

Release Notes for Cisco Identity Services Engine, Release 3.4

First Published: 2024-08-05

Introduction to Cisco Identity Services Engine

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

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

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

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

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

New and Changed Features in Cisco ISE, Release 3.4

This section lists the new and changed features in Cisco ISE 3.4.

Automatic Log Bundle Generation On Upgrade

From Cisco ISE Release 3.4, a mini log bundle, which contains only debug logs specific to the upgrade, is generated automatically during the upgrade process. This log bundle is copied to the repository from where the upgrade was started and can be used to troubleshoot the upgrade in case of failure. Automatic log bundle generation is available for all three upgrade options in Cisco ISE - full upgrade, split upgrade, and upgrade using CLI.

For more information, see the chapter "[Perform the Upgrade](#)" in the [Cisco Identity Services Engine Upgrade Guide, Release 3.4](#).

Backup Log Improvements from the Cisco ISE CLI

The **backup-logs** CLI command has now been updated to include all backup log options that are available on the Cisco ISE GUI such as core-files, date-from, date-to, db-logs, debug-logs, local-logs, mnt-report-logs, policy-cache-logs, policy-conf-logs, and system-logs. If no output options are included, all backup logs are generated.

For more information on this CLI command, see "[backup-logs](#)" in the chapter "Cisco ISE CLI Commands in EXEC Mode" in the *Cisco ISE CLI Reference Guide, Release 3.4*.

Cisco ISE Resiliency Use Cases

From Cisco ISE Release 3.4, the **Excessive RADIUS Network Device Communication** and **Excessive Endpoint Communication** alarms have been added to maintain the resiliency of Cisco ISE. For more information, see "[Cisco ISE Alarms](#)" in the chapter "Troubleshoot" in the *Cisco ISE Administrator Guide, Release 3.4*.

Certificate Authority Diagnostic Tool

To diagnose certificate management related issues, use the **CA Diagnostic Tool** option (option 37) in the **application configure ise** command. This tool suggests the possible reasons and remediations for the identified issues, helps to fix the issues, and provides related logs for troubleshooting.

For more information, see "[Diagnose Certificate Management Related Issues](#)" in the "Cisco ISE CLI Commands in EXEC Mode" chapter in the *Cisco Identity Services Engine CLI Reference Guide, Release 3.4*.

Create a URL Pusher pxGrid Direct Connector Type

You can create a pxGrid Direct connector using the Cisco ISE GUI and OpenAPI (REST API). From Cisco ISE Release 3.4, you can choose between a **URL Fetcher** pxGrid Direct connector type or a **URL Pusher** pxGrid Direct connector type. You can use the **URL Pusher** pxGrid Direct connector to push JSON data into the Cisco ISE database using pxGrid Direct Push APIs. You can use the **URL Pusher** pxGrid Direct connector type to push data without a server or a CMDB. This data remains in the Cisco ISE database and can be used in the authorization policy.

For more information, see "[Create a URL Pusher Connector Type](#)" in the "Asset Visibility" chapter in the *Cisco ISE Administrator Guide, Release 3.4* and the *Cisco ISE API Reference Guide*.

pxGrid Direct Support for Arrays in Dictionary Groups for Authorization Policy

From Cisco ISE Release 3.4, you can also use pxGrid Direct Connector data with arrays as dictionary attributes to configure an authorization policy. The operators "Contains" or "Matches" (in case of REGEX) must be used while configuring the policy. The operators "Equals" and "In" will not work when there are arrays. Multiple attributes can be nested using "AND" or "OR" conditions. For more information, see "[Authorization Policies](#)" in the chapter "Segmentation" in the *Cisco ISE Administrator Guide, Release 3.4*.

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 3.4*.

Configure Virtual Tunnel Interfaces (VTI) with Native IPsec

From Cisco ISE Release 3.4, 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 3.4*.

Debug Log Settings

You can configure the maximum file size and the maximum number of files allowed for each debug log component. You can view the current disk space usage and the estimated space usage based on the values set for **Max File Size** and **File Count** in the **Debug Level Configuration** page. You can also specify the date and time after which these values must be reset to default.

For more information, see "[Configure Debug Log Settings](#)" in the chapter "Troubleshoot" in the *Cisco ISE Administration Guide, Release 3.4*.

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 3.4*.

- 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 3.4*.

Enforcing Domain Controller Selection With Priority

You can now choose to override Cisco ISE's selection of domain controllers in case of a preferred domain controller failover. To do this, choose **Administration > Identity Management > External Identity Sources > Active Directory > Advanced Tools > Advanced Tuning**. Enter the **REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\PreferredDcAndGc\Priority\Enabled** registry key in the **Name** field and **1** in the Value field. This ensures that in the case of a domain controller failover, Cisco ISE overrides the existing priority values and selects the next domain controller in the preferred list in the order of input from left to right. The value of this registry key is set to **0** by default.

When the

REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\PreferredDcAndGc\Priority\Enabled registry key is enabled, you can also choose to set the failback interval (in seconds). The failback interval value can be between 60 and 86400. The default failback interval is 180 seconds.



Note This feature works only for direct domains that the domain controllers were configured on, and not for trust relationship domains.

For more information, see "[Active Directory Advanced Tuning](#)" in the Chapter "Asset Visibility" in the *Cisco Identity Services Engine Administrator Guide, Release 3.4*.

GUI Enhancements in Cisco ISE Release 3.4

In Cisco ISE Release 3.4, the Cisco ISE GUI has the following enhancements to make the user experience more intuitive.

- **Single Click Access to Endpoint Information**

Objects in the **Context Visibility** page, such as the attribute details of endpoints in the Cisco ISE GUI, now have detailed information available to users with a single click.

All endpoint attributes now appear on a single tab for ease-of-use and better visibility.

You can click:

- the MAC address of an endpoint to view all endpoint attributes on a single page.
- the **See full detail** option on the top right corner of this page to view all endpoint details in a new browser tab, which you can also share.
- the link icon next to the MAC address of an endpoint to open a full-page view of all endpoint details.

The following pages have been updated to include these enhancements:

- **Context Visibility > Endpoints.**
- **Work Center > Guest Access > Identities > Endpoints.**
- **Work Center > BYOD > Identities > Endpoints.**
- **Work Center > Network Access > Identities > Endpoints.**


- **Work Center > Profiler > Endpoint Classification.**

- Retention of user preferences for column displays: When you change the column display of a table (adjust column width, hide or show columns, reorder columns, and so on) in the Cisco ISE GUI, your preferences are retained.

Hotpatch Details Added to Show Version Command

The **show version** CLI command now includes hotpatch details, if any, for a specific Cisco ISE release. For more information, see "[show version](#)" in the Chapter "Cisco ISE CLI Commands in EXEC Show Mode" in the *Cisco ISE CLI Reference Guide, Release 3.4*.



To view hotpatch details on the Cisco ISE GUI, click the  icon and choose **About ISE and Server**.

Localized ISE Installation

While reinstalling Cisco ISE, you can use the **Localized ISE Install** option (option 25) 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 3.4*.

New Session Directory topic available using pxGrid

You can subscribe to the Session Directory All topic using pxGrid. The sessionTopicAll is similar to the existing sessionTopic (which continues to be supported), with one key difference. The sessionTopicAll also publishes events for sessions without IP addresses. For more information, see the [pxGrid API Guide](#).

