

# Release Notes for Cisco Identity Services Engine, Release 3.2

---

**First Published:** 2022-08-16

**Last Modified:** 2024-04-29

## 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 3.2?

This section lists the new and changed features in Cisco ISE 3.2.

### Cisco Private 5G

From Cisco ISE Release 3.2 onwards, Cisco ISE supports Cisco Private 5G. Cisco ISE provides policy configuration for 5G and 5G authorization, that is implemented with RADIUS authorize-only and accounting flows.

For more information, see "[Configure Cisco Private 5G as a service](#)" in the Chapter "Secure Access" in the *Cisco ISE Administrator Guide, Release 3.2*.

## Cisco AnyConnect Rebranding

Cisco AnyConnect is rebranded as Cisco Secure Client.

Cisco ISE 3.2 supports Cisco Secure Client only for Windows OS. Windows OS supports both AnyConnect (version 4.10.5075 and later) and Cisco Secure Client (version 5.00529 and later). You can configure both for your endpoints on Windows OS but only one policy will be considered at run time for an endpoint.

For more information, see the Chapter "[Compliance](#)" in the *Cisco Identity Services Engine Administrator Guide, Release 3.2*.

## Cisco pxGrid Direct

Cisco pxGrid Direct helps you to connect to external REST APIs that provide JSON data for endpoint attributes. The data that are collected is based on the attributes you specify in your pxGrid Direct configurations. Then, pxGrid Direct stores the collected data in the Cisco ISE database.

This data can be used in the authorization policies. pxGrid Direct helps to evaluate and authorize the endpoints faster as the fetched data is used in the authorization policies. This eliminates the need to query for endpoint attribute data each time an endpoint must be authorized.

## Configuration of Authorization Policies for PassiveID Login Users

Check the **Authorization Flow** check box in the **Active Directory Advanced Settings** window if you want to configure authorization policies for PassiveID login users.

You can configure an authorization policy to assign an SGT to a user based on the AD group membership. This allows you to create TrustSec policy rules even for PassiveID authorization.

For more information, see "[Active Directory Settings](#)" in the Chapter "Asset Visibility" in the *Cisco Identity Services Engine Administrator Guide, Release 3.2*.

## Data Connect

The Data Connect feature provides 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. Only read-only access to the data is provided.

You can extract any configuration or operational data about your network depending on your business requirement and use it to generate insightful reports and dashboards.




---

**Note** If the Data Connect feature is active on your Cisco ISE Release 3.2 Limited Availability release, when you upgrade to the Cisco ISE Release 3.2 General Availability release you must disable and then enable the Data Connect feature.

---

## Deploy Cisco ISE Natively on Cloud Platforms

Cisco ISE Release 3.2 is natively available on the cloud platforms Amazon Web Services (AWS), Azure Cloud, and Oracle Cloud Infrastructure (OCI). For information on configuring Cisco ISE on the cloud platforms, see [Deploy Cisco Identity Services Engine Natively on Cloud Platforms](#).

## EAP-TLS and TEAP Authorization Support with Azure AD

Cisco ISE supports certificate-based authentication and Microsoft Entra ID authorization. The certificate-based authentications can be either EAP-TLS or TEAP with EAP-TLS as the inner method. Then, you can select attributes from Microsoft Entra ID and add them to the Cisco ISE dictionary. These attributes can be used for authorization. EAP Chaining the TEAP User session with an authenticated TEAP Computer session is not supported. Only user authentication is supported.

## Endpoint and Logical Profile Summary Report

This report lists the logical and endpoint profiles, and the number of endpoints matching those profiles.

For more information, see ["Available Reports"](#) in the Chapter "Maintain and Monitor" in the *Cisco Identity Services Engine Administrator Guide, Release 3.2*.

## ERS APIs Open API Specification

The Open API specification (JSON file) for ERS APIs is available for download in the Cisco ISE GUI, in the **Overview** section of the **API Settings** window (**Administration** > **System** > **Settings** > **API Settings** > **Overview**).

This Open API JSON file can be used for auto-generation of API client code using any programming language such as Python, Java, and so on. For additional information about Open API specifications and tools, see <https://openapi.tools/>.

## ERS APIs PATCH Request Support

Cisco ISE now supports PATCH request for ERS APIs. PATCH request helps in updating a subset of attributes for a resource. Only the attributes sent as part of the request are updated instead of updating the entire configuration for that resource. For more details, see [API Reference Guide](#).

## Managing Passwords of Cisco ISE Users

From Cisco ISE Release 3.2, as an internal user of Cisco ISE, you can manage the lifetime of your Enable and Login passwords using the **Password Lifetime** option. For more information, see ["Cisco ISE Users"](#) in the Chapter "Asset Visibility" in the *Cisco Identity Services Engine Administrator Guide, Release 3.2*.

## Mobile Device Management Enhancement

You can configure the **General MDM or UEM Settings** to query multiple MDM servers when the endpoints are not registered with the primary MDM or UEM server, or the primary MDM or UEM server is not reachable.

For more information, see ["Configure General MDM or UEM Settings"](#) in the Chapter "Secure Access" in the *Cisco Identity Services Engine Administrator Guide, Release 3.2*.

## Posture Condition Script Support

You can create and upload a posture condition script to perform any kind of posture check on an endpoint. The following platforms and script types are supported:

Platform	Supported Script Type
Windows	PowerShell script (.ps1)

Platform	Supported Script Type
macOS	Shell script (.sh)
Linux	Shell script (.sh)

For more information, see "[Add a Script Condition](#)" in the Chapter "Compliance" in *Cisco Identity Services Engine Administrator Guide, Release 3.2*.

## Required URL for Smart Licensing

Cisco ISE Release 3.2 uses <https://smartreceiver.cisco.com> to obtain Smart Licensing information.

## Security Settings Enhancement

When the **Allow SHA-1** Ciphers option (under **Administration > System > Settings > Security Settings**) is enabled, Cisco ISE allows SHA-1 ciphers for communication with the following Cisco ISE components:

- Admin Access UI
- Cisco ISE Portals
- ERS
- pxGrid

The following ports are used by these components for communication:

- Admin Access: 443
- Cisco ISE Portals: 9002, 8443, 8444, 8445, 8449
- ERS: 9060, 9061, 9063
- pxGrid: 8910

This option is disabled by default.

When you upgrade to Cisco ISE Release 3.2, the **Allow SHA-1** Ciphers option is disabled even if you have enabled this option before the upgrade. You can enable this option after the upgrade if you want to allow the clients with only SHA-1 ciphers to communicate with Cisco ISE. You must restart all the nodes in a deployment after enabling or disabling this option.

For more information, see "[Configure Security Settings](#)" in the Chapter "Segmentation" in the *Cisco Identity Services Engine Administrator Guide, Release 3.2*.

## Single Entry for Endpoints with GUID in Endpoint Context Visibility Window

If an endpoint that uses random MAC addresses connects to Cisco ISE and meets the following conditions, the **Endpoint Context Visibility** window displays only the latest MAC address for the endpoint:

- The endpoint connects to Cisco ISE through a certificate-based authentication method (such as EAP-TLS).
- The endpoint connects to Cisco ISE through an MDM server.

An endpoint that meets the preceding conditions are identified through a unique attribute that is called a GUID, instead of its MAC address. In the Cisco ISE GUI, in the **Context Visibility > Endpoints** window, an endpoint with a GUID is listed only once with its latest random MAC address.

The **MDM-GUID** column displays the consistent GUID that is assigned to the endpoint.

All the endpoint data that was available with the previous MAC address entry is carried forward to the new entry.

## Support for Extra Small Virtual Machine Deployment

Cisco ISE 3.2 supports extra small virtual machine deployment. You can enable only the PSN persona on this node. PAN and MnT personas are not supported for this node.

