SAML authentication.
<a href="#">CSCwe64558</a>	The Cisco ISE admin account created from network access users can't change dark mode settings in the Cisco ISE GUI.
<a href="#">CSCwd30038</a>	Cisco ISE command injection vulnerability.
<a href="#">CSCwd30039</a>	Cisco ISE command injection vulnerability.
<a href="#">CSCwd07350</a>	Cisco ISE path traversal vulnerability.
<a href="#">CSCwd28431</a>	Endpoint Protection Service has been removed from the Cisco ISE code.
<a href="#">CSCwc93253</a>	The Cisco ISE network device captcha is prompted only when the filter matches a single network device.

Caveat ID Number	Description
<a href="#">CSCwd51812</a>	Certificate authentication permissions in the Cisco ISE GUI have been modified for Cisco ISE Release 3.1 patch 4.
<a href="#">CSCwc64346</a>	The Cisco ISE ERS SDK documentation for network device bulk requests is incorrect.
<a href="#">CSCwd31137</a>	Scheduled RADIUS authentication reports in Cisco ISE fail while exporting them to the SFTP repository.
<a href="#">CSCwc48509</a>	Windows server 2022 is working as the target domain controller and should be monitored.
<a href="#">CSCwc47015</a>	The resolution for CSCvz85074 breaks AD group retrieval in Cisco ISE.
<a href="#">CSCwe52296</a>	The Cisco ISE MNT authentication status API query should be optimized.
<a href="#">CSCvg66764</a>	The Cisco ISE-PIC agent provides session stitching support.
<a href="#">CSCwf33128</a>	The RADIUS used space in Cisco ISE reports incorrect usage. This is because it also takes TACACS tables into account for the final report.
<a href="#">CSCwf02093</a>	In Cisco ISE Release 3.2, hyper-V installations have DHCP enabled.
<a href="#">CSCwb83304</a>	Cisco ISE upgrade is failing because of custom security groups.
<a href="#">CSCwc47799</a>	Cisco ISE does not display an error message when importing a certificate and private key that contains "%" in the password.
<a href="#">CSCwd32591</a>	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.
<a href="#">CSCwd42311</a>	Unable to download REST-ID stores from Download Logs on the Cisco ISE GUI.
<a href="#">CSCwd48000</a>	Vulnerabilities in TomCat 9.0.14.
<a href="#">CSCwc31482</a>	The NetworkSetupAssistance.exe digital signature certificate is expired in the BYOD flow when using Sierra Pacific Windows (SPW windows in Microsoft Windows).
<a href="#">CSCwd92324</a>	Cisco ISE Release 3.2 ROPC basic serviceability improvements.
<a href="#">CSCwe12098</a>	In Cisco ISE Release 3.2, the ports for Guest Portal configuration do not open on Cisco ISE nodes that are installed on AWS.
<a href="#">CSCwf21585</a>	Using potentially insecure methods - HTTP PUT method accepted.
<a href="#">CSCwe49422</a>	From Cisco ISE Release 3.2, text passwords must be entered in the identity-store command.
<a href="#">CSCwe96633</a>	The support bundle does not contain terrors.log and times.log.
<a href="#">CSCwd19529</a>	Cisco ISE stored cross-site scripting vulnerability.
<a href="#">CSCwf22799</a>	The deferred update condition will not work if the compliance module is not compatible with Cisco Secure client.

