

Release Notes for Cisco Identity Services Engine, Release 3.3

First Published: 2023-07-05

Last Modified: 2024-05-24

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), or 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 ISE 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 the 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 ISE 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/host name/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 ISE Administration Guide, Release 3.3*.

Navigation Improvement


The Cisco ISE home page GUI has been modified for a better user experience. When you click the menu icon at the left-hand corner of the home page, 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, then 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 ISE 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 ISE 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 ISE Administration Guide, Release 3.3*.

Split Upgrade of Cisco ISE Deployment from GUI

Split upgrade is a multi step 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 ISE 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 Cisco Secure Network Server Appliance Hardware Installation Guide .
Cisco SNS-3655-K9 (medium)	
Cisco SNS-3695-K9 (large)	
Cisco SNS-3715-K9 (small)	
Cisco SNS-3755-K9 (medium)	
Cisco SNS-3795-K9 (large)	



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 higher 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 centre provided by VMware Cloud on AWS.
- Azure VMware Solution: Azure VMware Solution runs VMware workloads natively on Microsoft Azure. You can host Cisco ISE as a VMware virtual machine.
- Google Cloud VMware Engine: Google Cloud VMware Engine runs software defined data centre by VMware on the Google Cloud. You can host Cisco ISE as a VMware virtual machine on the software defined data centre provided by the VMware Engine.



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



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.

Supported Browsers

Cisco ISE 3.3 is supported on the following browsers:

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

- Google Chrome versions 112, 114, 116, 117, 119, 122, and 124
- Microsoft Edge version 112, 115, 117, 119, and 122



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
Active Directory	
Microsoft Windows Active Directory 2012	Windows Server 2012
Microsoft Windows Active Directory 2012 R2 1	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
LDAP Servers	
SunONE LDAP Directory Server	Version 5.2
OpenLDAP Directory Server	Version 2.4.23
Any LDAP v3 compliant server	Any version that is LDAP v3 compliant
AD as LDAP	Windows Server 2022 with Patch Windows10.0-KB5025230-x64-V1.006.msu
Token Servers	
RSA ACE/Server	6.x series
RSA Authentication Manager	7.x and 8.x series
Any RADIUS RFC 2865-compliant token server	Any version that is RFC 2865 compliant
Security Assertion Markup Language (SAML) Single Sign-On (SSO)	

External Identity Source	Version
Microsoft Azure MFA	Latest
Oracle Access Manager (OAM)	Version 11.1.2.2.0
Oracle Identity Federation (OIF)	Version 11.1.1.2.0
PingFederate Server	Version 6.10.0.4
PingOne Cloud	Latest
Secure Auth	8.1.1
Any SAMLv2-compliant Identity Provider	Any Identity Provider version that is SAMLv2 compliant
Open Database Connectivity (ODBC) Identity Source	
Microsoft SQL Server	Microsoft SQL Server 2012 Microsoft SQL Server 2022
Oracle	Enterprise Edition Release 12.1.0.2.0
PostgreSQL	9.0
Sybase	16.0
MySQL	6.3
Social Login (for Guest User Accounts)	
Facebook	Latest

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

See the [Cisco Identity Services Engine Administrator Guide](#) for more information.

Supported Antivirus and Antimalware Products

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

Validated OpenSSL Version

Cisco ISE 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 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 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 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 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*.

Subscribe to Session Directory All Topic Using pxGrid

From Cisco ISE Release 3.3 Cumulative Patch 2, you can subscribe to the Session Directory All topic using pxGrid. The sessionTopicAll is similar to the sessionTopic but with a 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
CSCwf47838	Space characters in command arguments are not preserved after CSV Export of TACACS + command set.
CSCwi48806	Authorization policy takes time to load, causing delays in Duo portal entries.
CSCwf24554	SR-Insights identifies an Umbrella defect that displays more information on SL registration failure.
CSCwf93165	In Cisco ISE 3.3, enabling the 'always show invalid usernames' option does not work.
CSCwh99534	Endpoint probe does not clean up SGT Exchange Protocol mappings.
CSCwh24823	Updating internal users through ERS need to retain values of Non-Mandatory Attributes.
CSCwi53104	Exporting the report beyond one-month period yields no data.
CSCwd67833	ERS API takes several seconds to update single endpoint.
CSCwh83323	In Cisco ISE 3.2: SMS is not sent in the "Reset Password" flow when using a custom "SMTP API Destination Address".