**Table 1: Extra Small Virtual Machine Requirements for On-premises Deployment**

Requirement Type	Specifications
No. of CPU cores	8
Memory	32 GB
Hard Disk	300 GB

**Table 2: Extra Small Virtual Machine Requirements for Cloud Deployment**

Cloud	Type/Size/Shape	vCPU	Memory
AWS	m5.2xlarge	8	32 GB
Azure	Standard_D8s_v4	8	32 GB
OCI	Standard3.Flex	8 (4 OCPU, where one Oracle Compute Unit [OCPU] is comparable to two vCPUs)	32 GB

For more information, see the [Cisco Identity Services Engine Installation Guide, Release 3.2](#).

## System 360

System 360 includes **Monitoring** and **Log Analytics**.

The **Monitoring** feature enables you to monitor a wide range of application and system statistics, and the key performance indicators (KPI) of all the nodes in a deployment from a centralized console. KPIs are useful to gain insight into the overall health of the node environment. Statistics offer a simplified representation of the system configurations and utilization-specific data.

Cisco ISE 3.2 and later releases are integrated with Grafana and Prometheus. Grafana is a third-party metrics dashboard and graph editor. It provides a graphical or text-based representation of statistics and counters collected in the Prometheus database. Prometheus is used as the datastore to store the KPIs in time series format. For more information about Grafana, see Grafana documentation.

The Grafana dashboard projects a comprehensive set of quantitative and qualitative data that helps you to analyze system metrics and take informed decisions. You can create customized Grafana dashboards to analyze

and monitor the required system metrics. To create customized Grafana dashboards, choose **Operations > System 360 > Monitoring**.

You can use built-in or custom queries for fetching the required data from the Prometheus data source. While creating Grafana dashboards, you can add new dashboard panels and specify the queries to be used for fetching the Prometheus data in the Queries tab.

The Monitoring service is enabled by default. You can disable or enable this service from **Operations > System 360 > Settings**.

**Log Analytics** provides a flexible analytics system for in-depth analysis of endpoint authentication, authorization, and accounting (AAA) and posture syslog data. You can also analyze the ISE health summary and ISE process statuses. You can generate reports similar to the ISE Counters and Health Summary reports. The Log Analytics service runs only on the MnT nodes.

Kibana, an open-source data visualization platform, is used to analyze and visualize the syslog data, and Elasticsearch is used to store and index the syslog data.

To enable Log Analytics, choose **Operations > System 360 > Settings** and enable the **Log Analytics** service.

For more information, see "[System 360](#)" in the Chapter "Maintain and Monitor" in the *Cisco Identity Services Engine Administrator Guide, Release 3.2*.

## View Cisco ISE in Default or Dark Mode

You can now view Cisco ISE in default (light) or dark mode. Choose the default or dark mode from the **Account Settings** dialog box in the Cisco ISE administrator portal.

See the topic "[Apply Default or Dark Mode in Cisco ISE](#)" in the chapter "Basic Setup" in the *Cisco ISE Administrator Guide, Release 3.2*.

## Zero Touch Provisioning – Security Update

The following security features are available, if you provision Cisco ISE through Zero Touch Provisioning (ZTP):

- **Public Key Authentication:** You can now login into the Cisco ISE CLI using your private key instead of password. For more information, see [Public Key Authentication](#).
- **First Login Password Change:** You will now be prompted to reset the admin password upon the first login into the Cisco ISE GUI. For more information, see [First Login Password Change](#).

## 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 3.2 can be installed on the following Secure Network Server (SNS) hardware platforms:

**Table 3: Supported Platforms**

Hardware Platform	Configuration
Cisco SNS-3595-K9 (large)	For appliance hardware specifications, see the <a href="#">Cisco Secure Network Server Appliance Hardware Installation Guide</a> .
Cisco SNS-3615-K9 (small)	
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)	

The following OVA templates are available for SNS 3600 series appliances:

- ISE-3.2.0.542a-virtual-SNS3615-SNS3655-300.ova
- ISE-3.2.0.542a-virtual-SNS3615-SNS3655-600.ova
- ISE-3.2.0.542a-virtual-SNS3655-SNS3695-1200.ova
- ISE-3.2.0.542a-virtual-SNS3695-1800.ova
- ISE-3.2.0.542a-virtual-SNS3695-2400.ova

The following OVA templates are available for SNS 3700 series appliances:

- ISE-3.2.0.542b-virtual-SNS3715-SNS3755-300.ova
- ISE-3.2.0.542b-virtual-SNS3715-SNS3755-600.ova
- ISE-3.2.0.542b-virtual-SNS3755-SNS3795-1200.ova
- ISE-3.2.0.542b-virtual-SNS3795-2400.ova



**Note** Cisco ISE 3.1 Patch 6 and above and Cisco ISE 3.2 Patch 2 and above support Cisco SNS 3700 series appliances.

## 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.
  - OVA templates: VMware version 14 or higher on ESXi 6.7 and ESXi 7.0.
  - ISO file supports ESXi 6.7 and later releases 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.

## Federal Information Processing Standard (FIPS) Mode Support

Cisco ISE uses embedded Federal Information Processing Standard (FIPS) 140-2-validated cryptographic module, Cisco FIPS Object Module Version 7.2 (Certificate #3790). For details about the FIPS compliance claims, see [Global Government Certifications](#).

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

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



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

## Supported Browsers

Cisco ISE 3.2 is supported on the following browsers:

- Mozilla Firefox versions 102, 103, 104, 105, 106, 107, 108, 110, 113, 114, 119, and 123
- Google Chrome versions 103, 104, 105, 106, 107, 108, 109, 110, 112, 114, 116, 117, 119, and 122
- Microsoft Edge versions 103, 104, 106, 107, 108, 109, 112, 115, and 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 4: Validated External Identity Sources**

External Identity Source	Version
<b>Active Directory</b>	
Microsoft Windows Active Directory 2012	Windows Server 2012
Microsoft Windows Active Directory 2012 R2 <a href="#">1</a>	Windows Server 2012 R2

External Identity Source	Version
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
<b>LDAP Servers</b>	
SunONE LDAP Directory Server	Version 5.2
OpenLDAP Directory Server	Version 2.4.23
Any LDAP v3 compliant server	Any version that is LDAP v3 compliant
AD as LDAP	Windows Server 2022 with Patch Windows10.0-KB5025230-x64-V1.006.msu
<b>Token Servers</b>	
RSA ACE/Server	6.x series
RSA Authentication Manager	7.x and 8.x series
Any RADIUS RFC 2865-compliant token server	Any version that is RFC 2865 compliant
<b>Security Assertion Markup Language (SAML) Single Sign-On (SSO)</b>	
Microsoft Azure MFA	Latest
Oracle Access Manager (OAM)	Version 11.1.2.2.0
Oracle Identity Federation (OIF)	Version 11.1.1.2.0
PingFederate Server	Version 6.10.0.4
PingOne Cloud	Latest
Secure Auth	8.1.1
Any SAMLv2-compliant Identity Provider	Any Identity Provider version that is SAMLv2 compliant
<b>Open Database Connectivity (ODBC) Identity Source</b>	
Microsoft SQL Server	Microsoft SQL Server 2012 Microsoft SQL Server 2022
Oracle	Enterprise Edition Release 12.1.0.2.0
PostgreSQL	9.0
Sybase	16.0

External Identity Source	Version
MySQL	6.3
<b>Social Login (for Guest User Accounts)</b>	
Facebook	Latest

<sup>1</sup> Cisco ISE supports all the legacy features in Microsoft Windows Active Directory 2012 R2. However, the new features in Microsoft Windows Active Directory 2012 R2, such as 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 3.2 is validated with OpenSSL 1.1.1k.

### 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.

### Microsoft Compliance Retrieval API Support for Ethernet MAC Address-based APIs

Microsoft Compliance Retrieval API currently does not support the Ethernet MAC attribute for MAC address-based APIs. This limitation will be addressed by Microsoft in January 2024. For wired deployments, we recommended that you to migrate to GUID-embedded certificates before upgrading to the following patches: Cisco ISE Release 3.1 Patch 8, Cisco ISE Release 3.2 Patch 4, or Cisco ISE Release 3.3 Patch 1.