Caveat ID Number	Description
<a href="#">CSCwc91917</a>	Users cannot add the quotation character in a TACACS authorization profile.
<a href="#">CSCwc85920</a>	Cisco ISE TrustSec Logging: The SGT create event is not logged to ise-psc.log file.
<a href="#">CSCwd97353</a>	Automatic backup stops working after 3 to 5 days.
<a href="#">CSCwd71574</a>	High CPU utilization due to agentless posture configured in Cisco ISE.
<a href="#">CSCwe27146</a>	Unable to parse CLI Username with '-' (hyphen/dash) in Cisco ISE Release 3.2 Patch 1.
<a href="#">CSCwc69492</a>	Metaspace exhaustion causes crashes on the Cisco ISE node in Cisco ISE Release 3.1.
<a href="#">CSCwe97989</a>	Cisco ISE Release 3.2 crashing with VN in authorization profile.
<a href="#">CSCwd24304</a>	Cisco ISE Release 3.2 ERS POST /ers/config/networkdevicegroup fails has the broken attribute othername/type/ndgtype.
<a href="#">CSCvz68091</a>	Configuration changes to guest types are not updated in the audit reports.
<a href="#">CSCwe70889</a>	Full upgrade from Cisco ISE Release 3.0 to Cisco ISE Release 3.1 failed due to DB service timeout.
<a href="#">CSCwd92835</a>	Network Device Profile shows HTML code as name.
<a href="#">CSCwe50710</a>	In Cisco ISE Release 3.2, an error is displayed when entering the DNS domain in the Cisco ISE deploy instance on cloud.
<a href="#">CSCwe49167</a>	In Cisco ISE Release 3.2, the SAML sign authentication request setting is getting unchecked upon saving the setting.
<a href="#">CSCwf33881</a>	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.
<a href="#">CSCwc44580</a>	Cisco ISE Release 3.1 creates cni-podman0 interface with IP 10.88.0.1 and IP route for 10.88.0.0/16.
<a href="#">CSCwe14808</a>	Cisco ISE fails to translate AD attribute of msRASSavedFramedIPAddress.
<a href="#">CSCwe57764</a>	The MDM connection to Microsoft SCCM fails after Windows DCOM Server Hardening for CVE-2021-26414.
<a href="#">CSCwf17490</a>	Post service licensing update, the Cisco ISE Licensing page shows Evaluation compliance status for consumed licenses.
<a href="#">CSCwd78306</a>	The ROPC authentication functionality is broken in Cisco ISE Release 3.2.
<a href="#">CSCwf13630</a>	The monitoring log processor service stops every night.
<a href="#">CSCwd38766</a>	Deleting SNMPv3 username with "-" or "_" character doesn't delete the hexadecimal username from Cisco ISE.
<a href="#">CSCvy69943</a>	Allow Guest Portal HTTP requests containing content-headers with {} characters.

Caveat ID Number	Description
<a href="#">CSCwe78540</a>	IoTAsset information is missing when using Get All Endpoints.
<a href="#">CSCwd07351</a>	Cisco ISE command injection vulnerability.
<a href="#">CSCwd05697</a>	The guest locations do not load in the Cisco ISE Guest Portal.
<a href="#">CSCwd03009</a>	RMQForwarder thread to control platform properties in the hardware appliance in Cisco ISE Release 2.7 patch 7.
<a href="#">CSCwc74531</a>	The Cisco ISE hourly cleanup should clean the cached buffers instead of the 95% memory usage.
<a href="#">CSCwd41018</a>	Cisco ISE command injection vulnerability.
<a href="#">CSCwd16837</a>	Cisco ISE OpenAPI HTTP repo patch install fails when direct listing is disabled.
<a href="#">CSCwa62202</a>	Cisco ISE with two interfaces configured for portal access is broken.
<a href="#">CSCwe24932</a>	Agentless posture fails when using multiple domain users in the endpoint login configuration.
<a href="#">CSCwc48311</a>	Cisco ISE vPSN with IMS performance degrades by 30-40% compared to UDP syslog.
<a href="#">CSCwa55233</a>	Queue link errors "Unknown CA" when utilizing third-party signed certificate for IMS.
<a href="#">CSCwf42496</a>	Attempt to delete "Is IPSEC Device" NDG causes all subsequent RADIUS/TACACS+ authentications to fail.
<a href="#">CSCwd41651</a>	The vertical scroll bar is missing in RBAC Data and Menu Permissions window in Cisco ISE Release 3.1.
<a href="#">CSCwe86793</a>	Cisco ISE filter of REST ID Store Groups displays "Error processing this request."
<a href="#">CSCwe40577</a>	Failed to handle API resource request: Failed to convert condition.
<a href="#">CSCwd16657</a>	Cisco ISE arbitrary file download vulnerability.
<a href="#">CSCwfl0004</a>	ISE IP SGT static mapping is not sent to SXP Domain upon moving it to another mapping group.
<a href="#">CSCwc75572</a>	Primary administration node application server remains stuck at the initializing stage.
<a href="#">CSCvv90394</a>	Cisco ISE Release 2.6 patch 7 is unable to match "identityaccessrestricted equals true" in the authorization policy.
<a href="#">CSCwe11676</a>	Data is lost when accessing Total Compromised Endpoints in the Cisco ISE dashboard Threat for TC-NAC.
<a href="#">CSCwe13780</a>	Cisco ISE is unable to join node to AD by REST API.
<a href="#">CSCwd45843</a>	Authentication step latency for policy evaluation due to garbage collection activity in Cisco ISE.
<a href="#">CSCwd78028</a>	Cisco ISE - Apache TomCat vulnerability CVE-2022-25762.