Caveat ID Number	Description
CSCwe25050	Wild card Certificate imported on PPAN is not replicated to other nodes in deployment.
CSCwi69659	TrustSec deploy verification - policy difference alarm while policy identical on Cisco ISE and NAD.
CSCwh74135	Unable to integrate with Prime Infrastructure due to a wrong password error.
CSCwi29253	The Cisco ISE AD Diagnostic Tool stops working upon upgrade, making it impossible to retrieve the list of available tests.
CSCvj75157	Cisco ISE API Does not recognize identity groups while creating user accounts.
CSCwf61673	Cisco ISE CLI Read only users cannot run show CPU usage command.
CSCwi61491	Application server crashes due to metaspace exhaustion.
CSCwi54722	In redirect URLs that use FQDN that end with IP, IP is replaced by Cisco ISE hostname.
CSCwa15336	In Cisco ISE PIC 3.1, the Live Session feature does not show terminated sessions.
CSCwi30707	Cisco ISE 3.1 patch 7 : Removed Device Types remain selectable in policy set.
CSCwi45090	Cisco ISE : REST API ERS : downloadableacl : The filter field 'name' is not supported.
CSCwi42628	MAR Cache replication fails between peer nodes for both NIC and NON-NIC bonding interfaces.
CSCwh81035	The PAN is missing non-significant attribute updates of endpoints from PSNs.
CSCwi21020	Cisco ISE Messaging Certificate generation does not replicate full certificate chain on secondary nodes.
CSCwi04514	Posture Client Provisioning Resources HTTP Error when dictionary attribute contains "-".
CSCwi36040	IP access list control in Cisco ISE 3.2 is not visible.
CSCwi15914	Additional IPv6-SGT session binding created for IPv6 link local address from SXP ADD operation.
CSCwi66126	Cisco ISE ERS API - Updating DACL does not modify last update timestamp.
CSCwh87732	Vulnerabilities in antisamy 1.5.9.
CSCvs77939	There are errors when editing AnyConnect configuration and Posture Agent profiles.
CSCwh21038	Session info not stored in timed session cache during third party posture flow.
CSCwh83482	Cisco ISE Database does not update the email field for Sponsor Accounts.
CSCwh96018	Failure due to case sensitive check when new MDMs are created with the same name but different case.
CSCwi54325	LINUX ISSUE - PRA fails if end point is within posture lease.

Caveat ID Number	Description
CSCwi53915	Advanced Filter "Save" option does not work for Client Provisioning Resources filtering.
CSCwf89224	Session ticket received from NAD decrypt fails when OU has & and @ characters in it.
CSCwh99772	All network device groups are deleted after removing a child item from any group.
CSCwh93498	Cisco ISE 3.1 endpoints purging rule is created automatically when My Devices portal is duplicated.
CSCwh90610	Cisco ISE - Abandoned Jedis connections are not being sent back to the threadPool.
CSCwh41977	Cisco ISE 3.2 : Verify existence of Per-User dACL in the Cisco ISE configuration.
CSCwi40089	Allow pxGrid session update publishing without IP Address.
CSCwi45879	Unable to select hotspot portal if an existent or duplicated authorization profile is selected.
CSCwh84446	Guest type save does not work when account expiration notification has special or newline character.
CSCwh71117	Cisco ISE Admin Access : Enabling only "User Services" enables Admin GUI Access as well.
CSCwi33361	Cisco ISE CLI access problems: Failed to connect to server.
CSCwi34117	Grafana UI and Kibana should have RBAC implemented in Identity Services Engine.
CSCwh55667	Cisco ISE Posture Failure: Internal System Error when premier license is disabled.
CSCwi59555	Cisco ISE 3.2 patch 4: ODBC : Search for MAC Address in format is ignored.
CSCwi18005	External Radius server list does not show up after upgrading to 3.2.
CSCwi17694	Cisco ISE: synflood-limit does not take effect if configured with more than 10000.
CSCwf34596	User Custom Attributes stuck on rendering.
CSCwe92640	In Cisco ISE 3.1/3.2, the validation for existing routes is missing during CLI configuration.
CSCwi03961	Location group information is missing from policy sets.
CSCwf61657	Gig0 always participate on TCP Handshake of Sponsor FQDN.
CSCwh77574	Cisco ISE is not allowing special characters for password while importing certificate.
CSCwi59312	Cisco ISE Authorization Profile does not persist data with "Security Group" and "Reauthentication" common tasks.
CSCwh90691	Show CLI commands throws exception after configuring log level to 5.

Caveat ID Number	Description
CSCwi59216	Sponsor Portal returns 400 Bad Request when clicking (Contact Support).
CSCwi45131	Apache Struts Vulnerability affecting Cisco Products: December 2023.
CSCwh95022	Sponsor portal shows wrong days of week information from [Setting date] tab when using Japanese UI.
CSCwi52264	Cisco ISE SAML ID provider Configuration Attributes are deleted though they are referenced.
CSCwf31073	Cisco ISE: Error 400 when fetching device admin network conditions through OpenAPI .
CSCwh92117	Sysaux tablespace full due to AUD\$ table size growth.
CSCwi25755	Cannot add SAML provider into Cisco ISE 3.2 or higher
CSCwi23166	Unable to save changes in the patch management condition.
CSCuz65708	FireFox 45+ or Chrome 72: Incorrect line numbering for DACL.
CSCwi34405	Unable to enforce IdentityAccessRestricted attribute during authorization.
CSCwi05905	Cisco ISE ERS API - /ers/config/deploymentinfo/getAllInfo returns different data on multi-node deployments.
CSCwf80386	Current value of Disable_RSA_PSS environmental value is not preserved upon patch installation.
CSCwi27497	Cisco ISE REST Authentication Service does not run due to iptables error.
CSCwi57950	Cisco ISE 3.2 : Nexpose Rapid 7 : Strict-Transport-Security malformed.
CSCwc85211	Cisco ISE Passive ID Agent error "id to load is required for loading".
CSCwh93925	When multiple static default routes are present Cisco ISE incorrectly routes RADIUS Traffic.
CSCwi28131	A custom attribute used in a 'never purge' rule is still purges endpoints.
CSCwi59567	Issues with updating the CoA retry count to "0" .
CSCwh92185	Radius Authentication reports exported from the Operational Data Purging pages are empty.
CSCwi73984	Cisco ISE 3.1p8 Installed Patches menu does not list all the patches.
CSCwi78722	Azure VM : Not able to register node to deployment.
CSCwh72754	Cisco ISE Active Directory process (lwsmd) is stuck at "Updating" and consumes 90-100% CPU.
CSCwi32576	PSN node crashes while assigning the CPMSessionID.