## Hot Patch for RADIUS Live Log Delays

In Cisco ISE Release 3.2 Cumulative Patches 2, 3, and 4, you may experience RADIUS live logs delay as explained in [CSCwi06794](#). You must install the following hot patch to fix this issue:  
ise-apply-CSCwi06794\_3.1.x\_patchall-SPA.tar.gz.

## Hyper-V Installations have DHCP Enabled on eth0 Interface

When Cisco ISE 3.2 main or patch release is installed on Microsoft Hyper-V (fresh installation), DHCP is enabled on eth0 interface. This issue is not seen when you upgrade to Cisco ISE 3.2 main or patch release.

You might see the following issues when Cisco ISE is installed on Hyper-V:

- Cisco ISE 3.2 node running on Hyper-V will be assigned a DHCP address in addition to the static IP configured during the initial setup.
- Gateway and NTP ping might fail inconsistently.
- Cisco ISE GUI might not be accessible in some cases.
- Deployment and other operations might fail due to network communication issues.

You must install the following hot patch to fix this issue:

ise-apply-CSCwf02093\_3.2.x\_patchall-SPA.tar.gz

To install this hot patch:

1. Log in to Cisco ISE CLI.
2. Run the following command to install the bundle that will apply the hot patch:

```
application install ise-apply-CSCwf02093_3.2.x_patchall-SPA.tar.gz <Repository_Name>
```

3. After the hot patch is successfully installed, run the **reset-config** command on the Hyper-V admin console to reset the network configurations such as ip address/mask/gateway, hostname, domain name, DNS server, and NTP server. This command will not reset the configuration data in Cisco ISE.



### Note

- Note that you need to run the **reset-config** command on the Hyper-V admin console.
- You must not use the **application reset-config ise** command

4. Enter the required setup details to complete reset-config operation.

## Antimalware Condition for ClamWin Products

You might see the following error message while trying to add an antimalware condition for ClamWin Pty Ltd vendor:

```
class com.cisco.cpm.posture.exceptions.PostureException:Check am_linux_def_v4_ClamWinPtyLtd
is not found
```

When multiple ClamWin products with 0.x version are listed in the **Baseline Condition** tab, if you select any of those products and configure an antimalware condition, the above error message might be displayed.

In such a scenario, you must run the posture feed update one or more times to remove the multiple entries for 0.x version.

As a workaround, you can select a product from the **Advanced Condition** tab and configure an antimalware condition for ClamWin Pty Ltd vendor.

## Host alias is not added or removed automatically when IPv6 address is configured on an interface

From Cisco ISE Release 3.2 onwards, the host alias of the corresponding IP address is not added or removed automatically, when IPv6 address is configured on an interface. You must add or remove the host alias manually by executing the following **ip host** commands.

To add the host alias:

```
ip host 2001:420:54ff:4::456:00 demo demo.cisco.com
```

To remove the host alias:

```
no ip host 2001:420:54ff:4::456:00 demo demo.cisco.com
```

## 3.2P5 SLR registered Node shows SL registered post patch rollback

If you install Cisco ISE Release 3.2 Patch 5 or later releases on a Cisco ISE node, enable Specific License Registration (SLR), and then roll back to an earlier release, the node is automatically registered to Smart Licensing (SL) instead of SLR. In this case, you cannot return SLR because deregistration or update operations will not work due to incorrect licensing configuration. This issue can be resolved through TAC intervention.

To avoid this, you must return SLR before rolling back to an earlier release. Each node has a unique code that you must submit in the Cisco Smart Software Manager (CSSM) to return SLR. If you had enabled SLR before installing Cisco ISE Release 3.2 Patch 5 or later, you do not have to return SLR before rolling back to an earlier release.

## 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 3.2

You can directly upgrade to Release 3.2 from the following Cisco ISE releases:

- 2.7
- 3.0
- 3.1

If you are on a version earlier than Cisco ISE, Release 2.7, you must first upgrade to one of the releases listed above, and then upgrade to Release 3.2.

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

Cisco ISE, Release 3.2, has parity with the Cisco ISE patch release: 2.7 Patch 7, 3.0 Patch 6, and 3.1 Patch 3, and earlier patches.

## Upgrade Packages

For information about the upgrade packages and the 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 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 3.2. 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 3.2 - Cumulative Patch 6

Caveat ID Number	Description
<a href="#">CSCwf47838</a>	Space characters in Command Arguments are not preserved after CSV Export of TACACS+ Command Set.
<a href="#">CSCwi60778</a>	Endpoint Loses Static Identity Group Assignment after Reauthentication.
<a href="#">CSCwf24553</a>	SR-Insights - Umbrella defect for providing information for terminologies used in Licensing page.
<a href="#">CSCwf24554</a>	SR-Insights - Umbrella defect for displaying more information on SL registration failure.
<a href="#">CSCwi89466</a>	Cisco ISE AD User SamAccountName parameter is null for user session (3.2 P3 or later).
<a href="#">CSCwi58699</a>	CoA is triggered through a Guest Flow when DNAC/EA dictionary attributes are updated on Cisco ISE.
<a href="#">CSCwi62078</a>	[404] Resource Not Found when using the built-in Authorization profile Block_Wireless_Access.
<a href="#">CSCwi58421</a>	PSN node does not update the DB with correct posture expiry time when posture lease is enabled.
<a href="#">CSCwi34405</a>	Unable to enforce IdentityAccesss Restricted attribute during authorization.
<a href="#">CSCwi61491</a>	Application Server Crashes Due to Metaspace exhaustion.
<a href="#">CSCwi29253</a>	Cisco ISE AD Diagnostic Tool stops working upon upgrade, unable to retrieve list of available tests.
<a href="#">CSCwh33160</a>	Cisco ISE does not send SNMPv3 disk traps to configured SNMP server.
<a href="#">CSCwi53104</a>	Export of the report beyond a one-month period yields no data.
<a href="#">CSCwf61673</a>	Cisco ISE CLI Read only users can not run show CPU usage command.
<a href="#">CSCwi54722</a>	Redirect URL use fqdn that ends with IP, IP is repalced by Cisco ISE hostname.
<a href="#">CSCwi15793</a>	Cisco Identity Services Engine custom attribute special characters error.
<a href="#">CSCwa15336</a>	Cisco ISE PIC 3.1: Live Session should not show terminated sessions.
<a href="#">CSCwi59868</a>	Sponsored guest account extension works more than maximum number of days.

Caveat ID Number	Description
<a href="#">CSCwi45090</a>	Cisco ISE : REST API ERS : downloadableacl : The filter field 'name' is not supported.
<a href="#">CSCwi89082</a>	Cisco ISE Portal (default) Deleted from database which is needed to configure SAML.
<a href="#">CSCwi42628</a>	MAR Cache replication failed between peer nodes for both NIC and NON-NIC bonding interfaces.
<a href="#">CSCwi36040</a>	IP access list control in Cisco ISE Release 3.2 is not visible.
<a href="#">CSCwi34117</a>	Grafana UI and Kibana should have RBAC implemented in Identity Services Engine.
<a href="#">CSCwh67500</a>	Cisco ISE 3.2 Could not find selected Authorization Profiles.
<a href="#">CSCvs77939</a>	Errors editing AnyConnect configuration and Posture Agent profiles.
<a href="#">CSCwj21203</a>	1000 DB connections exhausted due to "Dashboard System Status" query.
<a href="#">CSCwj03747</a>	Profiling is not suppressing CoA although we have suppress CoA for specific logical groups.
<a href="#">CSCwi32576</a>	PSN node crashes while assigning the cpmSessionId.
<a href="#">CSCwj16540</a>	Cisco ISE 3.2 Patch 4 Context Visibility does not match Live Logs or Sessions.
<a href="#">CSCwi45879</a>	Unable to select hotspot portal if an existent or duplicated authorization profile is selected.
<a href="#">CSCwi53915</a>	Advanced Filter "Save" option does not work for Client Provisioning Resources filtering.
<a href="#">CSCwf89224</a>	Decryption of Session ticket received from the client fails on Cisco ISE.
<a href="#">CSCwh99772</a>	All network device groups are deleted after removing a child item from any group.
<a href="#">CSCwi86161</a>	[ESXi VA] Functional: mDNAC role UNDEFINED and unable to start ACA migration after Cisco ISE integration.
<a href="#">CSCwj47769</a>	Invalid Request page in Cisco ISE Release 3.2 Patch 5.
<a href="#">CSCwh41977</a>	Cisco ISE 3.2 : Verify existence of Per-User dACL on Cisco ISE configuration.
<a href="#">CSCwh56565</a>	PPAN rest call to MNT nodes (live logs, reports) should not be load balanced.
<a href="#">CSCwj44477</a>	Upgrade Issue - "Database upgrade failed" message.
<a href="#">CSCwi57903</a>	No alarm generated for failed schedule backup.
<a href="#">CSCwj07319</a>	API ers/config/sessionsservicenode returns incorrect total.
<a href="#">CSCwi73984</a>	Cisco ISE 3.1P8 Installed Patches menu does not list all the patches.
<a href="#">CSCwi33361</a>	Cisco ISE CLI access problems: Failed to connect to server.