Caveat ID Number	Description
<a href="#">CSCwc74206</a>	Cisco ISE 3.0 is not saving SCCM MDM server objects with new password but works when a new instance is in use.
<a href="#">CSCwe07406</a>	Error loading page error is the output when creating a guest account in the Self-Registered Guest Portal in Cisco ISE.
<a href="#">CSCwe38610</a>	Make MDM API V3 certificate string case insensitive.
<a href="#">CSCwc44614</a>	Using "Export Selected" under Network Devices leads to the login screen with more selections.
<a href="#">CSCwe24589</a>	Cisco ISE Release 3.2 URT fails with "Failed (Import into cloned database failed)" on Cisco ISE Release 3.1.
<a href="#">CSCwe92624</a>	Cisco ISE Africa or Cairo timezone DST.
<a href="#">CSCwd26845</a>	APIC integration in Cisco ISE Release 3.2 is missing fvIP subscription.
<a href="#">CSCwc70197</a>	Cisco ISE Certificate API fails to return Trusted Certificate with hash character in the Friendly Name field.
<a href="#">CSCwe12618</a>	APIC integration in Cisco ISE Release 3.2 fails to get EPs null (com.cisco.cpm.apic.ConfImporter:521).
<a href="#">CSCwc98828</a>	Cisco ISE interface feature insufficient access control vulnerability.
<a href="#">CSCwc98824</a>	Posture Requirements only show the default entry in Cisco ISE.
<a href="#">CSCwe41824</a>	Cisco ISE Release 3.2 is missing secondary policy administration node key for PKI-based SFTP.
<a href="#">CSCvo61351</a>	Cisco ISE Live Session gets stuck at "Authenticated" state.
<a href="#">CSCwc88848</a>	Cisco ISE Release 3.1 Patch 1 does not create the Rest ID or ROPC folder logs.
<a href="#">CSCvy69539</a>	CIAM: openjdk - multiple versions.
<a href="#">CSCwc57240</a>	Cisco ISE GUI is not validating the default value while adding custom attributes.
<a href="#">CSCvy88380</a>	Unable to select ISE Messaging usage (appears grayed out) for an existing certificate in the Cisco ISE GUI.
<a href="#">CSCwf05309</a>	Cisco ISE SAML certificate is not replicating to other nodes.
<a href="#">CSCwe94012</a>	Evaluate Configuration Validator gets stuck when using a password with special characters in Cisco ISE.
<a href="#">CSCwa52678</a>	Cisco ISE GUI TCP DUMP gets stuck in the "Stop_In_Progress" state.
<a href="#">CSCwc62716</a>	IndexRebuild.sql script ran over the monitoring node in Cisco ISE.
<a href="#">CSCwd63661</a>	Entering the incorrect password in the Cisco ISE GUI shows the end user agreement in Cisco ISE Release 3.1 patch 1.