Caveat ID Number	Description
CSCwi19099	Issue while inserting the data to the config folder if any of the connector is disabled.
CSCwj27469	Cisco ISE 3.3 on Cloud (Azure, AWS, OCI) is not reading disk size properly, always defaults to 300 GB.

Open Caveats in Cisco ISE Release 3.3 - Cumulative Patch 2

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

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
CSCwf80509	Cisco ISE Passive ID sessions are always cleared after an hour.
CSCwh42683	Read-only admin group users have full access when logging into Cisco ISE GUI through SAML authentication.
CSCwh64195	Data corruption is causing an authentication failure with the error messages: FailureReason=11007 or FailureReason=15022.
CSCwf37679	Sponsor permissions are disabled on sponsor portal when accessed from the primary PAN persona.
CSCwf78003	In the pxGrid Endpoints page, the endpoint details are not displayed accurately.
CSCwh17386	The dedicated MnT nodes in a Cisco ISE deployment do not replicate the SMTP configuration.
CSCwe89459	Cisco ISE REST API documentation provides incorrect script while creating endpoint group.
CSCwf25955	A match authorization profile with SGT, VN name, VLAN fields empty causes port to crash.
CSCwh18487	Expired guest accounts don't receive SMS when they try to reactivate account.

Identifier	Headline
CSCwh71273	Disabled essential license leads to limited Cisco ISE GUI page access and inability to regenerate root CA.
CSCwh52589	Acs.Username is not being updated with guest username in first device connection.
CSCwd82539	Local or global exception rules are not matched for authorization policy.
CSCwh06338	GUI doesn't load when trying to edit Client Provisioning Portal config.
CSCwf68108	The OpenAPIs for endpoints are not working for the existing IOT asset attributes.
CSCwd79277	The sync status is displayed as failed when the maximum number of TrustSec objects are selected for syncing.
CSCwh79938	The PreferredDCs registry value cannot be set during advanced tuning.
CSCwe07822	Date of last purge has a wrong timestamp.
CSCwb63834	MNT log processor is enabled on non-MNT admin Cisco ISE node.
CSCwe95624	In Cisco ISE Release 3.2, the SNMP is not working following a node restart.
CSCvz48764	Allow launch program remediation to have a set order.
CSCwh95022	The Sponsor portal shows the wrong days of week information from the [Setting date] tab when using the Japanese Cisco ISE GUI.
CSCwf22794	Inconsistency in VLAN ID results in error message: Not a valid ODBC dictionary.
CSCwh69045	In Cisco ISE Release 3.1 Patch 5: Some internal users passwords are not expiring after the configured global password expiry dates.
CSCwe74135	In Cisco ISE Release 3.1 Patch 5: An attempt to remove the guest portal after a PAN failure leads to a ORA-02292 integrity constraint.
CSCwd28431	Removal of EPS from the Cisco ISE code.
CSCvq79397	Cisco ISE GUI pages are not loading properly with custom admin menu workcenter permissions.
CSCwh51156	Cisco ISE cannot load corrupted NAD profiles causing authorization failures with the following reasons: failureReasons 11007 and 15022.
CSCwh47299	Cisco ISE Alarm and Dashboard Summary does not load.
CSCwh51548	Cisco ISE 3.2.0.542: The hot patches are not getting installed when both the patch and hot patches are in ZTP configuration.
CSCwc26835	RADIUS server sequence configuration gets corrupted.
CSCwf44906	Reconfiguring repository with credentials is required following the restoration of a configuration backup.