Opening TAC Support Cases in Cisco ISE

From Cisco ISE Release 3.4, 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 3.4*.

Option to Add Identity Sync After Creating Duo Connection

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

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

For more information, see "[Integrate Cisco Duo With Cisco ISE for Multifactor Authentication](#)" in the Chapter "Segmentation" in the *Cisco Identity Services Engine Administrator Guide, Release 3.4*.

PAC-less RADIUS Communication For TrustSec Integrations

From Cisco ISE Release 3.4, Cisco ISE supports PAC-less RADIUS communication for TrustSec integrations. This PAC-less enforcement replaces PAC-based RADIUS authentications wherever supported and is enforced through a shared secret ensuring secure communication between Cisco ISE and the TrustSec device. This feature does not require configuration changes in Cisco ISE. The network devices in the deployment may require a change in configuration. PAC-less RADIUS communication is only supported on network devices with IOS-XE version 17.15.1 or higher.

Per-user Dynamic Access Control List Behavior Change

While evaluating authorization profiles with per-user dynamic access control lists (DACLS), if a DACL does not exist in Cisco ISE configuration, authorization will fail, and Cisco ISE will send an Access-Reject response to that user. You can view this information in the **Live Log Details** page and the **AAA Diagnostics** report. From Cisco ISE Release 3.4 onwards, an authorization failure alarm is also displayed in the **Alarms** dashlet in the Cisco ISE dashboard.

For more information, see "[Downloadable ACLs](#)" in the "Segmentation" chapter in the *Cisco ISE Administrator Guide, Release 3.4*.

pxGrid Filtering

From Cisco ISE Release 3.4, pxGrid supports filtering of information based on the specific requirements of the clients. The pxGrid filtering feature enables clients to only receive relevant information from the publisher on a per-subscription basis. The filtering of information is achieved using the filtering API on the pxGrid server. For more information, see "[pxGrid Filtering](#)" in the Chapter "Cisco pxGrid" in *Cisco ISE Administrator Guide, Release 3.4*.

RADIUS Suppression and Reports Enhancement

From Cisco ISE Release 3.4, the RADIUS suppression and reports feature has been enhanced to facilitate easier RADIUS (**Administration > System > Settings > Protocols > RADIUS > RADIUS Settings**) configurations. For more information, see "[RADIUS Settings](#)" in the chapter "Segmentation" in the *Cisco ISE Administrator Guide, Release 3.4*.

Support for Multiple Cisco Application Centric Infrastructure Connectors

Cisco ISE enables you to create and enforce consistent access policies across multiple domains. Cisco ISE can share the SGTs and SGT bindings with Cisco Application Centric Infrastructure (Cisco ACI). Cisco ISE can also learn the endpoint groups (EPGs), endpoint security groups (ESGs), and endpoint information from Cisco ACI. You can add multiple Cisco ACI connections to Cisco ISE.

You can configure rules to manage the learned context in Cisco ISE and to optimize the context flows between Cisco ISE and Cisco ACI connectors.

Cisco ISE supports Cisco ACI Multi-Tenant, and Multi-Virtual Routing and Forwarding deployments. You can define multi-fabrics through multiple connections. This integration supports multi-pod and individual Cisco ACI fabrics.

For more information, see "[Connect Cisco Application Centric Infrastructure with Cisco ISE](#)" in the Chapter "Segmentation" in the *Cisco ISE Administration Guide, Release 3.4*.



Note Support for multiple Cisco Application Infrastructure (Cisco ACI) connectors is a controlled introduction (Beta) feature. We recommend that you thoroughly test this feature in a test environment before using it in a production environment. For best use of this Beta feature, install [this hot patch](#).

TLS 1.3 Support for Cisco ISE Workflows

Cisco ISE Release 3.4 allows 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 3.4, TEAP with 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 3.4, 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 3.4*.

Deprecated Features

End of Support for Legacy IPsec (ESR)

From Cisco ISE Release 3.4, 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 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*.

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 3.4. You must choose a different connection method as Cisco ISE Release 3.4 does not support Transport Gateway. If you upgrade to Cisco ISE Release 3.4 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.

GUI Deprecations

The following pages have been removed from the Cisco ISE GUI in Cisco ISE Release 3.4:

- Location Services (**Administration** > **Network Resources** > **Location Services**).
- NAC Managers (**Administration** > **Network Resources** > **NAC Managers**).

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 3.4 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)	

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](#).

Supported Virtual Environments

Cisco ISE supports the following virtual environment platforms:

- For Cisco ISE Release 3.0 and later releases, we recommend that you update to VMware ESXi 7.0.3 or later releases. Cisco ISE Release 3.3 is the last release to support VMware ESXi 6.7.

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

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

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

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



Note From Cisco ISE 3.1, you can use the VMware migration feature to migrate virtual machine (VM) instances (running any persona) between hosts. Cisco ISE supports both hot and cold migration. Hot migration is also called live migration or vMotion. Cisco ISE need not be shut down or powered off during the hot migration. You can migrate the Cisco ISE VM without any interruption in its availability.

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



Note Cisco ISE cannot be installed on OpenStack.

- Nutanix AHV 20220304.392

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

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

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

Validated Browsers

Cisco ISE 3.4 is supported on the following browsers:

- Mozilla Firefox versions 123, 124, 125, 127, and later
- Google Chrome versions 122, 123, 124, and later
- Microsoft Edge versions 123, 124, 125, and later

- Safari 18.0



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
Microsoft Windows Active Directory 2025	Windows Server 2025
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 Protected User Groups, are not supported.

Supported Antivirus and Antimalware Products

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

Validated OpenSSL Version

Cisco ISE 3.4 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.

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.

Upgrade Information



Note Native cloud environments must use the Cisco ISE backup and restore method for upgrades. Upgrades cannot be performed on Cisco ISE nodes deployed in native cloud environments. You must deploy a new node with a newer version of Cisco ISE and restore the configuration of your older Cisco ISE deployment onto it.

Upgrading to Release 3.4

You can directly upgrade to Release 3.4 from the following Cisco ISE releases:

- 3.1
- 3.2
- 3.3

If you are on a version earlier than Cisco ISE, Release 3.1, you must first upgrade to one of the releases listed above, and then upgrade to Release 3.4.

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](#).

Upgrade Procedure Prerequisites

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

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

Cisco ISE Integration with Cisco Catalyst Center

Cisco ISE can integrate with Cisco Catalyst Center. For information about configuring Cisco ISE to work with Catalyst Center, see the [Cisco Catalyst Center documentation](#).

For information about Cisco ISE compatibility with Catalyst Center, see the [Cisco SD-Access Compatibility Matrix](#).

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

Resolved Caveats in Cisco ISE Release 3.4

The resolved caveats in Cisco ISE Release 3.4, have parity with these Cisco ISE patch releases: 3.3 Patch 3, 3.2 Patch 6, and 3.1 Patch 9.

The following table lists the resolved caveats in Release 3.4.