Caveat ID Number	Description
<a href="#">CSCwc65802</a>	Save button for SAML configuration is grayed out in the Cisco ISE GUI.
<a href="#">CSCwe17953</a>	Cisco ISE path traversal vulnerability.
<a href="#">CSCwe17338</a>	Hostnames on Cisco ISE should not exceed 19 characters when deployed via AWS.
<a href="#">CSCwc65711</a>	MAC - CSC 5.0554 web deployment packages failed to upload.
<a href="#">CSCwc62415</a>	Cisco ISE unauthorized file access vulnerability.
<a href="#">CSCwe43468</a>	Static IP-SGT mapping with VN reference causes Cisco DNA Center Group-Based Policy sync to fail.
<a href="#">CSCwd71496</a>	Cisco ISE is not deleting all the sessions from the SXP mapping table.
<a href="#">CSCvv10712</a>	The transaction table should be truncated after a 2 million record count.
<a href="#">CSCwc62413</a>	Cisco ISE cross-site scripting vulnerability.
<a href="#">CSCwc13859</a>	Unable to create a scheduled backup with the admin user from "System Admin" AdminGroup in Cisco ISE.
<a href="#">CSCwf26226</a>	CPU spike due to memory leak with EP purge call.
<a href="#">CSCwf40128</a>	Accept client certificate without KU purpose validation per CiscoSSL rules.
<a href="#">CSCwe20314</a>	PIC license consumption in Cisco ISE-PIC Release 3.1.
<a href="#">CSCwe00424</a>	Cisco ISE- SQLException sent to the Collection Failure Alarm caused by NAS-Port-ID length.
<a href="#">CSCwe98833</a>	Cisco ISE cross-site scripting vulnerability.
<a href="#">CSCwe98831</a>	Cisco ISE stored cross-site scripting vulnerability.
<a href="#">CSCwe86494</a>	Cisco ISE displaying Tomcat stacktrace when using a specific URL.
<a href="#">CSCwd97582</a>	Cisco ISE Release 3.1 patch 5 verifies CA certificate EKU causing the "unsupported certificate" error.
<a href="#">CSCwe37041</a>	Internal CA certificate chain becomes invalid if the original primary administration node is removed.
<a href="#">CSCwe52461</a>	Unable to enable the firewall condition in Cisco ISE Release 3.1.
<a href="#">CSCwa82521</a>	There are issues in the Trusted Certificates menu in Cisco ISE Release 3.1.
<a href="#">CSCwd41098</a>	Getting pxGrid error logs in ise-psc.log after disabling pxGrid.
<a href="#">CSCwd24286</a>	Cisco ISE is not sending the hostname attribute to Cisco DNA Center.
<a href="#">CSCwd74898</a>	"Posture Configuration detection" alarms should be at the "INFO" level and must be reworded.

Caveat ID Number	Description
<a href="#">CSCwc36788</a>	In Cisco ISE Release 3.2, users are not able to delete the rules that were added during IP access rule addition.
<a href="#">CSCwc81729</a>	"All devices were successfully deleted" error after trying to delete one particular network access device by filtering.
<a href="#">CSCwd74560</a>	PUT operation failing with payload via Cisco DNA Center to Cisco ISE (ERS).
<a href="#">CSCwc42712</a>	Cisco ISE RADIUS and PassiveID session merging.
<a href="#">CSCwd15888</a>	Not able to access Time Settings Configuration Export on Cisco ISE ERS API.
<a href="#">CSCwc15013</a>	Add serviceability & fix "Could not get a resource since the pool is exhausted" Error in Cisco ISE Release 3.0.
<a href="#">CSCwf26482</a>	REST AUTH services not running after upgrading from Cisco ISE Release 3.1 to Cisco ISE Release 3.2.
<a href="#">CSCwe37018</a>	Cisco ISE integration with Cisco DNA Center fails if there are invalid certificates in the Cisco ISE trusted store.
<a href="#">CSCwd05040</a>	Unable to import certificates on Secondary node post registration to the deployment.
<a href="#">CSCwd31405</a>	Latency is observed during query of Session.PostureStatus.
<a href="#">CSCwc36242</a>	TACACS Command Accounting report export is not working.
<a href="#">CSCwe15576</a>	Not able to configure KRON job.
<a href="#">CSCwb18744</a>	SG and contracts with multiple backslash characters in a row in the description cannot sync to Cisco ISE.
<a href="#">CSCwe70975</a>	In Cisco ISE, the SMS Javascript customization is not working for SMS email gateway.
<a href="#">CSCwc85867</a>	Cisco ISE Change Configuration Audit Report does not clearly indicate the SGT creation and deletion events.
<a href="#">CSCwc66841</a>	CIAM: openjdk - multiple versions.
<a href="#">CSCwd51409</a>	Cisco ISE cannot retrieve repositories and scan policies of Tenable Security Center.
<a href="#">CSCwd79921</a>	Cisco ISE arbitrary file download vulnerability.
<a href="#">CSCwd13555</a>	Cisco ISE abruptly stops consuming passive-id session from a third-party syslog server.
<a href="#">CSCwe13110</a>	Cisco ISE Release 3.1 configuration backup is executed on the primary monitoring node.
<a href="#">CSCwd70658</a>	Unable to add Network Access Device due to the error: "There is an overlapping IP Address in your device".
<a href="#">CSCwd63717</a>	PKI-enabled SFTP Repositories not working in Cisco ISE Release 3.2.
<a href="#">CSCwe45245</a>	Smart license registration is not working.