Caveat ID Number	Description
<a href="#">CSCwi21020</a>	Cisco ISE Messaging Certificate generation does not replicate full certificate chain on secondary nodes.
<a href="#">CSCwh72754</a>	Cisco ISE active directory process (lwsmd) stuck at "Updating" and consuming 90-100% CPU.
<a href="#">CSCwi66126</a>	Cisco ISE ERS API - Updating DACL does not modify last update timestamp.
<a href="#">CSCwc85211</a>	Cisco ISE Passive ID Agent error "id to load is required for loading".
<a href="#">CSCwi57950</a>	Cisco ISE 3.2 : Nexpose Rapid 7 : Strict-Transport-Security malformed.
<a href="#">CSCwi98793</a>	Profiler caching mdm attribute with wrong values.
<a href="#">CSCwi17694</a>	Cisco ISE: synflood-limit does not take effect if configured with more than 10000.
<a href="#">CSCwd67833</a>	ERS API takes several seconds to update single endpoint.
<a href="#">CSCwi67639</a>	Command show cpu usage does not display information on Cisco ISE 3.X.
<a href="#">CSCwi30707</a>	Cisco ISE 3.1 patch 7 : Removed Device Types remain selectable in Policy Set.
<a href="#">CSCwi73981</a>	Cannot remove identity store from CLI that was added using uppercase FQDN.
<a href="#">CSCwi89689</a>	Cisco ISE - Invalid IP or hostname error.
<a href="#">CSCwi94938</a>	Cisco ISE 3.2 guest user API gives incorrect results when filter used.
<a href="#">CSCwi59216</a>	Sponsor Portal returns 400 Bad Request when clicking (Contact Support).
<a href="#">CSCwi59567</a>	Issues with updating the CoA retry count to "0" .
<a href="#">CSCwi52264</a>	Cisco ISE SAML ID provider Configuration Attributes are deleted though they are referenced.
<a href="#">CSCvt75833</a>	Cisco ISE should do nslookup again when the token server is FQDN.
<a href="#">CSCwi17200</a>	Cisco ISE: TROUBLESHOOTING.EncryptionOffPeriod causes RPC netlogon failure.
<a href="#">CSCwi48806</a>	Authorization policy take time to load cause duo portal enteries.
<a href="#">CSCwi96581</a>	Upgrade CXF Version as 3.4.2 is vulnerable.
<a href="#">CSCwi88504</a>	Cisco ISE Release 3.2P5 : missing step and resolution text in live logs for attribute.
<a href="#">CSCwi59230</a>	Non super-admin users cannot edit or delete endpoints when Cisco ISE has more than 1k identity groups.
<a href="#">CSCwf80386</a>	Current value of Disable_RSA_PSS environmental value is not preserved upon patch installation.
<a href="#">CSCwi63725</a>	SNMPD process causing memory leak on Cisco ISE.
<a href="#">CSCwi25755</a>	From Cisco ISE 3.2 or higher. Cannot Add SAML Provider.

Caveat ID Number	Description
<a href="#">CSCwh25160</a>	Swap cleanup script to drop the swap area and program the cron.
<a href="#">CSCwf51766</a>	Cisco ISE cannot create a Authentication Policy with DenyAccess Identity Source through OpenAPI.
<a href="#">CSCwj06401</a>	Endpoints has null key value pair in the attributes section is interrupting the purge flow.
<a href="#">CSCwd14523</a>	'accountEnabled' attribute causes authentication issues for EAP-TLS with Azure AD.
<a href="#">CSCwh61339</a>	Export of more than 90k Network Devices time out.
<a href="#">CSCwa32407</a>	ENH : resend the user account details for all or specific guest users to the sponsor.
<a href="#">CSCwh92366</a>	3.1P8: Observing Insufficient Virtual Machine Resource Alarm in 3.1P8 Longevity setup.
<a href="#">CSCwf17714</a>	Cisco ISE 3.3 BH : Multiple entries of DockerMetric seen in reports.

## New Features in Cisco ISE Release 3.2 - Cumulative Patch 5

### Opening TAC Support Cases in Cisco ISE

From Cisco ISE Release 3.2 Patch 5, you can open TAC Support Cases for Cisco ISE directly from the Cisco ISE GUI.

For more information, see "[Open TAC Support Cases in Cisco ISE](#)" in the chapter "Troubleshoot" in *Cisco ISE Administrator Guide, Release 3.2*.

### Localized ISE Installation

While reinstalling Cisco ISE, you can use the **Localized ISE Install** option (option 36) in the **application configure ise** command to reduce the installation time. By using this option, you can reduce the reinstallation time from an average of 5-7 hours, to approximately 1-2 hours.

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 "[application configure](#)" in the Chapter "Cisco ISE CLI Commands in EXEC Mode" in the *Cisco Identity Services Engine CLI Reference Guide, Release 3.2*.

### 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 3.2*.

## Resolved Caveats in Cisco ISE Release 3.2 - Cumulative Patch 5

Caveat ID	Description
<a href="#">CSCwb57672</a>	GCMP256 authentication for SHA384 with RSA4096 certificate failed
<a href="#">CSCwh36544</a>	PxGrid not showing topic registration details
<a href="#">CSCwh42683</a>	Read-Only permissions for SAML users
<a href="#">CSCwh64195</a>	Data corruptions causing FailureReason=11007 or FailureReason=15022
<a href="#">CSCwh99534</a>	Endpoint Probe does not clean up SXP mappings
<a href="#">CSCwh24823</a>	When non-mandatory attributes are not included in the PUT requests, those values are reset to empty or default
<a href="#">CSCwd48787</a>	ISE - SSL buffer is not cleared and affects PAC decryption
<a href="#">CSCwh90691</a>	Show CLI commands throws exception after configuring log level to 5
<a href="#">CSCwh83323</a>	SMS not sent in "Reset Password" flow when a custom "SMTP API Destination Address" is used
<a href="#">CSCwe25050</a>	Wildcard certificate imported on PPAN not replicated to other nodes in deployment
<a href="#">CSCwi18005</a>	External RADIUS server list does not show up after upgrading to ISE 3.2
<a href="#">CSCwd21798</a>	ISE-PIC license expiration alarms
<a href="#">CSCvj75157</a>	ISE API doesn't recognize identity groups while creating user accounts
<a href="#">CSCwh63501</a>	Vulnerabilities in log4net 2.0.8.0
<a href="#">CSCwi37249</a>	Endpoints profiled incorrectly as Android devices
<a href="#">CSCvz86688</a>	Aruba-MPSK-Passphrase needs encryption support
<a href="#">CSCwh58768</a>	Unable to delete existing devices in My Device portal after restoring from ISE 2.7 version
<a href="#">CSCwh47601</a>	Unable to create SNMPv3 user with auth and priv passwords equal to 40 characters
<a href="#">CSCwh18899</a>	Need support for system certificate import for multi-node cluster in ISE OpenAPI
<a href="#">CSCwc04447</a>	Unable to filter the TACACS Live Logs via Network Device IP
<a href="#">CSCwh17285</a>	Portals fail to initialize if IPv6 enable is the only IPv6 command on interface
<a href="#">CSCwh70696</a>	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability
<a href="#">CSCwi04514</a>	Posture client provisioning resources HTTP error when dictionary attribute contains "-"
<a href="#">CSCwh24754</a>	Excess number of AD groups mapped to sponsor groups causing latency in sponsor login