Caveat ID Number	Description
CSCwf80509	The aging time of Cisco ISE Passive ID is always 1 hour regardless of the configuration.
CSCwf32641	Cisco ISE Release 3.3: The automatically generated SNMPv3 engine ID is identical on all the nodes. The ID displayed is AKHGCM5MKGF.
CSCwi59868	Account extension isn't properly defined in the Sponsor-based Guest Portal.
CSCwh81035	The Cisco ISE PAN is missing updates of nonsignificant attributes for endpoints from the Cisco ISE PSN.
CSCwh89520	Cisco ISE CLI upgrade fails with the error "Internal error during command execution".
CSCwj42214	Syslogs for Cisco ISE MnT purge events are incorrectly formatted.
CSCwi59216	The Sponsor Portal displays the error "400 Bad Request" when you click the Contact Support option on the Cisco ISE GUI.
CSCwi18917	Cisco ISE SNMP polling doesn't work with privacy protocol AES 192 or AES 256.
CSCwf16588	Adding the second NTP authentication key removes all authentication keys from the Cisco ISE GUI.

Caveat ID Number	Description
CSCwh84446	If the Account Expiration notification has special characters, you can't save the Guest Type.
CSCwb63834	The MnT log processor service occasionally runs on other Cisco ISE admin nodes.
CSCwe95624	In Cisco ISE Release 3.2, SNMP doesn't work after a node restart.
CSCwi58421	When posture lease is enabled, Cisco ISE PSN doesn't update the database with the correct posture expiry time.
CSCwe74135	Guest portal removal failure and integrity constraint in Cisco ISE Release 3.1 Patch 5.
CSCwd28431	Removal of EPS from Cisco ISE code.
CSCwj60692	TLS is restricted to use only a few ciphers in Cisco ISE Release 3.3, but the ports 8905, 9094, and 9095 use all TLS ciphers.
CSCwi67503	Cisco ISE couldn't find the selected authorization profile if the profile has been created using API.
CSCwi57950	Strict transport security is incorrectly formed in Cisco ISE Release 3.2.
CSCwh95587	NFS repository stops working suddenly on a single node in a distributed deployment in Cisco ISE Release 3.2.
CSCwi57812	Listening noted on port TCP and 67 in Cisco ISE Release 3.2.
CSCwf72037	Administrator login report displays the error "Administrator authentication failed" every five minutes in Cisco ISE Release 3.1.
CSCwj48359	The pxGrid Databases Synchronization Test on Cisco ISE displays the error "Out of Sync".
CSCwh47601	Unable to create a user with auth-password and priv-password equal to 40 characters in Cisco ISE Release 3.2 Patches 2 and 3.
CSCwj04049	When using an LDAP connection to connect to AD, Cisco ISE can't translate the value of AD attribute "msRASSavedFramedIPAddress" or "msRADIUSFramedIPAddress".
CSCwc64144	The attributes TotalAuthenLatency and ClientLatency don't work for TACACS+ in Cisco ISE.
CSCwe10898	Unable to add an endpoint's MAC address to Endpoint Identity Group when using grace access in the Guest portal.
CSCwi15914	Additional IPV6-SGT session binding created for IPV6 to link local address from SXP ADD operation.
CSCwf10516	The authorization policy feature isn't working in Cisco ISE Release 3.2.
CSCwf88944	Guest portal FQDN is mapped with the IP address of the node in the database.

Caveat ID Number	Description
CSCwh83482	Cisco ISE database doesn't update the email field for Sponsor accounts.
CSCwf80292	Cisco ISE can't retrieve a peer certificate during EAP-TLS authentication.
CSCvo60450	Enhancement for encryption to only send AES256 for MS-RPC calls.
CSCwf10773	Cisco ISE restarts services directly without a prompt with the error "no ip name-server" displayed.
CSCvw81130	Unable to disable Active Directory Diagnostic Tool scheduled tests in Cisco ISE Release 2.7.
CSCwj84815	The error "No session available" is displayed in Cisco ISE Release 3.3 Patch 2.
CSCvv90394	Unable to match "identityaccessrestricted equals true" in the authorization policy in Cisco ISE Release 2.6 Patch 7.
CSCwj14217	The Device Network Conditions GUI page doesn't load.
CSCwi61700	The "iselocalstore" logs aren't getting collected in the support bundle logs obtained from the Cisco ISE CLI.
CSCwh23986	The pxGrid getUserGroups API request returns an empty response.
CSCwk25064	Enabling the SXP role on the Cisco ISE PSN causes high CPU load and utilization.
CSCwj06401	Endpoints having a null key value pair in the attributes section are interrupting the purge flow.
CSCwh61339	Cisco ISE times out when using the Export All option on the Network Devices page to export more than 90,000 network devices.
CSCwf47838	Space " " characters in the command arguments are being replaced by forward slash "/" characters after the command set is exported as a CSV file.
CSCwi60778	The endpoint is losing the static identity group assignment after reauthentication.
CSCwj91517	You need to disable the unbound-anchor while starting Cisco ISE.
CSCwi18005	The external RADIUS server list doesn't show up after upgrading to Cisco ISE Release 3.2.
CSCwh24754	An excess number of AD groups being mapped to sponsor groups is causing latency in sponsor login
CSCwh70275	During the registration of a node that was previously registered to the deployment, it's observed that all the certificates of the deployment were deleted and that all the nodes in the deployment were restarted.
CSCwi05445	Unable to delete a support bundle from the Cisco ISE GUI in Cisco ISE Release 3.1 Patch 7.

Caveat ID Number	Description
CSCwk14636	An issue with the Insufficient Virtual Machine Resources Alarm on AWS is seen in Cisco ISE Release 3.2 Patch 6.
CSCwi59555	In Cisco ISE Release 3.2 Patch 4, the search for MAC address in the format is ignored.
CSCwd49321	When Cisco ISE has pxGrid enabled on two nodes, the integration fails with the error "pxGrid not enabled on ISE".
CSCwk32677	The ise-duo.log isn't collected at the time of support bundle creation.
CSCwf26951	Profiler CoA sent with the wrong session ID.
CSCwi38644	The agent rule defaults to the default rule setting while editing an existing agent.
CSCwh38464	Cisco ISE CLI admin user is unable login after not logging in over a two-month period.
CSCwf35760	The ct_engine root is using 100% of the CPU.
CSCwi37079	Cisco ISE URT bundle upgrade fails with the error "RADIUS dictionary attribute duplicate entry exists".
CSCwi54325	The PRA fails if the endpoint is in a posture lease.
CSCwi03961	Location group information is missing from policy sets.
CSCwh71157	The mobile number format field for JavaScript code doesn't support more than 100 characters.
CSCwd36753	The AnyConnect posture script isn't attempted when the script condition name contains a period.
CSCwi29623	Scheduled backup configuration details aren't visible to Read-only user in Cisco ISE Release 3.1 Patch 7.
CSCwf36285	The row of "Manage SXP Domain filters" only displays a maximum of 25 filters.
CSCwi48806	Unable to load the authorization policy due to duplicate portal entries.
CSCwj09890	When upgrading to Cisco ISE Release 3.4, the Duo seeder is missing in the MnT table post the upgrade.
CSCwj43912	The application remediation disappears after editing.
CSCwh83323	In Cisco ISE Release 3.2, the SMS is not sent during the "Reset Password" flow when using a custom "SMTP API Destination Address".
CSCwf92635	In Cisco ISE Release 3.3, the PAN failover component is missing from the debug log configuration.
CSCwa15336	In Cisco ISE PIC Release 3.1, the live session shouldn't show the terminated sessions.
CSCwi04514	Posture client provisioning resources display an HTTP error when the dictionary attribute contains "-".