Caveat ID Number	Description
<a href="#">CSCwe99961</a>	Sponsored Portal in Germany - Calendar shows Thursday (Donnerstag) as Di not Do.
<a href="#">CSCwf23981</a>	Cisco ISE Authorization Profile displays wrong Security Group or VN value.
<a href="#">CSCwd73282</a>	In Cisco ISE Release 3.1 Patch 3, the Sponsor Portal - Session Cookie SameSite value set to none.
<a href="#">CSCwc80243</a>	Cisco ISE TCP DUMP stuck at the error "COPY_REPO_FAILED" state when no repository is selected.
<a href="#">CSCwe54318</a>	SXP service gets stuck at initializing due to H2 DB delay in querying bindings.
<a href="#">CSCwc23593</a>	LSD is causing high CPU usage.
<a href="#">CSCwf09674</a>	Registered Endpoint Report shows unregistered guest devices.
<a href="#">CSCwc93451</a>	Profiler should ignore non-positive RADIUS syslog messages while forwarding the messages from the default RADIUS probe.
<a href="#">CSCwc85546</a>	In Cisco ISE Release 3.1, the error "Illegal hex characters in escape (%) pattern ? For input string: ^F" is displayed.
<a href="#">CSCwf40861</a>	The Cisco ISE GUI shows HTML hexadecimal code for the characters in the command set.
<a href="#">CSCwf36285</a>	The row of "Manage SXP Domain filters" only displays maximum 25.
<a href="#">CSCwe53550</a>	Cisco ISE and CVE-2023-24998.
<a href="#">CSCwe30235</a>	Vulnerabilities in jszip 3.0.0.
<a href="#">CSCwf44942</a>	Cisco ISE TACACS primary service node crashed during maximum user session authentication flow.
<a href="#">CSCwc80844</a>	Cisco ISE VMSA-2022-0024 - VMware Tools update addresses a local privilege escalation vulnerability.
<a href="#">CSCwe84210</a>	Authorization policy evaluation failing due to NullPointerException in LicenseConsumptionUtil.java.
<a href="#">CSCwd10864</a>	Cisco ISE XML external entity injection vulnerability.
<a href="#">CSCwe36063</a>	No validation of PBIS registration key configuration on the advance tuning page.
<a href="#">CSCwe25138</a>	Identity user cannot be created if the user custom attribute includes \$ or ++.
<a href="#">CSCwd13425</a>	Patch install from the Cisco ISE GUI fails.
<a href="#">CSCwe69189</a>	LSD is causing high bandwidth utilization.
<a href="#">CSCwd98296</a>	Network Device Port Conditions: IP Addresses or Device Groups don't accept valid port strings.
<a href="#">CSCwc36987</a>	Cisco ISE BETA certificate is shown as stale certificate and must be cleaned up.