Caveat ID	Description
<a href="#">CSCwh81035</a>	PAN missing non-significant attribute updates of endpoints from PSNs
<a href="#">CSCwh10401</a>	Cannot generate pxGrid client certificate leveraging CSR
<a href="#">CSCwh60726</a>	ISE lwsm decodes are not done properly
<a href="#">CSCwh77574</a>	ISE not allowing special characters for password while importing certificate
<a href="#">CSCwh55667</a>	Posture failure due to expired or invalid license reported as Internal System Error in AnyConnect ISE Posture reports
<a href="#">CSCwh88801</a>	0.0.0.0 default static routes configured on all interfaces get deleted post reload
<a href="#">CSCwfl0516</a>	Authorization policy search feature not working
<a href="#">CSCwi45131</a>	Apache Struts Vulnerability Affecting Cisco Products: December 2023
<a href="#">CSCwi27497</a>	REST Auth service not running on ISE node
<a href="#">CSCwh52589</a>	Acs.Username is not being updated with guest username in first device connection
<a href="#">CSCwh30723</a>	ISE Context Visibility doesn't validate static MAC entries if they miss a separator like colon
<a href="#">CSCwh92185</a>	Radius Authentication report exported from the Operational Data Purging page are empty
<a href="#">CSCwh83482</a>	ISE database not updating the email field for Sponsor Accounts
<a href="#">CSCwh96018</a>	Failure due to case sensitive check when new MDMs are created with the same name but different case
<a href="#">CSCwh99772</a>	All network device groups are deleted when a child item is removed from any group
<a href="#">CSCwh93498</a>	Endpoints purging rule automatically created when duplicate option is used for My Devices portal
<a href="#">CSCwh90610</a>	ISE Abandoned Jedis connections not being sent back to the threadPool
<a href="#">CSCvo60450</a>	Enhancement for encryption to only send AES256 for MS-RPC calls
<a href="#">CSCwi03961</a>	Location group information is missing from policy sets
<a href="#">CSCwh41977</a>	Verify existence of Per-User dACL on ISE configuration
<a href="#">CSCwh79938</a>	Cannot set PreferredDCs registry value in advanced tuning
<a href="#">CSCwh30893</a>	Profiling not processing the Calling Station ID values with the following format "xxxxxxxxxx"
<a href="#">CSCwh84446</a>	Guest Type save doesn't work when Account Expiration Notification has special or newline character

Caveat ID	Description
<a href="#">CSCwh45472</a>	Operational Backups from the GUI fail to SFTP Repositories if the PKI key pair passphrase contains +
<a href="#">CSCwh38464</a>	ISE CLI admin user unable to login after 2 months of inactive period
<a href="#">CSCwi06794</a>	RADIUS Live log delay Regression for CSCwe00424
<a href="#">CSCwh71117</a>	Enabling only "User Services" enables Admin GUI Access as well.
<a href="#">CSCwh95022</a>	Sponsor portal shows wrong days of week information from [Setting date] tab when using Japanese UI
<a href="#">CSCwf25955</a>	Matching authorization profile with SGT, VN name, Vlan empty causes prrt to crash
<a href="#">CSCwf61657</a>	Gig0 always involved in TCP Handshake of Sponsor FQDN
<a href="#">CSCwd34467</a>	Authorization rule evaluation broken for attempts using eap-chaining and Azure AD groups
<a href="#">CSCwi15914</a>	Additional IPV6-SGT session binding created for IPV6 link local address from SXP Add operation
<a href="#">CSCwh70275</a>	Registering node with left over certificates from deregistration can delete in use certificates
<a href="#">CSCwh69045</a>	Few internal users password not expiring after configured global password expiry days
<a href="#">CSCwh26698</a>	Add a mechanism to fetch user data for pxGrid connector
<a href="#">CSCwf98849</a>	Critical Error displayed while saving changes made to Client Provisioning portal
<a href="#">CSCwh71273</a>	Limited GUI access/Inability to regenerate Root CA when essentials licenses are disabled
<a href="#">CSCwi23166</a>	Unable to save changes in the patch management condition
<a href="#">CSCwh51156</a>	Corrupted NAD profiles are not loaded and authentication failed with FailureReasons 11007 and 15022
<a href="#">CSCwi59555</a>	Search for MAC Address in xx:xx:xx:xx:xx:xx format ignored
<a href="#">CSCwh47299</a>	ISE Alarm and Dashboard Summary does not load
<a href="#">CSCwf64662</a>	SXP can create inconsistent mapping between IP address and SGT
<a href="#">CSCwh26288</a>	pxGrid Direct: Premier license is required to add a connector, feature should only need Advantage
<a href="#">CSCwc53824</a>	ISE limits connection to AMP AMQP service to TLSv1.0
<a href="#">CSCwi05905</a>	ISE ERS API - /ers/config/deploymentinfo/getAllInfo returns different data on multi-node deployments

Caveat ID	Description
<a href="#">CSCwh23367</a>	ISE 3.2 Self-Reg Email Subject line truncates everything after "=" sign on Sponsor-Guest Portal
<a href="#">CSCwh53159</a>	Unable to change admin password if it contains "\$"
<a href="#">CSCwh71435</a>	Enable password of the internal users is created even when this is not specified through ERS API
<a href="#">CSCwf38083</a>	ISE services stuck in initializing state with secure syslog
<a href="#">CSCwh93925</a>	ISE incorrectly routes RADIUS Traffic when multiple static default routes are configured
<a href="#">CSCwi28131</a>	Endpoints with custom attributes used in Never Purge rule are still purged
<a href="#">CSCwf55795</a>	After ADE-OS restore, ISE UI and CLI not accessible in 3.2P1 and above
<a href="#">CSCwi36954</a>	When MnT database usage exceeds threshold, database purge done based on retention days set for RADIUS
<a href="#">CSCwf72037</a>	Administrator Login Report shows "Administrator authentication failed" every 5 minutes
<a href="#">CSCwh21038</a>	Session information is not stored in the timed session cache during third party posture flow
<a href="#">CSCwi19099</a>	Issue while inserting the data to the config folder if any of the connector is disabled

## Open Caveats in Cisco ISE Release 3.2 - Cumulative Patch 5

These are open caveats in Cisco ISE Release 3.2 - Cumulative Patch 5.

Caveat ID Number	Description
<a href="#">CSCwh92366</a>	In 3.1 Patch 8: Observing Insufficient Virtual Machine Resource Alarm in 3.1 Patch 8 Longevity setup.

## New Features in Cisco ISE Release 3.2 - Cumulative Patch 4

### 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 3.2](#).

## 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 3.2 Patch 4, 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](#).