Caveat ID Number	Description
CSCwi61950	Cisco ISE is reaching the context limit in proxy flows when querying LDAP groups for authorization policies.
CSCwh60726	Cisco ISE automatic crash decoder isn't decoding functions properly.
CSCwh69267	Post ADEOS restore, the app server is stuck at the initializing phase.
CSCwh16289	Add an option to delete temporary files from "/opt/backup" if the CLI backup process fails during transfer.
CSCwj89479	When joining multiple Cisco ISE nodes to the domain controller simultaneously duplicate accounts are created.
CSCwf31477	profiler is triggering Port Bounce when there are multiple sessions exist on a switch port
CSCwh69466	In Cisco ISE Release 3.1, the detailed report doesn't show both user and machine authentication policies for EAP chaining.
CSCwk13212	In Cisco ISE Release 3.2 and later releases, the System 360 monitoring debug log level needs to be reduced.
CSCwf55641	German and Italian emails can't be saved under Account Expiration Notification in Guest Types.
CSCwi73984	In Cisco ISE Release 3.1 Patch 8, the Installed Patches menu doesn't list all the patches.
CSCwi73981	An identity store added using uppercase FQDN can't be removed from the CLI.
CSCwf03445	In Cisco ISE Release 3.1, there's an intermittent failure in displaying Live Log details and the error "No Data available for this record" is displayed.
CSCwf66781	Bulk Creating Egress Matrix Policy Via ERS Fails With an Error
CSCwf42496	An attempt to delete an "Is IPSEC Device" NDG causes all subsequent RADIUS and TACACS+ authentications to fail.
CSCwi17694	If the configured synflood-limit is beyond 10000, the limit isn't working.
CSCwh90691	Show CLI commands throw an exception after configuring log level up to five.
CSCwh74135	Unable to integrate to prime Infrastructure due to a wrong password error.
CSCwi89689	Cisco ISE displaying "Invalid IP or hostname" error.
CSCwi46648	The PRA fails if the endpoint is within posture lease.
CSCwi45131	Apache Struts Vulnerability affecting Cisco products: December 2023
CSCwh39008	Not able to schedule or edit schedule for a configuration backup.
CSCwf32255	Cisco ISE Release 3.2 Patch 2 provides no response from SNMP when the "snmp-server host" is configured.

Caveat ID Number	Description
CSCwj01310	Intensive GC observed due to the SXP component causing node longevity issues in Cisco ISE Release 3.4.
CSCwh51136	Cisco ISE drops a RADIUS request with the error message "Request from a nonwireless device was dropped".
CSCwj77067	Provide a comprehensible description for the error displays while editing internal users.
CSCwf59310	Context Visibility for pxGrid ContextIn is missing custom attributes in Cisco ISE Release 3.1 Patch 7.
CSCwh25160	Swap memory usage is high.
CSCwh64195	Data corruptions causing FailureReason=11007 or FailureReason=15022 in Cisco ISE.
CSCwf23271	The deployment SEC_TRNREP_STATUS isn't getting updated from the "In Progress" state.
CSCwf22527	In the Context Visibility page, the Endpoint Custom Attributes can't be filtered using special characters.
CSCwh71273	In Cisco ISE Release 3.2, there's limited GUI access and an inability to regenerate root CA when Essentials licenses are disabled.
CSCwh06338	The Cisco ISE GUI doesn't load when trying to edit the Client Provisioning Portal configuration.
CSCwi57761	CVE-2023-48795 seen in OpenSSH in Cisco ISE.
CSCwf27484	Unable to match Azure AD group if the user belongs to more than 99 groups.
CSCwj83460	Discrepancy in the count of identity groups between the CV and Oracle databases.
CSCwh71117	Enabling only "User Services" also enables admin GUI access.
CSCwi61491	The application server is crashing as a result of Metaspaces exhaustion.
CSCwh77574	Cisco ISE doesn't allow special characters in passwords while importing certificates.
CSCwf22794	Inconsistence on VLAN ID or name with the error "Error: Not a valid ODBC dictionary".
CSCwh69045	In Cisco ISE Release 3.1 Patch 5, the passwords of a few internal users aren't expiring even after the configured global password expiry date.
CSCwj44649	In Cisco ISE Release 3.3, TACACS data isn't retained and is purged.
CSCwh47299	The Cisco ISE Alarm and Dashboard Summary doesn't load.
CSCwi10922	The message description for message code 13036 has a misspelled word.
CSCwk30610	In Cisco ISE Release 3.2, the TACACS+ end-station network condition has high step latency while accessing the NAD using the console.

Caveat ID Number	Description
CSCwa32407	Resend the user account details for all guest users or specific guest users to the sponsor.
CSCwh36544	pxGrid doesn't show topic registration details.
CSCwi69659	During the TrustSec deployment verification, the policy difference alarm is triggered while policy the is identical on Cisco ISE and the NAD.
CSCwe12974	The text of the Out of Compliance for 30 days alarm needs to be updated.
CSCwh97876	Cisco Identity Services Engine Arbitrary File Upload Vulnerability.
CSCwd57628	In Cisco ISE Release 3.1, the NAD RADIUS shared secret key is incorrect when it starts with ' (apostrophe).
CSCwh70696	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability.
CSCwj21203	1000 database connections are exhausted due to "Dashboard System Status" query.
CSCwh05599	Cisco ISE Sponsor Portal is showing an invalid input when special characters are used in the Guest Type.
CSCwj39533	High CPU usage caused by RMQforwarder.
CSCwj60125	The User Account search and Manage Accounts functionality has been enhanced.
CSCwf89224	Decryption of session tickets received from the client fails on Cisco ISE.
CSCwi43166	TrustSec update with CoA or CoA-push is broken.
CSCwf36985	AD group retrieval fails while evaluating authorization policies.
CSCwi79159	Cisco ISE Release 3.2 Patch 4 displays a "deleteCertFromStore:- Failed to parse certificate" error.
CSCwk07483	The Profiler NetworkDeviceEventHandler failed to add a device as a result of the input containing "0-255" in the string.
CSCwj05508	The error "Name or service not known" is displayed when you try to reach the configured IP host under certain procedures.
CSCwc39545	The Docker Metrics Report needs to be changed.
CSCwf31073	Cisco ISE displays a 400 error when fetching the device administration network conditions using OpenAPI.
CSCwi86762	Right COA to be triggered in VPM flow when posture and MDM flows are configured together.
CSCwj43362	An upgrade to Cisco ISE Release 3.2 fails with the error - integrity constraint (CEPM.REF_HOSTCONFIG_HA_PEER1) violated.
CSCwh28528	The TopN device administration reports don't work when incoming TACACS records exceed 40 million records per day.