Identifier	Headline
CSCwf72037	Cisco ISE Release 3.1: Administrator Login Report shows 'Administrator authentication failed' every 5 minutes.
CSCwh36544	pxGrid does not show the topic registration details.
CSCwf39620	Agentless posture is not working in Windows if the username starts with the special character '\$'.
CSCwd36753	The AnyConnect posture script does not run when the script condition name contains a period.
CSCwh17448	Cisco ISE Release 3.1: Agentless posture flows fail when the domain user is configured for an endpoint login.
CSCwf72918	In Cisco ISE Release 3.2, the order of the IP name-servers in the running configuration is fallible.
CSCvj75157	Cisco ISE API doesn't recognize the identity groups while creating user accounts.
CSCwh63501	Vulnerabilities in log4net 2.0.8.0.
CSCwh47601	Cisco ISE Release 3.2 Patches 2 and 3: Unable to create a user with authorization and privacy password that is equal to 40 characters.
CSCwh58768	Unable to delete existing devices in My Device Portal following a restoration from Cisco ISE Release 2.7.
CSCwd57628	NAD RADIUS shared secret key is incorrect when it starts with an apostrophe on Cisco ISE Release 3.1 Patches 1, 2, 3, 4, and 5.
CSCwh46669	After an admin certificate change, Cisco ISE is not restarting services if the bond interface is configured.
CSCwh17285	Cisco ISE Release 3.2 Patch 3 and Cisco ISE Release 3.3: The initialization of portals fail if <i>IPV6 enable</i> is the only IPV6 command on the interface.
CSCwe10898	An endpoint's MAC address is not added to the endpoint identity group when using grace access in the guest portal.
CSCwf07855	Cisco ISE SXP bindings API call returns 2xx response when the call fails.
CSCwh42009	Cisco ISE Release 3.2 Patch 3: The adapter.log remains in the INFO state even if the Cisco ISE GUI configuration is set to TRACE or DEBUG.
CSCwh03740	CRL retrieval is failing.
CSCwf22527	Context visibility: Endpoint custom attributes cannot be filtered with special characters.
CSCwf10516	In Cisco ISE Release 3.2, the authorization policy search feature is not working.
CSCwh05599	Cisco ISE Sponsor Portal is displaying an invalid input error when special characters are used in the guest type.

Identifier	Headline
CSCwh18899	Cisco ISE Open API: /certs/system-certificate/import must support multi-node deployment.
CSCwf88944	Guest portal FQDN is mapped with IP address of the node in the database.
CSCwh23367	In Cisco ISE Release 3.2, the self-registered email subject line truncates everything after the equal (=) sign on the sponsor guest portal.
CSCwf72123	In pxGrid direct, if the user data information is stored in a nested object within the data array, Cisco ISE is unable to process it.
CSCwf80292	Cisco ISE cannot retrieve a peer certificate during EAP-TLS authentication.
CSCvo60450	Cisco ISE: Enhancement for the encryption to only send AES256 for MS-RPC calls.
CSCwfl0773	Removing one of multiple DNS servers using "no ip name-server <IP_of_DNS_server>" command restarts Cisco ISE services without a restart prompt.
CSCvw81130	Cisco ISE Release 2.7: Unable to disable the scheduled Active Directory Diagnostic Tool tests.
CSCwh26288	pxGrid Direct: Premier license is required to add a connector. To use the feature, you need the Advantage license.
CSCwf30570	Agentless posture script does not run when the endpoint is not connected to an AC power source.
CSCwf24158	Terms and Conditions check box disappears when Portal Builder is used for Cisco ISE Release 3.0 and later releases.
CSCwf94289	Cisco ISE Release 3.0 Patch 6: Policy export fails to export the policies.
CSCwc39545	DockerMetrics - Report needs to be changed.
CSCwa08802	Cisco ISE Release 3.1 on AWS gives a false negative on the DNS check for Health Checks.
CSCwf09393	Cisco ISE Release 3.1: Services failed to start after restoring a backup from Cisco ISE Release 2.7.
CSCwe15945	Guest account cannot be seen by sponsors in a specific sponsor group.
CSCwf34391	Cisco ISE EasyConnect stitching does not happen when the PassiveID syslog is received by MnT before the active authentication syslog.
CSCwh42442	Cisco ISE Release 3.2 Patch 3: CRL Download failure.
CSCwf79582	The certificates API - /admin/API/PKI/TrustCertificates is not exposed but breaks Cisco DNA Center integration with AD username.
CSCwfl4365	"Configuration Missing" warning is seen when navigating to the Log Analytics page.

Identifier	Headline
CSCwh24823	Updates to the internal users using ERS APIs must retain the values of non-mandatory attributes.
CSCwh90691	The Show CLI command throws an exception after configuring the log level to 5.
CSCwf66934	Cisco ISE Release 3.2: GUI issues are noticed in Windows when adding a new context visibility dashboard.
CSCwh14249	Cisco ISE 3.x: There is a spelling mistake in the API gateway settings.
CSCvz86688	Aruba-MPSK-Passphrase needs encryption support.
CSCwf09364	The user identity group and endpoint identity group description fields have a character limit of 1199.
CSCwc04447	Cisco ISE Release 2.7 Patch 6 is unable to filter TACACS live logs by network device IP.
CSCwh30893	Profiling is not processing calling station ID values with the following format: XXXXXXXXXXXXX.
CSCwh10401	Cisco ISE Release 3.1 Patch 5: Cannot generate pxGrid client certificate leveraging the CSR option.
CSCwh70275	While registering node with left over certificates from deregistration, the certificates that are currently in use get deleted.
CSCwf47038	Trash all or selected option at pxGrid policy should not touch entries for internal group.
CSCwf07444	Cisco ISE patch GUI installation is stuck on a specific Cisco ISE node in deployment.
CSCwh04251	Cisco ISE agentless posture does not support password containing a colon.
CSCvu56500	An export of all the network devices on Cisco ISE results in an empty file.
CSCwf66237	Cisco ISE: Get All Endpoints request takes a longer time to execute from Cisco ISE Release 2.7.
CSCwf59058	RBAC policy with custom permissions is not working when the administration menu is hidden.
CSCwd97984	Meraki Sync service not running immediately after a Cisco ISE application server restart.
CSCwf66880	Endpoint .csv file import displays "no file chosen" after selecting the file.
CSCwh08408	Cisco ISE Release 3.3 cannot register new nodes to the deployment post upgrade due to the node exporter password not being found.
CSCwf26951	Profiler CoA sent with the wrong session ID.
CSCwh45472	Operational backups from the Cisco ISE GUI to the SFTP repositories fail if the PKI key pair passphrase contains a plus (+) symbol.