Caveat ID Number	Description
<a href="#">CSCwd31414</a>	The Guest portal page displays "Error Loading Page" when the reason for the visit field contains special characters.
<a href="#">CSCwd39056</a>	Cisco ISE Release 3.1 Patch 4 Passive DC configuration is not saving the username correctly.
<a href="#">CSCwd45783</a>	pxGrid session publishing stops when reintegrating FMC while P-PIC is down.
<a href="#">CSCwf21960</a>	During upgrade the deregister call fails to remove all the nodes from the database.
<a href="#">CSCwd82119</a>	EAP-TLS authentication with ECDSA certificate fails on Cisco ISE Release 3.1.
<a href="#">CSCwc53895</a>	In Cisco ISE Release 3.1 Patch 3, SAML SSO does not work if the active policy service node goes down.
<a href="#">CSCwe61215</a>	SFTP and FTP validation is failing through CLI when 16+ characters in the password is configured.
<a href="#">CSCvz08319</a>	Cisco ISE's Application Server process is restarting during Dot1X due to buffer length = 0 for eapTLS.
<a href="#">CSCwc99178</a>	Unable to add many authorization profiles with the active sessions alarm setting.
<a href="#">CSCwd10997</a>	Node syncup fails to replicate wildcard certificate with the portal role.
<a href="#">CSCwe63873</a>	Qualys adapter is unable to download the knowledge base: Stuck with the error "knowledge download in progress".
<a href="#">CSCwc65821</a>	Cisco ISE ERS API doesn't allow for use of minus character in "Network Device Group" name.
<a href="#">CSCwd12453</a>	Cisco ISE Release 3.1 portal tag has an issue with special character validation.
<a href="#">CSCwa37580</a>	Cisco ISE Release 3.0 NFS share stuck.
<a href="#">CSCwe53921</a>	Support for concatenating AD group attributes when they exceed the length of the RADIUS attribute.
<a href="#">CSCwc44622</a>	The session gets stuck indefinitely until Cisco ISE is restarted.
<a href="#">CSCwd84055</a>	Cisco ISE Release 3.1 Azure AD autodiscovery for MDM API V3 is incorrect.
<a href="#">CSCwe92177</a>	In Cisco ISE, the Mexico time zone incorrectly changes to Daylight Saving Time.
<a href="#">CSCwd68070</a>	Import of SAML metadata fails.
<a href="#">CSCwe71804</a>	In Cisco ISE Release 3.1, certain key attributes in the SessionCache are missing when a third-party network device profile is in use.
<a href="#">CSCwc76720</a>	Cisco ISE Release 3.1 displays an error when using the SNMPv3 privacy password.
<a href="#">CSCvx15522</a>	The command to enable DNSCache in FQDN syslog popup needs correction.
<a href="#">CSCwc99664</a>	Support for macOS 12.6.

Caveat ID Number	Description
<a href="#">CSCwe71729</a>	In Cisco ISE Release 3.2, the Data Connect password expiry alarm is consistently visible even when the Data Connect feature is disabled.
<a href="#">CSCwd57978</a>	All network access devices are deleted while filtering based on NDG location and IP address.
<a href="#">CSCwe39781</a>	Cisco ISE does not remove SXP mapping when the SGT changes after CoA.
<a href="#">CSCwc64480</a>	Cisco ISE fails to establish a secure connection when new certificates are imported for the guest portal.
<a href="#">CSCwd38137</a>	Cisco ISE XML external entity injection vulnerability.
<a href="#">CSCwf28229</a>	VLAN detection interval should not be more than 30 seconds.
<a href="#">CSCwc26482</a>	The Replogns table space on the primary administration node increases when there are replication issues in the deployment.
<a href="#">CSCwf19039</a>	Agentless posture failures cause the TMP folder to increase in size in Cisco ISE Release 3.1 Patch 5.
<a href="#">CSCwd57752</a>	DB Connections are increasing in longevity and the maximum DB connections are 994 in Cisco ISE Release 3.1 Patch 5.
<a href="#">CSCwe44750</a>	The reprofiling result is not updated to Oracle/VCS after a feed incremental update.
<a href="#">CSCwd54844</a>	Cisco ISE ERS API schema for network device group creation.
<a href="#">CSCwe49183</a>	Cisco ISE SAML Destination attribute is missing for signed authorization requests.
<a href="#">CSCwd39746</a>	MSAL support is needed for SCCM integration with Cisco ISE as MS is deprecating ADAL.
<a href="#">CSCwc87670</a>	In Cisco ISE Release 3.1 patch 3, users are unable to import endpoints from .csv file if SAML is used.
<a href="#">CSCwd82134</a>	Incorrect SLR out of compliance error reported in Cisco ISE.
<a href="#">CSCwe80760</a>	Unable to save the launch program remediation when the parameter contains a double quote ("").
<a href="#">CSCwd64649</a>	Cisco DNA Center integration issue due to more internal CA certificates.
<a href="#">CSCwd69072</a>	Session directory write failed alarm with Cisco NAD using "user defined" NAD profile.
<a href="#">CSCvz86446</a>	SyncRequest timeout monitor thread does not terminate the file transfer after timeout during Cisco ISE replication.
<a href="#">CSCwe55529</a>	Authentication failed due to missing certificate private key.
<a href="#">CSCwc07082</a>	"The phone number is invalid" error is displayed when trying to import users from .csv file.