Caveat ID Number	Description
CSCwc85211	Cisco ISE Passive ID agent displays error "id to load is required for loading".
CSCwf51766	Cisco ISE can't create an authentication policy with DenyAccess identity source using OpenAPI.
CSCwj85626	Unable to retrieve the endpoint IP address using API calls.
CSCwi67639	The command "show cpu usage" doesn't display information in Cisco ISE 3.x releases.
CSCwj35581	Cisco ISE Missing Rate Limiting Protection.
CSCwj05881	Authentication fails and the advanced options are ignored in Cisco ISE.
CSCwh14249	There's a spelling mistake in API gateway settings in Cisco ISE 3.x releases.
CSCvz86688	Aruba-MPSK-Passphrase needs encryption support.
CSCwf09364	User and Endpoint Identity Groups description fields become not editable when using long-form text.
CSCwh10401	In Cisco ISE Release 3.1 Patch 5, the pxGrid client certificate can't be generated by using CSR.
CSCwj12489	Unable to delete Network Device Group.
CSCwh04251	Cisco ISE agentless posture doesn't support passwords containing ":" character.
CSCwk09094	A misleading pop-up seen while setting the password lifetime as more than 365 days.
CSCwf66237	Cisco ISE Get All Endpoints request takes a long time to execute since Cisco ISE Release 2.7.
CSCwk04644	In Cisco ISE Release 3.2 and later releases, System 360 Monitoring debug log rotation isn't working.
CSCwi38377	Unable to trigger COA and is stuck at the dispatcher queue.
CSCwi92655	The Context Visibility pages open drawer action displays an error while loading subtitles in Cisco ISE Release 3.3 Patch 1.
CSCwb18744	Security groups and contracts with multiple backslash characters in a row in the description can't sync to Cisco ISE.
CSCwd67833	This Cisco ISE ERS API is taking several seconds to update a single endpoint.
CSCwj35602	The requirement to enter the current password during a password update can be bypassed in Cisco ISE.
CSCwf96294	Connection attempts to domains in the "not allowed domains" list are observed in Cisco ISE Release 3.0.
CSCwd14523	The 'accountEnabled' attribute is causing authentication issues for EAP-TLS with Azure AD.

Caveat ID Number	Description
CSCwd34467	In Cisco ISE, the authorization rule evaluation appears to be broken for authorization attempts that use EAP-chaining and Azure AD groups.
CSCwj80589	An error is displayed while launching the Log Analytics page.
CSCwf23981	Cisco ISE authorization profile displays the wrong security group and VN value.
CSCwh64394	After the Import button is clicked, the .csv file shouldn't be selected and the Import button shouldn't work.
CSCvt75833	Cisco ISE should perform a NSLookup again when FQDN is the token server.
CSCwf64662	SXP creates inconsistent mapping between IP address and SGT.
CSCwj66951	The first name and last name fields in Network Access User doesn't allow for "OR" in the names.
CSCwe53824	Cisco ISE limits connection to AMP - AMQP service to TLSv1.0.
CSCwf82055	Unable to disable SHA1 for ports associated with Passive ID agents.
CSCwh53159	Unable to change the admin password if it contains "\$" in Cisco ISE Release 3.1 Patch 7.
CSCwi45090	The filter field 'name' isn't supported for downloadable ACLs through Cisco ISE ERS APIs.
CSCwi59567	Issues seen when the COA retry count is updated to "0".
CSCwe82004	TCP socket exhaustion.
CSCwj82298	Assigned logical profile is repeated in the endpoint attributes and reports on the Context Visibility page.
CSCwh48978	Evaluation of Open VM tools CVE-2023-20900.
CSCwj83459	Unable to create a new internal user and the error "couldn't execute statement; SQL [n/a]; constraint [CEPM.BKUPSLASTAUGHTIMEENTRY]" is displayed on the Cisco ISE GUI.
CSCwf71870	Evaluation of TACACS deployment with zero days won't work following smart licensing registration.
CSCvy34255	Extra pop-up screen appears while viewing the RADIUS and TACACS key after enabling "Require Admin password" to view sensitive data.
CSCwi36040	IP access list control in Cisco ISE Release 3.2 isn't visible.
CSCwj97449	The Cisco ISE admin isn't alerted about incorrect engineID format in snmp-server host during SNMPv3 configuration.
CSCwh67500	Cisco ISE Release 3.2 couldn't find selected authorization profiles.
CSCvs77939	Errors encountered while editing AnyConnect configurations and Posture agent profiles.

Caveat ID Number	Description
CSCwh88801	0.0.0.0 default static routes configured on all interfaces are deleted post Cisco ISE reload.
CSCwk07230	Duplicating network devices recreate the devices without RADIUS settings in Cisco ISE Release 3.3 Patch 2.
CSCwf72123	In pxGrid Direct, if the user data information is stored in nested objects within the data array, Cisco ISE is unable to them and it won't be visible in the pxGrid Direct Connector information in the Context Visibility page.
CSCwi66105	Custom attribute failure seen in Cisco ISE Release 3.1 Patch 7.
CSCwh41693	Cisco ISE on AWS doesn't work if Metadata (IMDS) version value "V2 only" selected.
CSCwh05647	Static IPV6 routes are removed after a reload in Cisco ISE Release 3.2.
CSCwh96376	Cisco ISE Release 3.3 can't switch the administration certificate role.
CSCwf34596	The user custom attributes are stuck in the rendering stage.
CSCwh38484	Manually deleting the static routes cause Cisco ISE to send packets with wrong MAC addresses in Cisco ISE Release 3.0 Patch 7.
CSCwj31619	In Cisco ISE Release 3.2 and later releases, conditions from Condition Studio has a default disabled icon in the information pop-up.
CSCwi52264	Cisco ISE SAML ID provider configuration attributes are deleted even when they are referenced elsewhere.
CSCwh00049	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability.
CSCwf59005	PEAP and EAP-TLS don't work on FIPS mode in Cisco ISE Release 3.2 Patch 3.
CSCwf80951	Can't edit or create admin user due to the error "xwt.widget.repeater.DataRepeater".
CSCwh01022	IPv6 default route disappears from the routing table after modifying the IPv6 address.
CSCwj80950	Cisco ISE isn't sharing posture-compliant session properly over pxGrid.
CSCwh30723	Cisco ISE context visibility doesn't validate static MAC entries if a separator like colon is omitted.
CSCwf38083	Cisco ISE services are stuck in the initializing state with secure syslogs.
CSCwi28131	Custom attributes used in the Never Purge rule are still purging the endpoints.
CSCwj12359	Interrupting execution of "show tech-support" causes services to stop on Cisco ISE.
CSCwj67980	Primary Guest Report shows duplicate entries of title when exported to an external repository.
CSCwi29253	Cisco ISE AD Diagnostic Tool stops working upon upgrade and you can't retrieve the list of available tests.