Identifier	Headline
CSCwh28528	TopN device admin reports do not work when incoming TACACS exceeds 40M records per day.
CSCwf40265	Cisco ISE Max Session Counter time limit is not working.
CSCwf97173	Asynchronous policy engine affecting CoA for ANC quarantine of active VPN clients.
CSCwh48026	pxgriddirect-connector.log shows a discrepancy between the actual clock time and the time it prints the logs.
CSCwf83193	Unable to login to secondary admin node's GUI using AD credentials.
CSCwf96294	Cisco ISE Release 3.0: A connection attempt to not allowed on the domains.
CSCwd34467	Cisco ISE authorization rule evaluation is broken for attempts using EAP-chaining and Azure AD groups.
CSCwf98849	A critical error seen in Client Provisioning Portal customization.
CSCwf61939	Using an apostrophe in the First Name and/or Last name field presents an invalid name error.
CSCwf64662	SXP can create inconsistent mapping between IP address and SGT.
CSCwc36589	Cisco ISE Intune MDM integration may be disrupted due to end of support for MAC address-based APIs from Intune.
CSCwh18731	Upgrade to Cisco ISE Release 3.2 with LSD disabled prior to the upgrade is causing EP profiler exception.
CSCwc53824	Cisco ISE limits connection to AMP AMQP service to TLSv1.0.
CSCwc53550	Cisco ISE and CVE-2023-24998.
CSCwf82055	Cisco ISE - Unable to disable SHA1 for ports associated with Passive ID agents.
CSCwh53159	Cisco ISE Release 3.1 Patch 7: Unable to change admin password if it contains special character '\$'.
CSCwf62744	Add the "disable EDR internet check" tag.
CSCwh26698	Add a mechanism to fetch user data for pxGrid connector.
CSCwh28098	Cisco ISE Release 3.2 Patch 3: CoA disconnect is sent instead of CoA push during posture assessment with the RSD disabled.
CSCwb57672	GCMP256 auth with SHA384withRSA4096 certificate (Android 12 requirement) failing authorization.
CSCwc82004	TCP Socket Exhaustion.
CSCwf98944	Vulnerabilities in axios 0.21.1.

Identifier	Headline
CSCwh38464	Cisco ISE CLI user is unable login after about 2 months of not using the Cisco ISE CLI.
CSCwd21798	Cisco ISE-PIC license expiration alarms.
CSCwf71870	TACACS deployment with 0 days evaluation will not work after registering to smart licensing.
CSCwh46877	Need CoA port-bounce while removing ANC policy with PORT_BOUNCE.
CSCwf62987	Vulnerabilities in AntiSamy 1.5.9.
CSCwh32290	After performing a reset configuration, there is a mismatch in the FQDN value in the GUI and CLI.
CSCwh60726	The Cisco ISE automatic crash decoder is faulty.
CSCwf31477	Profiler is triggering a port bounce when multiple sessions exist on a switch port.
CSCwh71435	Enable password of the internal users is created when it has not been specified through the ERS API.
CSCwf55641	German and Italian emails cannot be saved under Account Expiration Notification in Guest Types.
CSCwf28452	The other conditions are reordered after saving in Client Provisioning Policy.
CSCwh41693	ISEaaS: AWS - Support IMDS v2.
CSCwh05647	Static IPV6 routes are removed after a reload in Cisco ISE Release 3.2.
CSCwh44407	Cisco ISE Release 3.2 API: System certificate import does not work for Cisco ISE node in deployment.
CSCwf27484	Unable to match Azure AD group if the user belongs to more than 99 groups.
CSCwe03624	Smart license registration fails with "communication send error" alarms occur intermittently.
CSCwf81550	Cisco ISE is changing the MAC address format according to the selected MAC Address Format even when it is not a MAC.
CSCwf54680	Unable to edit or delete authorization profiles with parentheses in their names.
CSCwh38484	Manual deletion of the static route will cause Cisco ISE to send a packet with wrong MAC addresses in Cisco ISE Release 3.0 Patch 7.
CSCwf35760	ct_engine is using 100% CPU.
CSCwh39008	Not able to schedule or edit schedule for configuration backup.
CSCwf60904	ANC remediation is not functioning with AnyConnect VPN.