Caveat ID Number	Description
<a href="#">CSCwe37826</a>	Users cannot change the condition operator from AND to OR in posture policy conditions.
<a href="#">CSCwe34566</a>	Authentication against ROPC identity store fails with RSA key generation error.
<a href="#">CSCwf22816</a>	Authorization policy failing due to wrong condition evaluation.
<a href="#">CSCwc91923</a>	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.
<a href="#">CSCvw59025</a>	Misspelled PassiveID errors seen in logs and reports.
<a href="#">CSCwc60997</a>	The SAML flow with load balancer is failing due to incorrect token handling on Cisco ISE.
<a href="#">CSCwc49580</a>	The Adaptive Network Control (ANC) CoA is sent to the NAS IP address instead of the Device IP address.
<a href="#">CSCwe87660</a>	In Cisco ISE Release 3.1, the previous version of the hot patch is still visible in the DB.
<a href="#">CSCwe49504</a>	Cisco ISE Release 3.2 does not support passwords with more than 16 characters for the identity-store configuration command.
<a href="#">CSCwb72948</a>	Unable to access the system certificates page for the registered node in Cisco ISE Release 3.0 patch 4.
<a href="#">CSCwf32255</a>	No response received from SNMP server when the "snmp-server host" is configured in Cisco ISE Release 3.2 patch 2.
<a href="#">CSCwe96739</a>	TLS 1.0/1.1 is accepted in the Cisco ISE Release 3.0 admin portal.
<a href="#">CSCwe98676</a>	Vulnerable JS library issue found while executing ZAP.
<a href="#">CSCwe39262</a>	Passive ID agent sending incorrect time format events.
<a href="#">CSCwfl5130</a>	Permission for collector.log file is set to root automatically.
<a href="#">CSCwe30606</a>	Unable to download the support bundle of size greater than 1 GB from the Cisco ISE GUI.
<a href="#">CSCvv99093</a>	Cisco ISE nodes intermittently trigger the queue link alarms.
<a href="#">CSCwd61906</a>	Sysaux tablespace allocation should be done based on the profile of the node.
<a href="#">CSCwfl6165</a>	An NTP authentication key with more than 15 characters is getting the error "% ERROR: Bad hashed key".
<a href="#">CSCwc98823</a>	Cisco ISE command injection vulnerability.
<a href="#">CSCwfl9463</a>	Layering of drag and drop action in the Conditions Studio.
<a href="#">CSCwc03220</a>	Removing an IP access list from Cisco ISE destroys the distributed deployment.

Caveat ID Number	Description
<a href="#">CSCwe59587</a>	Some items are displayed as [Test] in the Japanese Cisco ISE GUI.

## Open Caveats in Cisco ISE Release 3.3

The following table lists the open caveats in Release 3.3.

Caveat ID Number	Description
<a href="#">CSCwf78050</a>	Enabling log analytics in lower models 3615/3715 may cause Cisco ISE to become unresponsive.
<a href="#">CSCwf02597</a>	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.
<a href="#">CSCwf49520</a>	Cisco ISE Release 3.3: Labelling ML-proposed rule has issues with special character and overlapping.
<a href="#">CSCwf76160</a>	MFC profiler shows "No data" for all the metrics in grafana dashboard.
<a href="#">CSCwf69829</a>	Cisco ISE Release 3.3: MFC_EPType isn't showing as Phone for iPhone in case of Wi-Fi analytics.
<a href="#">CSCwf14365</a>	"Configuration Missing" warning seen when browsing to log analytics page.
<a href="#">CSCwh36667</a>	Cisco ISE monitoring GUI page stuck at "Welcome to Grafana".
<a href="#">CSCwh08408</a>	Cisco ISE Release 3.3 cannot register new nodes to deployment post upgrade due to node exporter password not found.
<a href="#">CSCwh92366</a>	In 3.1 Patch 8: Observing Insufficient Virtual Machine Resource Alarm in 3.1Patch 8 Longevity setup

## Additional References

See [Cisco ISE End-User Resources](#) 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 NON-INFRINGEMENT 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](http://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 Cisco Systems, Inc. All rights reserved.