Caveat ID Number	Description
CSCwh93925	Cisco ISE incorrectly routes RADIUS Traffic when multiple static default routes are present.
CSCwh17386	Dedicated MnT nodes in Cisco ISE don't replicate SMTP configuration.
CSCwe89459	The script provided for creating endpoint group in the Cisco ISE REST API document is incorrect.
CSCwf25955	Matching authorization profiles with SGT, VN name, and VLAN causes PRRT to crash.
CSCwh18487	Expired guest accounts don't receive SMS when they try to reactivate their accounts.
CSCwj82278	Stale lock files are blocking the API gateway and the Context Visibility page.
CSCwb77915	Toggle to enable or disable RSA PSS cipher based on policies under Allowed Protocols.
CSCwh52589	When a guest user connects for to Cisco ISE for the first time, Cisco ISE doesn't update the ACS.Username field with the guest username.
CSCwh42442	CRL download failure seen in Cisco ISE Release 3.2 Patch 3.
CSCwi53915	The "Save" option under Advanced filters isn't working for filtering Client Provisioning resources.
CSCwj68795	Replication error "Error synchronizing object: EDF2EndPoint: Operation: Update" is displayed during replication in Cisco ISE.
CSCwh93498	In Cisco ISE Release 3.1, the endpoints purging rule is automatically created after duplicating the My Devices portal in Cisco ISE BYOD configuration causing endpoints to be deleted from the Cisco ISE database after 30 days.
CSCwh90610	The abandoned Jedis connections aren't being sent back to the thread pool in Cisco ISE.
CSCwf91508	Cisco ISE GUI packet captures that were taken from CLI can't be deleted.
CSCwe07822	Cisco ISE date of last purge has the wrong time stamp.
CSCwh55667	Internal system error for posture is seen when premier license is disabled in Cisco ISE.
CSCvz48764	Allow Launch program remediation to have a set order.
CSCwi19460	Unsupported message codes 91092 and 91103, and respective alarms seen in syslogs.
CSCwj14231	Cisco ISE Release 3.2 custom filters for TACACS reports don't work as expected.
CSCwh06081	Deregistering a Cisco ISE node should verify whether the process has been initiated by the primary PAN.
CSCwi17200	When configuring "TROUBLESHOOTING.EncryptionOffPeriod" advanced tuning with any nonzero value of minutes for decrypting the communication with Active Directory for troubleshooting, then RPC net logon fails for all Active Directory authentications on that Cisco ISE node.

Caveat ID Number	Description
CSCuz65708	The numbering of DACL entries is off in Mozilla Firefox 45 and above.
CSCwh51548	Hotpatches aren't getting installed when both patches and hotpatches are in ZTP configuration.
CSCwc26835	RADIUS server sequence configuration is corrupted.
CSCwi66608	In Cisco ISE Release 3.2, the RMQ is sending outgoing RST packets with APIPA IP 169.254.2.2.
CSCwj25817	Initial setup fails if the default gateway and configured IP address are on different subnets.
CSCwf39620	Windows Agentless Posture isn't working if the username starts with \$ (dollar sign).
CSCwh17448	In Cisco ISE Release 3.1, the Agentless Posture flows fail when the domain user is configured for endpoint login.
CSCvj75157	Cisco ISE API doesn't recognize identity groups while creating user accounts.
CSCvy30859	In Cisco ISE Release 2.6, it's impossible to create static IP-SGT mapping for EPGs imported from ACI.
CSCwi42412	In Cisco ISE 3.x releases, Interactive Help throws an error in the console and logs.
CSCwh81943	The portal name and results filters aren't working in the Primary Guest report.
CSCwh03740	CRL retrieval is failing.
CSCwj81776	Unable to use the advanced filter in Cisco ISE Release 3.2 for "Empty" and "Not Empty" filters.
CSCwj27469	Cisco ISE Release 3.3 on Cloud (Azure, AWS, OCI) isn't reading disk size properly and always defaults to 300 GB.
CSCwh96018	Failure due to case-sensitive check when new mobile device managers are created with the same name but with a different case.
CSCwk07593	Get-All Guest User API isn't retrieving all the guest accounts.
CSCwh99772	All network device groups are deleted after a child item is removed from any group.
CSCwf44906	After restoring a configuration backup, you must reconfigure the repository with new credentials.
CSCwj35576	Validation is missing on the Cisco ISE server.
CSCwi57903	No alarm is generated for a failed scheduled backup.
CSCwk07789	Invalid IP or hostname error is displayed when using "_" as the first character in the NSLookup request.
CSCwe12961	Evaluation Period Expired alarm is observed when the SLR license is out of compliance due to overconsumption.

Caveat ID Number	Description
CSCwj23933	The AD connector in not joined status update.
CSCwi11762	Korean support issue on Context Visibility page.
CSCwi59230	Only superadmin users can edit or delete endpoints when Cisco ISE has more than 1000 identity groups.
CSCwe15945	Guest accounts can't be seen by sponsors in a specific sponsor group.
CSCwf34391	When the PassiveID syslog is received by the MnT before the Active Authentication syslog, session integration isn't happening in Cisco ISE.
CSCwi57069	NA PRRT needs to be decoupled from logging using the main thread pool.
CSCwk13244	The ise-messaging.log not visible for download on the Cisco ISE GUI.
CSCwf14365	The warning "Configuration Missing" is seen when navigating to the Log Analytics page.
CSCwh24823	When nonmandatory attributes aren't included in the body of Update PUT requests, their values are reset to empty or the default value.
CSCwi53884	Vulnerabilities in OpenSSL 1.0.2o.
CSCwe25050	Wild-card certificate imported on primary PAN isn't replicated to other nodes in deployment.
CSCwc04447	Cisco ISE Release 2.7 Patch 6 is unable to filter NAD IP by IP address.
CSCwh30893	Profiling isn't processing the Calling Station ID values that are in the format "XXXXXXXXXXXXX".
CSCwi32576	PSN node crashed during assignment of CPMSessionID.
CSCwf40861	The Cisco ISE GUI is showing the HTML Hexadecimal code for the characters in the command set.
CSCwi11965	Cisco Identity Services Engine Server-Side Request Forgery Vulnerability.
CSCvu56500	Export of all network devices gives an empty file in Cisco ISE.
CSCwf59058	RBAC policy with custom permissions is working when the administration menu is hidden.
CSCwk32104	Both agentprobeoom.sh & restprobeoom.sh need to clean up their own OOM Heap files to optimize Cisco ISE database usage.
CSCwf85644	Cisco-av-pair throws an error when using % for PSK.
CSCwf66880	Endpoint .csv file import displays the error "No file chosen" after selecting the file.
CSCwa82035	Garbage collector logs, thread dump, and HEAP dump are missing from the support bundle.

Caveat ID Number	Description
CSCwh45472	Operational backups from the Cisco ISE GUI fail with the following status: "Backup Failed; copy to repository failed".
CSCwf40265	Cisco ISE maximum session counter time limit isn't working.
CSCwj07319	The API ers/config/session servicenode is returning the incorrect total.
CSCwf83193	Unable to log in to the secondary admin node's Cisco ISE GUI using AD credentials.
CSCwk00439	pxGrid Direct service is stuck in the initializing state because the lock file isn't removed.
CSCwf61939	Using an apostrophe in the First Name and Last name fields displays an invalid name error.
CSCwh18731	Upgrade to Cisco ISE Release 3.2 with LSD disabled before the upgrade workflow is causing a profiler exception.
CSCwh42009	In Cisco ISE Release 3.2 Patch 3, the adapter log information remains constant.
CSCwk20019	While using the SMS HTTP method as the SMS gateway the attribute name in the SMS HTTP URL causes problems.
CSCwk35172	The DumpClearOnExceed files are using excessive disk space on the Cisco ISE PSN nodes.
CSCwf62744	Addition of the "Disable EDR Internet Check" tag is a feature enhancement.
CSCwf44736	Cisco Identity Services Engine Cross-Site Request Forgery Vulnerability.
CSCwh26698	Addition of a mechanism to fetch user data for pxGrid connectors.
CSCwb57672	The GCMP256 authorization with the SHA384withRSA4096 certificate, a requirement in Android 12 for authorization, is failing the authorization process.
CSCwh41977	Verify the existence of per-user DACL on Cisco ISE configurations in Cisco ISE Release 3.2.
CSCwd21798	Cisco ISE-PIC license expiration alarms.
CSCwi53104	Exporting a report for a time period of over one month provides a report with no data.
CSCwj72680	HS_err files are being generated on the MnT nodes.
CSCvv77007	Cisco ISE is constantly requesting internal super admin users in response to external RADIUS token servers.
CSCwh46877	A COA port-bounce must take place when an ANC policy with PORT_BOUNCE is removed.
CSCwj72117	Operational data purging only shows the name of the primary monitoring node.
CSCwh32290	After performing a reset configuration with the FQDN value, a mismatch occurs between the GUI and the CLI.