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

Open Caveats in Cisco ISE Release 3.3 - Cumulative Patch 1

Caveat ID Number	Description
CSCwe92640	Cisco ISE Releases 3.1 and 3.2: Missing validation for existing routes during CLI configuration.
CSCwf55795	In Cisco ISE Release 3.2 Patch 1, the Cisco ISE GUI and CLI are inaccessible following a configuration restoration with ADE-OS.
CSCwh92366	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
CSCwe34204	The Upgrade tab in Cisco ISE shows that the upgrade is in progress after installing a patch.
CSCwd07345	Cisco ISE privilege escalation vulnerability.
CSCwe50392	The <i>fetch</i> command of ROPC groups with nearly 53k groups is not working in the Cisco ISE GUI.

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

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

Caveat ID Number	Description
CSCwe54466	A sponsor portal print issue in Cisco ISE displays guest user settings based on From-First-Login guest account setting instead of the configured purge settings.
CSCwc62419	Cisco ISE insufficient access control vulnerability.
CSCwe33360	The anomalous behavior detection is not working as expected in Cisco ISE.
CSCwe69179	The latest IP access restriction configuration removes the previous configuration in Cisco ISE.
CSCwd90613	The RADIUS server sequence page displays "no data available".
CSCwd30433	The email notification when a guest account creation is denied is not sent to the admin.
CSCwc86067	Cisco ISE authorization bypass vulnerability.
CSCwd31524	Cisco ISE Release 3.2 does not support 16-character passwords for SFTP configuration.
CSCwd12357	The SXP service gets stuck in the initial setup due to an exception on 9644.
CSCwd41219	Cisco ISE command injection vulnerability.
CSCwfl9811	In Cisco ISE Release 3.1, the SXP Bindings report displays the "No data found" error.
CSCwe70402	Cisco ISE 3.2 does not support portal customization scripts that include single-line JavaScript comments.
CSCwe15315	The TrustSec PAC Information Field attribute values are lost when importing a network device CSV template file.
CSCwe37978	Scheduled reports with large data sizes are displayed as "empty" in the Cisco ISE repository.
CSCwd87161	In Cisco ISE Release 3.1, the certificate-based login asks for license files only if the Device Admin license is enabled.
CSCwe22934	Cisco ISE authentication latency is observed because of devices with no MAC addresses.
CSCwe43002	"Read-only Admin" not available for Cisco ISE admin SAML authentication.
CSCwe64558	The Cisco ISE admin account created from network access users can't change dark mode settings in the Cisco ISE GUI.
CSCwd30038	Cisco ISE command injection vulnerability.
CSCwd30039	Cisco ISE command injection vulnerability.
CSCwd07350	Cisco ISE path traversal vulnerability.
CSCwd28431	Endpoint Protection Service has been removed from the Cisco ISE code.
CSCwc93253	The Cisco ISE network device captcha is prompted only when the filter matches a single network device.

Caveat ID Number	Description
CSCwd51812	Certificate authentication permissions in the Cisco ISE GUI have been modified for Cisco ISE Release 3.1 patch 4.
CSCwc64346	The Cisco ISE ERS SDK documentation for network device bulk requests is incorrect.
CSCwd31137	Scheduled RADIUS authentication reports in Cisco ISE fail while exporting them to the SFTP repository.
CSCwc48509	Windows server 2022 is working as the target domain controller and should be monitored.
CSCwc47015	The resolution for CSCvz85074 breaks AD group retrieval in Cisco ISE.
CSCwc52296	The Cisco ISE MNT authentication status API query should be optimized.
CSCvg66764	The Cisco ISE-PIC agent provides session stitching support.
CSCwf33128	The RADIUS used space in Cisco ISE reports incorrect usage. This is because it also takes TACACS tables into account for the final report.
CSCwf02093	In Cisco ISE Release 3.2, hyper-V installations have DHCP enabled.
CSCwb83304	Cisco ISE upgrade is failing because of custom security groups.
CSCwc47799	Cisco ISE does not display an error message when importing a certificate and private key that contains "%" in the password.
CSCwd32591	In Cisco ISE Release 3.2, the SFTP repositories are not operational from the Cisco ISE GUI even after clicking the "generate key pairs" option.
CSCwd42311	Unable to download REST-ID stores from Download Logs on the Cisco ISE GUI.
CSCwd48000	Vulnerabilities in TomCat 9.0.14.
CSCwc31482	The NetworkSetupAssistance.exe digital signature certificate is expired in the BYOD flow when using Sierra Pacific Windows (SPW windows in Microsoft Windows).
CSCwd92324	Cisco ISE Release 3.2 ROPC basic serviceability improvements.
CSCwc12098	In Cisco ISE Release 3.2, the ports for Guest Portal configuration do not open on Cisco ISE nodes that are installed on AWS.
CSCwf21585	Using potentially insecure methods - HTTP PUT method accepted.
CSCwc49422	From Cisco ISE Release 3.2, text passwords must be entered in the identity-store command.
CSCwc96633	The support bundle does not contain terrors.log and times.log.
CSCwd19529	Cisco ISE stored cross-site scripting vulnerability.
CSCwf22799	The deferred update condition will not work if the compliance module is not compatible with Cisco Secure client.