## 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 3.2](#).

## Resolved Caveats in Cisco ISE Release 3.2 - Cumulative Patch 4

Caveat ID	Description
<a href="#">CSCwf80509</a>	Cisco ISE Passive ID session aging time is always an hour irrespective of the configuration.
<a href="#">CSCwc71060</a>	Deleted network device groups still show up on policy sets.
<a href="#">CSCwe37377</a>	Cisco ISE srl retrieval failing alarm needs to print the server on which the srl download failed.
<a href="#">CSCwc33290</a>	Unable to delete custom endpoint attributes.
<a href="#">CSCwf83193</a>	Unable to log into secondary administration node's GUI using AD credentials.
<a href="#">CSCwf32641</a>	Cisco ISE Release 3.3 BH SNMP engine ID is the same in all nodes.
<a href="#">CSCwh17386</a>	Dedicated MNT nodes do not replicate the SMTP configuration.
<a href="#">CSCwe89459</a>	ISE Rest API document provided by the script is incorrect while creating the endpoint group.
<a href="#">CSCwe15576</a>	Unable to configure the KRON job.
<a href="#">CSCwh18487</a>	Guest expired accounts do not receive SMS when you reactivate the account.
<a href="#">CSCwd82539</a>	For local and global exception rules, if only SecGroup is selected in results, the rule does not match.

Caveat ID	Description
<a href="#">CSCwh06338</a>	Cisco ISE GUI does not load when you edit Client Provisioning Portal configuration.
<a href="#">CSCwf68108</a>	'Asset' attributes and pxGrid context-in through OpenAPI.
<a href="#">CSCwe54318</a>	SXP service gets stuck at initializing state due to H2 DB delay in querying bindings.
<a href="#">CSCwd12453</a>	Cisco ISE Release 3.1 portal tag with special character validation issues.
<a href="#">CSCwb63834</a>	MNT log processor runs on a non-management admin Cisco ISE node.
<a href="#">CSCwf27484</a>	Unable to match Azure AD group in authorization due to lack of paging in the query to Azure.
<a href="#">CSCwf19811</a>	Cisco ISE 3.1 SXP bindings report shows no data found.
<a href="#">CSCwf22794</a>	Inconsistency in VLAN ID and Name 'Error: Not a valid ODBC dictionary'.
<a href="#">CSCvq79397</a>	UI pages do not load properly with custom admin menu workcenter permissions.
<a href="#">CSCuz65708</a>	Mozilla Firefox 45 and Google Chrome 72: Incorrect line numbering for DACL.
<a href="#">CSCwf59005</a>	Cisco ISE Release 3.2 Patch 3: PEAP and EAP-TLS do not work in FIPS mode.
<a href="#">CSCwh51548</a>	Cisco ISE 3.2.0.542: Hotpatches don't install when both patch and hotpatches are in ZTP Configuration.
<a href="#">CSCwc26835</a>	RADIUS server sequence configuration is corrupted.
<a href="#">CSCwf44906</a>	Reconfiguring repositories with credentials is necessary after restoration of configuration backup.
<a href="#">CSCwf39620</a>	Windows agentless posture does not work if the username starts with \$ (dollar sign).
<a href="#">CSCwh17448</a>	Cisco ISE Release 3.1 - Agentless posture flows fail when domain user is configured for endpoint login.
<a href="#">CSCwf72918</a>	In Cisco ISE Release 3.2, the order of IP name-servers in the running configuration is incorrect.
<a href="#">CSCwd57628</a>	Cisco ISE Release 3.1 NAD radius shares a secret key incorrectly when it starts with an apostrophe symbol.
<a href="#">CSCwh46669</a>	After the admin certificate change, Cisco ISE does not restart services if the bond interface is configured.
<a href="#">CSCwh26288</a>	pxGrid Direct: A premier license is required to add a connector. The feature should only need advantage license.
<a href="#">CSCwe10898</a>	The endpoint MAC address is not added to Endpoint Identity Group when using grace access in guest portal.
<a href="#">CSCwh42009</a>	Cisco ISE Release 3.2 Patch 3 : Adapter log issue.
<a href="#">CSCwf22527</a>	Context Visibility: Endpoint custom attributes cannot be filtered with special characters.



Caveat ID	Description
<a href="#">CSCwf88944</a>	Guest portal FQDN is mapped with the IP address of node in database.
<a href="#">CSCwd38766</a>	Deleting SNMPv3 username with a "-" or "_" character does not delete the hexadecimal username from Cisco ISE.
<a href="#">CSCwe74135</a>	Cisco ISE Release ISE 3.1 Patch 5 : Guest portal removal failure : ORA-02292: integrity constraint.
<a href="#">CSCwf10773</a>	"no ip name-server" restarts services directly without prompt.
<a href="#">CSCvw81130</a>	Cisco ISE Release 2.7 - Unable to disable active directory diagnostic tool scheduled tests.
<a href="#">CSCwd34685</a>	Cisco ISE messaging service oscillating between "Not running" and "Initializing".
<a href="#">CSCwf30570</a>	Agentless script does not run if the computer is not on AC power.
<a href="#">CSCwf24158</a>	The 'terms and conditions' checkbox disappears when Portal Builder is used for Cisco ISE Release 3.0 and later releases.
<a href="#">CSCwf94289</a>	Cisco ISE Release 3.0 Patch 6: Policy export does not export policies.
<a href="#">CSCwa08802</a>	Cisco ISE Release 3.1 on AWS shows a false negative on the DNS check for health checks.
<a href="#">CSCwe15945</a>	Guest account cannot be seen by sponsors in a specific sponsor group.
<a href="#">CSCwf34391</a>	Cisco ISE Easyconnect stitching does not work if PassiveID happens before active authentication.
<a href="#">CSCwh42442</a>	Cisco ISE Release 3.2 Patch 3: CRL download failure.
<a href="#">CSCvy88380</a>	Unable to select Cisco ISE messaging usage (grayed out) for an existing certificate.
<a href="#">CSCwf21585</a>	Using potentially insecure methods - HTTP PUT method is accepted.
<a href="#">CSCwh14249</a>	There is a Cisco ISE 3.x spelling mistake in API gateway settings.
<a href="#">CSCwf09364</a>	User & endpoint identity groups description field is not editable for long text.
<a href="#">CSCwf47038</a>	Trash All or Selected at pxGrid policy should not touch entries for internal group.
<a href="#">CSCwh04251</a>	Cisco ISE agentless posture does not support a password containing the ":" character.
<a href="#">CSCvu56500</a>	Cisco ISE exports all network devices and gives an empty file.
<a href="#">CSCwf66237</a>	The Cisco ISE "Get All Endpoints" request takes time to execute since Cisco ISE Release 2.7.
<a href="#">CSCwf59058</a>	RBAC policy with custom permissions does not work when the administration menu is hidden.
<a href="#">CSCwd97984</a>	Meraki Sync Service does not run immediately after Cisco ISE application server restarts.

Caveat ID	Description
<a href="#">CSCwf66880</a>	Endpoint .csv file import displays "No file chosen" after selecting a file.
<a href="#">CSCwf26951</a>	Profiler CoA sent with the wrong session ID.
<a href="#">CSCwd17322</a>	Cisco ISE in AWS - health check input and output bandwidth performance and check false alarm.
<a href="#">CSCwe27438</a>	Launch page level help does not work with patch management, upgrade, and health checks.
<a href="#">CSCwf40265</a>	The Cisco ISE maximum session counter time limit does not work.
<a href="#">CSCwb18744</a>	SG and contracts with multiple backslash characters in a row in the description cannot sync with Cisco ISE.
<a href="#">CSCwh48026</a>	pxGrid direct-connector.log discrepancy between the actual clock and the time it prints the logs.
<a href="#">CSCwf37679</a>	Sponsor permissions are disabled on the sponsor portal when accessed from the primary PAN.
<a href="#">CSCwf96294</a>	Cisco ISE Release 3.0: Connection attempt to disallowed domains.
<a href="#">CSCwf23981</a>	Cisco ISE Authorization Profile shows the wrong Security Group and VN value.
<a href="#">CSCwf61939</a>	Using an apostrophe in the First Name and Last name fields presents an invalid name error.
<a href="#">CSCwd36753</a>	AnyConnect posture script does not run when the script condition name includes a period.
<a href="#">CSCwc36589</a>	Cisco ISE Intune MDM integration might be disrupted due to the End of Support for MAC address-based APIs from Intune.
<a href="#">CSCwh18731</a>	Upgrading to Cisco ISE Release 3.2 with LSD disabled before upgrade causes EP profiler exception.
<a href="#">CSCwc53824</a>	Cisco ISE limits connection to AMP AMQP service to TLSv1.0.
<a href="#">CSCwf36285</a>	Row of "Manage SXP Domain filters" only displays maximum 25.
<a href="#">CSCwf07855</a>	Cisco ISE SXP bindings API call returns 2xx response when the call fails.
<a href="#">CSCwf82055</a>	Unable to disable SHA1 for ports associated with passive ID agents.
<a href="#">CSCwf62744</a>	ENH: Add "Disable EDR Internet Check" tag.
<a href="#">CSCwh28098</a>	Cisco ISE Release 3.2 Patch 3: CoA Disconnect is sent instead of CoA Push during posture assessment with RSD disabled.
<a href="#">CSCwf14365</a>	"Configuration Missing" warning is seen on the Log Analytics page.
<a href="#">CSCwe82004</a>	TCP socket exhaustion.