Caveat ID Number	Description
CSCwc80574	Cisco ISE AD connector fails during a join operation.
CSCvg54133	There are changes to the hostname during printing on the CLI.
CSCvz62183	The debug profile isn't removed when the "reset to default" option is used in the debug log configuration.
CSCwk13234	Old Cisco ISE nodes are shown in the TCP dump and debug profile configuration after a restore operation.
CSCwj07675	Cisco ISE Release 3.2 is sending outgoing RST packets with APIPA IP 169.254.4.x.
CSCwf44942	Cisco ISE PSN crashes when maximum number of users are a part of the user session authentication flow using TACACS.
CSCwf22816	Authorization based on internal user ID group is failing without the RADIUS-token authorization for VPN.
CSCwi74567	Corruption in the Cisco ISE portal due to inconsistencies in the database.
CSCwh39802	Cisco ISE is sending misleading messages when it's unable to send an email to a guest after sponsor approval.
CSCwi72309	Cisco ISE is stuck in a profiling loop, slowing down replication, and causing errors.
CSCwe96739	TLS 1.0 or TLS 1.1 is accepted in the admin portal of Cisco ISE Release 3.0.
CSCwf54680	Unable to edit or delete authorization profiles which have parentheses in their names.
CSCwj74175	Compress restprobe-OOMHeap dumps.
CSCwf60904	ANC remediation isn't functioning properly with AnyConnect VPN.
CSCvm56115	Cisco ISE allows a policy to be saved even when the corresponding ID store is deleted from another browser tab.
CSCwf56826	Cores related to jstack can be observed on the primary PAN nodes in a regression setup.
CSCwd20521	AD connector process doesn't shut down.
CSCwh79938	You can't set the value of the preferred domain controllers registry during advanced tuning.
CSCwh03306	Threads get blocked on primary PAN if the port 1521 isn't available.
CSCwf78003	The endpoint details in the pxGrid Endpoints page are incorrect.
CSCwh42683	Read-only permissions provided for Cisco ISE admin access during SAML authentication.
CSCwi58699	COA is triggered using a Guest Flow when Cisco Catalyst Center or Endpoint Analytics dictionary attributes are updated on Cisco ISE.

Caveat ID Number	Description
CSCwh01906	The deleted MDM server is still listed in the allowed values under MDMServerName attribute.
CSCwi88583	The erl_crash.dump must be handled in a better way.
CSCwi42628	MAR cache replication fails between peer nodes for both NIC and Non-NIC bonding interfaces.
CSCwi75143	Unable to update the profiling settings as the PriorityType is mandated.
CSCwf97087	Posture feed update error is incorrect when there's a problem with the proxy.
CSCwj76445	Cisco ISE ERS Guest documentation should be updated to exclude the Portal ID from GET calls.
CSCwi93050	Endpoint import fails for RBAC when Azure SAML is used for administration access.
CSCwi12671	The TCP Dump diagnostic tool doesn't allow for simultaneous multiple interface captures on a node.
CSCwi33361	Problems seen with Cisco ISE CLI access as it fails to connect to the server.
CSCwh08440	Live log events 5422 and 5434 don't show any data in the Authentication and Authorization columns.
CSCwi34405	Unable to enforce the IdentityAccessRestricted attribute in the authorization policy.
CSCwj58727	Cisco ISE shouldn't allow a user to save the Allowed Protocols when no protocols have been checked.
CSCwf59338	Lack of cross-origin HTTP security headers in Cisco ISE.
CSCwh95022	Sponsor portal shows the wrong days of week information in the "Setting date" tab when using the Japanese GUI.
CSCvq79397	Cisco ISE GUI pages aren't loading properly with custom administration menu work center permissions.
CSCwh51156	Cisco ISE can't load corrupted NAD profiles causing authorization drops due to failure reasons 11007 and 15022.
CSCwh23367	In Cisco ISE Release 3.2, the subject line of the self-registration email truncates everything after the "=" sign on the Sponsor-Guest portal.
CSCvv85789	Cisco ISE HSTS header vulnerability on port 8084.
CSCwj47769	Cisco ISE can't download Passive ID agent.
CSCwi27497	Cisco ISE REST authorization service isn't running due to an error in the IP tables.
CSCwj32716	MDM configuration fails when the GUID in the client certificate is used to validate the compliance of the device.

Caveat ID Number	Description
CSCwf55795	With the ADE-OS restore option, the Cisco ISE GUI and CLI aren't accessible in Cisco ISE Release 3.2 Patch 1 and later releases.
CSCwi38912	The debug elements repeat three or more times in the debug profile configuration in Cisco ISE Release 3.3.
CSCwf40128	Accept client certificate without KU purpose validation as per CiscoSSL rules.
CSCwi20027	The TrustSec deployment request fails as the CoA request gets stuck while fetching NAD information.
CSCwf07855	Cisco ISE SXP Bindings API call returns 2x response when the call fails.
CSCwk38279	The ea.log file must be included in the support bundle.
CSCwh17285	In Cisco ISE Release 3.2 Patch 3 and Cisco ISE Release 3.3, the portals don't initialize if "IPV6 is enable" is the only IPV6 command on the interface.
CSCwj51329	MDM compliance check fails when there are multiple MAC addresses with VMWare Workspace One as the mobile device management server.
CSCwf02093	Nodes in Cisco ISE Release 3.2 running on Hyper-V are being assigned a DHCP address in addition to the static IP configured during the initial setup.
CSCwi63725	SNMPD process causes memory leak on Cisco ISE.
CSCwf30570	Agentless posture script is not running if the computer isn't connected to an AC power source.
CSCwh68651	Recreating the undo-tablespace causes URT to fail in Cisco ISE Release 3.1 Patch 7.
CSCwf94289	Policy export fails to export the policies in Cisco ISE Release 3.0 Patch 6.
CSCwj48827	Unable to add multiple tasks within quotes "" in the launch program remediation.
CSCwa08802	Cisco ISE Release 3.1 on AWS gives a false negative on the DNS check under health checks.
CSCwh88911	Cisco ISE database only allows for 100 characters in the email field for a Sponsor account.
CSCwf09393	In Cisco ISE Release 3.1, the services fail to start after restoring a backup from Cisco ISE Release 2.7.
CSCwf79582	AD Credentials fail to integrate with Cisco ISE with 2.2.1.x and later releases.
CSCwe99498	Cisco ISE includes a version of libcurl that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE-2023-27536,CVE-2023-27535,CVE-2023-27538.
CSCwh33160	Cisco ISE isn't sending SNMPv3 disk traps to configured SNMP servers.
CSCwh99534	The endpoint probe doesn't clean up SXP mappings.