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

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

Caveat ID Number	Description
CSCwc74206	Cisco ISE 3.0 is not saving SCCM MDM server objects with new password but works when a new instance is in use.
CSCwe07406	Error loading page error is the output when creating a guest account in the Self-Registered Guest Portal in Cisco ISE.
CSCwe38610	Make MDM API V3 certificate string case insensitive.
CSCwc44614	Using "Export Selected" under Network Devices leads to the login screen with more selections.
CSCwe24589	Cisco ISE Release 3.2 URT fails with "Failed (Import into cloned database failed)" on Cisco ISE Release 3.1.
CSCwe92624	Cisco ISE Africa or Cairo timezone DST.
CSCwd26845	APIC integration in Cisco ISE Release 3.2 is missing fvIP subscription.
CSCwc70197	Cisco ISE Certificate API fails to return Trusted Certificate with hash character in the Friendly Name field.
CSCwe12618	APIC integration in Cisco ISE Release 3.2 fails to get EPs null (com.cisco.cpm.apic.ConfImporter:521).
CSCwc98828	Cisco ISE interface feature insufficient access control vulnerability.
CSCwc98824	Posture Requirements only show the default entry in Cisco ISE.
CSCwe41824	Cisco ISE Release 3.2 is missing secondary policy administration node key for PKI-based SFTP.
CSCvo61351	Cisco ISE Live Session gets stuck at "Authenticated" state.
CSCwc88848	Cisco ISE Release 3.1 Patch 1 does not create the Rest ID or ROPC folder logs.
CSCvy69539	CIAM: openjdk - multiple versions.
CSCwc57240	Cisco ISE GUI is not validating the default value while adding custom attributes.
CSCvy88380	Unable to select ISE Messaging usage (appears grayed out) for an existing certificate in the Cisco ISE GUI.
CSCwf05309	Cisco ISE SAML certificate is not replicating to other nodes.
CSCwe94012	Evaluate Configuration Validator gets stuck when using a password with special characters in Cisco ISE.
CSCwa52678	Cisco ISE GUI TCP DUMP gets stuck in the "Stop_In_Progress" state.
CSCwc62716	IndexRebuild.sql script ran over the monitoring node in Cisco ISE.
CSCwd63661	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
CSCwc65802	Save button for SAML configuration is grayed out in the Cisco ISE GUI.
CSCwe17953	Cisco ISE path traversal vulnerability.
CSCwe17338	Hostnames on Cisco ISE should not exceed 19 characters when deployed via AWS.
CSCwc65711	MAC - CSC 5.0554 web deployment packages failed to upload.
CSCwc62415	Cisco ISE unauthorized file access vulnerability.
CSCwe43468	Static IP-SGT mapping with VN reference causes Cisco DNA Center Group-Based Policy sync to fail.
CSCwd71496	Cisco ISE is not deleting all the sessions from the SXP mapping table.
CSCvv10712	The transaction table should be truncated after a 2 million record count.
CSCwc62413	Cisco ISE cross-site scripting vulnerability.
CSCwc13859	Unable to create a scheduled backup with the admin user from "System Admin" AdminGroup in Cisco ISE.
CSCwf26226	CPU spike due to memory leak with EP purge call.
CSCwf40128	Accept client certificate without KU purpose validation per CiscoSSL rules.
CSCwc20314	PIC license consumption in Cisco ISE-PIC Release 3.1.
CSCwe00424	Cisco ISE- SQLException sent to the Collection Failure Alarm caused by NAS-Port-ID length.
CSCwc98833	Cisco ISE cross-site scripting vulnerability.
CSCwc98831	Cisco ISE stored cross-site scripting vulnerability.
CSCwe86494	Cisco ISE displaying Tomcat stacktrace when using a specific URL.
CSCwd97582	Cisco ISE Release 3.1 patch 5 verifies CA certificate ECU causing the "unsupported certificate" error.
CSCwe37041	Internal CA certificate chain becomes invalid if the original primary administration node is removed.
CSCwe52461	Unable to enable the firewall condition in Cisco ISE Release 3.1.
CSCwa82521	There are issues in the Trusted Certificates menu in Cisco ISE Release 3.1.
CSCwd41098	Getting pxGrid error logs in ise-psc.log after disabling pxGrid.
CSCwd24286	Cisco ISE is not sending the hostname attribute to Cisco DNA Center.
CSCwd74898	"Posture Configuration detection" alarms should be at the "INFO" level and must be reworded.