Caveat ID	Description
<a href="#">CSCwe53550</a>	Cisco ISE and CVE-2023-24998.
<a href="#">CSCwf71870</a>	TACACS deployment with 0 days evaluation will not work after registering for smart licensing.
<a href="#">CSCwh46877</a>	Need CoA Port-Bounce while removing ANC Policy with PORT_BOUNCE.
<a href="#">CSCwf62987</a>	Vulnerabilities present in antisamy 1.5.9.
<a href="#">CSCwh32290</a>	There is a mismatch between the FQDN value in the GUI and CLI after performing reset-configuration.
<a href="#">CSCwf42496</a>	Attempting to delete "Is IPSEC Device" NDG causes all subsequent RADIUS/T+ authentications to fail.
<a href="#">CSCwc44622</a>	Session gets stuck indefinitely until it restarts when NAD (Meraki) misbehaves.
<a href="#">CSCwh51136</a>	Cisco ISE drops RADIUS request with the message "Request from a non-wireless device was dropped".
<a href="#">CSCwf33018</a>	A fix to the bug CSCwd35608 is causing CoA calls from UI to be sent to the wrong IP address.
<a href="#">CSCwf44942</a>	TACACS:PSN crashes during max user session authentication flow.
<a href="#">CSCwf19039</a>	Cisco ISE Release 3.1 Patch 5: Agentless posture failures cause /tmp/ folder to increase in size.
<a href="#">CSCwf31477</a>	Profiler triggers port bounce when multiple sessions exist on a switch port.
<a href="#">CSCwf55641</a>	German and Italian emails are not saved under Account Expiration Notification in Guest Types.
<a href="#">CSCwh28528</a>	TopN Device administration reports don't work when TACACS incoming messages exceed 40 million records per day.
<a href="#">CSCwe96739</a>	TLS 1.0 and TLS 1.1 accept Cisco ISE Release 3.0 admin portal.
<a href="#">CSCwe95624</a>	Cisco ISE Release 3.2 SNMP does not work after node restarts.
<a href="#">CSCwe03624</a>	Smart license registration fails with "communication send error" alarms intermittently.
<a href="#">CSCwf81550</a>	Cisco ISE changes the MAC address format according to the selected MAC address format even when it is unnecessary.
<a href="#">CSCwf54680</a>	Unable to edit or delete authorization profiles with parentheses in their names.
<a href="#">CSCwh38484</a>	Manually deleting the static route will cause Cisco ISE to send a packet with the wrong MAC in Cisco ISE Release 3.0 Patch 7.
<a href="#">CSCwf35760</a>	Ct_engine uses 100% CPU.
<a href="#">CSCwh39008</a>	Unable to schedule or edit the schedule for configuration backup.

Caveat ID	Description
<a href="#">CSCwf60904</a>	ANC remediation does not function with AnyConnect VPN.
<a href="#">CSCwh03227</a>	Cisco ISE does not use a license when authorized with no authorization profile rule.
<a href="#">CSCwf80951</a>	Unable to edit or create admin user due to "xwt.widget.repeater.DataRepeater" error.
<a href="#">CSCwe98676</a>	Vulnerable JavaScript library issue found while executing ZAP.
<a href="#">CSCwd20521</a>	Active Directory connector does not stop.
<a href="#">CSCwf59310</a>	Cisco ISE Release 3.1 Patch 7 : Context Visibility : pxGrid ContextIn : Missing Custom Attributes.
<a href="#">CSCwh05647</a>	Static IPv6 routes are removed after a reload in Cisco ISE Release 3.2.
<a href="#">CSCwh41693</a>	Cisco ISEaaS: AWS - Support IMDS v2 issue.
<a href="#">CSCwh00049</a>	Cisco ISE stored cross-site scripting vulnerability.

## Open Caveats in Cisco ISE Release 3.2 - Cumulative Patch 4

These are open caveats in Cisco ISE Release 3.2 - Cumulative Patch 4.

Caveat ID Number	Description
<a href="#">CSCwh92366</a>	In 3.1 Patch 8: Observing Insufficient Virtual Machine Resource Alarm in 3.1Patch 8 Longevity setup.

## New Features in Cisco ISE Release 3.2 - Cumulative Patch 3

### Link External LDAP Users to Cisco ISE Endpoint Groups

From Cisco ISE Release 3.2 Patch 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 3.2*.

### 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, although the process might take longer than a full upgrade.

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 3.2*.

### Ukrainian Language Support in Portals

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

## Resolved Caveats in Cisco ISE Release 3.2 - Cumulative Patch 3

Caveat ID	Description
<a href="#">CSCwe61215</a>	SFTP and FTP validation fails through CLI when password is configured with more than 16 characters.
<a href="#">CSCwfl5717</a>	ISE 3.2 - System 360 is not available only with Device Admin license.
<a href="#">CSCvr79992</a>	Session.CurrentDate attribute is not calculated correctly during authentication.
<a href="#">CSCwe68336</a>	Posture Assessment By Condition generates ORA-00904: "SYSTEM_NAME": invalid identifier.
<a href="#">CSCwe15315</a>	TrustSec PAC Information Field attribute values are lost when network device CSV template file is imported.
<a href="#">CSCwfl4957</a>	TrustSec status cannot be changed if using Japanese UI in ISE.
<a href="#">CSCwe69085</a>	PSN GUI is not accessible when only device administration license is enabled
<a href="#">CSCwd97022</a>	ISE-PIC 3.2 p3 Smart Licensing Disabled PIC Upgrade is out of compliance.
<a href="#">CSCwd46505</a>	ISE-PIC does not show Queue Link errors.
<a href="#">CSCwe24932</a>	Agentless posture fails when using multiple domain users in the endpoint login configuration.
<a href="#">CSCwe54318</a>	SXP service gets stuck into initializing due to H2 DB delay in querying bindings.
<a href="#">CSCvt62460</a>	Unable to retrieve groups or attributes from different LDAPs when defined per node.
<a href="#">CSCwe49261</a>	ISE PassiveID Agent probes the status of all domains even the ones without passiveID configuration.
<a href="#">CSCwd47111</a>	ISE is unable to save the subnet or IP address pool name for voice vlans.
<a href="#">CSCwd79277</a>	Sync status shows as failed when maximum trustsec objects are selected for sync.
<a href="#">CSCwf26973</a>	Network Device Group information is missing when admin account is Read-Only.
<a href="#">CSCwd97606</a>	Multiple requests for same IP+VN+VPN combinations with different session IDs creates duplicate records.
<a href="#">CSCwe07822</a>	ISE date of last purge has wrong timestamp.
<a href="#">CSCwd90613</a>	Radius Server Sequence page shows "no data available".
<a href="#">CSCwf28229</a>	VLAN detection interval should not be more than 30 seconds.
<a href="#">CSCwd12357</a>	SXP service gets stuck in initializing due to an exception on port 9644.
<a href="#">CSCwe59587</a>	Some items are displayed as [Test] in Japanese display.
<a href="#">CSCwe37978</a>	Scheduled report with huge size comes up as empty on the repository when exported.