Caveat ID Number	Description
CSCwj95818	Maximum concurrent CLI sessions don't work in Cisco ISE Release 3.4.
CSCwf61657	Gig 0 always participates in the TCP handshake of the sponsor FQDN.
CSCwh92185	RADIUS Authentication reports exported from the Operational Data Purging page are empty.
CSCwi54722	Redirect URLs using FQDN that end with the IP address have the IP address replaced by the Cisco ISE hostname.
CSCwh58768	Unable to delete existing devices in the My Device portal after restoring from Cisco ISE Release 2.7.
CSCwi89466	Cisco ISE AD User SamAccountName parameter is null for user sessions in Cisco ISE Release 3.2 Patch 3.
CSCwi78164	Cisco ISE DNS Resolvability Health Check fails due to a duplicated entry (IP, name, and FQDN).
CSCwk04493	Methods used for retrieving policy details use the internal method and aren't cached in Cisco ISE Release 3.1 Patch 6.
CSCwj03747	Profiling isn't suppressing CoA even if the option to suppress CoA for specific logical groups is enabled.
CSCwh21038	The session information isn't stored in the time session cache during third-party posture flows.
CSCwj80616	Endpoint details in the Cisco ISE Context Visibility page don't match with the RADIUS live logs or sessions during the MDM flow.
CSCwj48625	Agentless posture fails for EAP-TLS flows with multiple domains configured for endpoints to log in.
CSCwi45879	Unable to select hotspot portal if an existent or duplicated authorization profile is selected.
CSCwh65018	The Cisco ISE Release 3.1 Patch 5 install stalls indefinitely.
CSCwj59848	The Log Analytics page isn't launching in Cisco ISE.
CSCwh08408	Cisco ISE Release 3.3 can't register new nodes to the deployment after an upgrade as the node exporter password isn't found.
CSCwh72754	Impact on the authentications that use Active Directory as the identity source.
CSCwi66126	Updating the DACL doesn't modify the last update timestamp in the Cisco ISE ERS API.
CSCwi98793	Profiler is caching the MDM attributes with wrong values.
CSCwf37679	Sponsor permissions are disabled on the sponsor portal when they are accessed from the primary PAN.

Caveat ID Number	Description
CSCwi30707	In Cisco ISE Release 3.1 Patch 7, the removed device types can still be selected in the policy set.
CSCwi52041	Changes in rank cause the authorization rule to be committed to the database table which triggers the save call from the G UI
CSCwf98849	A critical error seen in Client Provisioning Portal customization.
CSCwi59312	Cisco ISE authorization profiles don't persist data with "Security Group" and "Reauthentication" common tasks.
CSCwh92117	The Sysaux tablespace is full due to the growth size of the AUD\$ table.
CSCwfl17714	Multiple entries of DockerMetric seen in reports in Cisco ISE Release 3.3.
CSCwc36589	Cisco ISE - Intune MDM integration may be disrupted due to the end of support for MAC address-based APIs from Intune.
CSCwf72918	In Cisco ISE Release 3.2, the order of the IP name-servers in the running configuration isn't respected.
CSCwf67438	Some VNs from the Author node aren't synced to the Reader node.
CSCwj52266	Endpoint description in the Context Visibility page is updated with the Static Identity Group description.
CSCwi94938	In Cisco ISE Release 3.2, the guest user API gives incorrect results when the filter is used.
CSCwj07717	Cisco ISE audit reports log APIPA addresses as the source of the API requests.
CSCwh28098	In Cisco ISE Release 3.2 Patch 3, the CoA Disconnect call is sent instead of the CoA Push call during a Posture Assessment when the RSD is disabled.
CSCwh46669	After the administration certificate change, Cisco ISE doesn't restart the services if the Bond interface is configured.
CSCwj43480	Cisco ISE Release 3.3 doesn't invoke MFA for the user with UPN (User Principle Name).
CSCwe53550	Cisco ISE and CVE-2023-24998.
CSCwi15793	An error with custom attribute special characters in Cisco ISE.
CSCwi89082	The Cisco ISE default portal is deleted from the database and is needed for SAML configuration.
CSCwh92366	Observing the Insufficient Virtual Machine Resource alarm in Cisco ISE Release 3.1 Patch 8.
CSCwj06269	No report or alarm is triggered for changes in the Device Administration settings.
CSCwj33906	IP or SXP mappings aren't created for VPN clients.

Caveat ID Number	Description
CSCwj21403	REST authorization services won't be enabled when hosts have multiple entries.
CSCwj36716	Cisco ISE Self-Persistent Cross-Site Scripting (XSS) is seen in My Reports.
CSCwh56565	Primary PAN REST calls to MnT nodes for live logs and reports aren't loaded balanced.
CSCwk61938	Cisco ISE to evaluate OpenSSH CVE-2024-6387.
CSCwh95232	Cisco ISE allows duplicate interface IP addresses.
CSCwi21020	Cisco ISE messaging certificate generation doesn't replicate the full certificate chain on secondary nodes.
CSCwf05178	Running the URT shows cosmetic warnings or errors.
CSCwi26921	The DumpClearOnExceed files can be seen by using the "dir" command in the Cisco ISE CLI.
CSCwj40026	Backups triggered from the Cisco ISE GUI have errors saying that backups were triggered from the CLI.
CSCwe03624	Smart license registration failure with "communication send error" alarms triggered intermittently.
CSCwf81550	Cisco ISE is changing the MAC address format according to the selected MAC address format even when it isn't a MAC device.
CSCwh36667	Cisco ISE monitoring GUI is stuck at the "Welcome to Grafana" page.
CSCwk07324	The main thread pool in Cisco ISE is stuck due to the ACE third-party library ContextIn leak.
CSCwh74236	The detailed Live Log page isn't loading for the TACACS+ authorization flow.
CSCwi25755	SAML Provider can't be added in Cisco ISE Release 3.2 and later releases.
CSCwi23166	Unable to save changes in the patch management condition.
CSCwh03227	Cisco ISE doesn't use the license during authorization.
CSCwh71435	The "Enable Password" of the internal users is created even when it's specified through ERS API.
CSCwh44407	The System Certificate Import doesn't work for Cisco ISE nodes in a deployment in Cisco ISE Release 3.2.

Open Caveats in Cisco ISE Release 3.4

This is the list of open caveats in Cisco ISE Release 3.4.

Caveat ID Number	Description
CSCwj57668	After upgrade, the MFC Profiler dashboard displays no data.

Caveat ID Number	Description
CSCwk38205	SGTs are not deleted when an ACI connection is deleted.
CSCwk39635	Duo MFA with VPN login does not work with MS-CHAP-v2.
CSCwk67747	RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS).
CSCwk74068	SXP bulk download missing entries after SXP node reload.
CSCwk78054	Endpoints are not listed in the Context Visibility page, but they are listed in the Live Logs and Live Sessions pages, when a standalone node is assigned both PPAN and PSN personas.
CSCwk79595	Page-level help for Inbound and Outbound SGT Domain Rules page is not working.
CSCwk85207	Authorization fails if DACL is not found in ISE configuration.
CSCwk98467	Data Upgrade and Restore from Cisco ISE 3.3 to 3.4 fails if username suffix is not configured in REST ID store.

Additional References

See [Cisco ISE End-User Resources](#) for additional resources that you can use when working with Cisco ISE.

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

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

Documentation Feedback

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

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

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

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

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

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

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

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

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

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.