Caveat ID Number	Description
CSCwc36788	In Cisco ISE Release 3.2, users are not able to delete the rules that were added during IP access rule addition.
CSCwc81729	"All devices were successfully deleted" error after trying to delete one particular network access device by filtering.
CSCwd74560	PUT operation failing with payload via Cisco DNA Center to Cisco ISE (ERS).
CSCwc42712	Cisco ISE RADIUS and PassiveID session merging.
CSCwd15888	Not able to access Time Settings Configuration Export on Cisco ISE ERS API.
CSCwc15013	Add serviceability & fix "Could not get a resource since the pool is exhausted" Error in Cisco ISE Release 3.0.
CSCwf26482	REST AUTH services not running after upgrading from Cisco ISE Release 3.1 to Cisco ISE Release 3.2.
CSCwc37018	Cisco ISE integration with Cisco DNA Center fails if there are invalid certificates in the Cisco ISE trusted store.
CSCwd05040	Unable to import certificates on Secondary node post registration to the deployment.
CSCwd31405	Latency is observed during query of Session.PostureStatus.
CSCwc36242	TACACS Command Accounting report export is not working.
CSCwc15576	Not able to configure KRON job.
CSCwb18744	SG and contracts with multiple backslash characters in a row in the description cannot sync to Cisco ISE.
CSCwc70975	In Cisco ISE, the SMS Javascript customization is not working for SMS email gateway.
CSCwc85867	Cisco ISE Change Configuration Audit Report does not clearly indicate the SGT creation and deletion events.
CSCwc66841	CIAM: openjdk - multiple versions.
CSCwd51409	Cisco ISE cannot retrieve repositories and scan policies of Tenable Security Center.
CSCwd79921	Cisco ISE arbitrary file download vulnerability.
CSCwd13555	Cisco ISE abruptly stops consuming passive-id session from a third-party syslog server.
CSCwc13110	Cisco ISE Release 3.1 configuration backup is executed on the primary monitoring node.
CSCwd70658	Unable to add Network Access Device due to the error: "There is an overlapping IP Address in your device".
CSCwd63717	PKI-enabled SFTP Repositories not working in Cisco ISE Release 3.2.
CSCwc45245	Smart license registration is not working.

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

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

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

Caveat ID Number	Description
CSCwe37826	Users cannot change the condition operator from AND to OR in posture policy conditions.
CSCwe34566	Authentication against ROPC identity store fails with RSA key generation error.
CSCwf22816	Authorization policy failing due to wrong condition evaluation.
CSCwc91923	Uploading the AnyConnect agent from the Cisco ISE GUI triggered high CPU utilization on the primary administration node and took nearly 7 hours to complete.
CSCvw59025	Misspelled PassiveID errors seen in logs and reports.
CSCwc60997	The SAML flow with load balancer is failing due to incorrect token handling on Cisco ISE.
CSCwc49580	The Adaptive Network Control (ANC) CoA is sent to the NAS IP address instead of the Device IP address.
CSCwe87660	In Cisco ISE Release 3.1, the previous version of the hot patch is still visible in the DB.
CSCwe49504	Cisco ISE Release 3.2 does not support passwords with more than 16 characters for the identity-store configuration command.
CSCwb72948	Unable to access the system certificates page for the registered node in Cisco ISE Release 3.0 patch 4.
CSCwf32255	No response received from SNMP server when the "snmp-server host" is configured in Cisco ISE Release 3.2 patch 2.
CSCwe96739	TLS 1.0/1.1 is accepted in the Cisco ISE Release 3.0 admin portal.
CSCwe98676	Vulnerable JS library issue found while executing ZAP.
CSCwe39262	Passive ID agent sending incorrect time format events.
CSCwf15130	Permission for collector.log file is set to root automatically.
CSCwe30606	Unable to download the support bundle of size greater than 1 GB from the Cisco ISE GUI.
CSCvv99093	Cisco ISE nodes intermittently trigger the queue link alarms.
CSCwd61906	Sysaux tablespace allocation should be done based on the profile of the node.
CSCwf16165	An NTP authentication key with more than 15 characters is getting the error "% ERROR: Bad hashed key".
CSCwc98823	Cisco ISE command injection vulnerability.
CSCwf19463	Layering of drag and drop action in the Conditions Studio.
CSCwc03220	Removing an IP access list from Cisco ISE destroys the distributed deployment.

Caveat ID Number	Description
CSCwe59587	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
CSCwf78050	Enabling log analytics in lower models 3615/3715 may cause Cisco ISE to become unresponsive.
CSCwf02597	Cisco ISE Release 3.3: ML on Cisco ISE: Cisco ISE cluster will not be able to connect to ML cloud if clock diff is more than 5 minutes.
CSCwf49520	Cisco ISE Release 3.3: Labelling ML-proposed rule has issues with special character and overlapping.
CSCwf76160	MFC profiler shows "No data" for all the metrics in grafana dashboard.
CSCwf69829	Cisco ISE Release 3.3: MFC_EPTYPE isn't showing as Phone for iPhone in case of Wi-Fi analytics.
CSCwfl4365	"Configuration Missing" warning seen when browsing to log analytics page.
CSCwh36667	Cisco ISE monitoring GUI page stuck at "Welcome to Grafana".
CSCwh08408	Cisco ISE Release 3.3 cannot register new nodes to deployment post upgrade due to node exporter password not found.
CSCwh92366	In 3.1 Patch 8: Observing Insufficient Virtual Machine Resource Alarm in 3.1Patch 8 Longevity setup

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 NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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

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

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

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

© 2024 Cisco Systems, Inc. All rights reserved.