Caveat ID	Description
<a href="#">CSCwe92640</a>	ISE 3.1 and 3.2 - Validation is missing for existing routes during CLI configuration.
<a href="#">CSCwe43002</a>	"Read-only Admin" is not available for ISE admin SAML authentication.
<a href="#">CSCwc93253</a>	ISE - Network device captcha prompts only when filter matches one network device.
<a href="#">CSCwe64558</a>	Admin account created from network access users cannot change dark mode setting.
<a href="#">CSCwf19463</a>	Conditions Studio drag and drop layering.
<a href="#">CSCwc64346</a>	ISE ERS SDK network device bulk request documentation is not correct.
<a href="#">CSCwe85828</a>	Trust store does not update admin certificate after generating new admin certificate.
<a href="#">CSCwc47015</a>	Fix for CSCvz85074 breaks AD group retrieval in ISE.
<a href="#">CSCwe52296</a>	ISE MNT Auth Status API query should be optimized.
<a href="#">CSCwf33128</a>	Radius used space reports incorrect usage as it also takes into account a few TACACS tables.
<a href="#">CSCwb83304</a>	ISE upgrade fails because of custom security group.
<a href="#">CSCwc47799</a>	ISE does not show any error when importing a certificate and private key when the password has % .
<a href="#">CSCwe11676</a>	Data lost when accessing Total Compromised Endpoints in Cisco ISE dashboard Threat for TC-NAC.
<a href="#">CSCwe41695</a>	ISE 3.1P4 and P5: Standalone ISE crashes if restarted after removing admin access restriction.
<a href="#">CSCwe80760</a>	Unable to save launch program remediation when the parameter contains double quote ("").
<a href="#">CSCwe17954</a>	Cisco Identity Services Engine Information Disclosure Vulnerability.
<a href="#">CSCwe70402</a>	ISE 3.2 cannot handle portal customization scripts that include single-line JavaScript comments.
<a href="#">CSCwf40128</a>	Accept client certificate without KU purpose validation as per CiscoSSL rules.
<a href="#">CSCwe52461</a>	Unable to enable the firewall condition in ISE 3.1.
<a href="#">CSCwe96633</a>	Support bundle does not contain terrors.log and times.log.
<a href="#">CSCwf22799</a>	Deferred Update condition does not work if compliance module is not compatible with Secure Client.
<a href="#">CSCwd39746</a>	For SCCM integration with ISE need MSAL support as MS is deprecating ADAL.
<a href="#">CSCwe97989</a>	ISE 3.2 crashes with VN in authorization profile.
<a href="#">CSCwe38800</a>	Vulnerabilities in hibernate-validator - multiple versions.

Caveat ID	Description
<a href="#">CSCwe49167</a>	ISE 3.2 SAML sign authentication request setting gets unchecked on being saved.
<a href="#">CSCwf33881</a>	ISE 3.2 P1 establishes connections to servers not listed in ISE ports or resources reference guides.
<a href="#">CSCwfl3630</a>	Mnt Log Processor service stops every night.
<a href="#">CSCwe12098</a>	ISE 3.2: Ports for Guest Portal configuration do not open on ISE nodes installed on AWS node.
<a href="#">CSCwe86793</a>	ISE filter of REST ID Store Groups displays: Error Processing this request.
<a href="#">CSCwe40577</a>	Failed to handle API resource request: Failed to convert condition.
<a href="#">CSCwe70975</a>	In ISE the SMS Javascript Customization does not work for SMS email gateway.
<a href="#">CSCwe69179</a>	ISE - latest IP access restriction configuration removes previous configuration.
<a href="#">CSCwf31073</a>	ISE 3.1 OpenAPI Error 400 when device admin network conditions are fetched.
<a href="#">CSCwf33421</a>	Update warning message while changing timezone.
<a href="#">CSCwe49422</a>	From ISE 3.2, clear text passwords must be entered in the identity-store command.
<a href="#">CSCwf09393</a>	ISE 3.1 services fail to start after restoring backup from old ISE vrsion 2.7.
<a href="#">CSCwe70197</a>	ISE Certificate API fails to return trusted certificate with hash character in friendly name.
<a href="#">CSCwfl5130</a>	Permission for collector.log file is set as root automatically.
<a href="#">CSCwe38610</a>	Make MDM API V3 certificate string case insensitive.
<a href="#">CSCwe57240</a>	GUI does not validate default value while adding custom attributes.
<a href="#">CSCwe55215</a>	ISE smart licensing now uses smart transport.
<a href="#">CSCwf05309</a>	ISE SAML certificate does not replicate to other nodes.
<a href="#">CSCwe83868</a>	Vulnerabilities in spring-framework 5.1.3.
<a href="#">CSCwf34596</a>	User Custom Attributes are stuck on rendering.
<a href="#">CSCwe78540</a>	IotAsset information is missing when Get All Endpoints is invoked.
<a href="#">CSCwe43468</a>	Static IP-SGT mapping with VN reference causes DNAC Group-Based Policy sync to fail.
<a href="#">CSCwe13859</a>	Unable to create Scheduled backup with admin user from "System Admin" AdminGroup.
<a href="#">CSCwf26226</a>	CPU spike due memory leak with EP purge call.
<a href="#">CSCwe20314</a>	ISE-PIC 3.1 : PIC License : Consumption 0.

Caveat ID	Description
<a href="#">CSCwf40861</a>	UI shows HTML hexadecimal code for the characters in the command set.
<a href="#">CSCwd55061</a>	ERS API internal error seen while creating existing NDG.
<a href="#">CSCwe86494</a>	ISE displays tomcat stacktrace when using a specific URL.
<a href="#">CSCwd41098</a>	Getting pxGrid error logs in ise-psc.log after disabling pxGrid.
<a href="#">CSCwe41824</a>	ISE 3.2 Missing S-PAN Key for PKI-based SFTP.
<a href="#">CSCwd82119</a>	EAP-TLS authentication with ECDSA certificates fails on ISE 3.1.
<a href="#">CSCwf26482</a>	REST AUTH services not running after upgrade from ISE 3.1 to version 3.2.
<a href="#">CSCwd05040</a>	Unable to import certificates on secondary node post registration to the deployment.
<a href="#">CSCwf10004</a>	ISE IP SGT static mapping is not sent to SXP domain on moving it to another mapping group.
<a href="#">CSCwe36242</a>	TACACS Command Accounting report export does not work.
<a href="#">CSCwc85867</a>	ISE Change Configuration Audit Report does not clearly indicate SGT create and delete events.
<a href="#">CSCwd70658</a>	Unable to add Network Access Device. Reason: "There is an overlapping IP Address in your device" .
<a href="#">CSCwe99961</a>	Sponsored Portal in Germany - Calendar shows Thursday (Donnerstag) as Di not Do.
<a href="#">CSCwf23981</a>	ISE Authorization Profile displays wrong Security Group and VN value.
<a href="#">CSCwd73282</a>	ISE 3.1 Patch 3 : Sponsor Portal : Session Cookie SameSite value set to none.
<a href="#">CSCwf09674</a>	Registered Endpoint Report shows unregistered guest devices.
<a href="#">CSCwc85546</a>	ISE 3.1 ENH "Illegal hex characters in escape (%) pattern ? for input string: ^F".
<a href="#">CSCwf17490</a>	Post SL update, ISE licensing page shows evaluation compliance status for consumed licenses.
<a href="#">CSCwe30235</a>	Vulnerabilities in jszip 3.0.0.
<a href="#">CSCwe84210</a>	Authorization policy evaluation fails due to NullPointerException in LicenseConsumptionUtil.java.
<a href="#">CSCwe69189</a>	LSD causes high bandwidth utilization.
<a href="#">CSCwb44638</a>	Enhancement: To have separate log file with MNT DB metrics.
<a href="#">CSCwd31414</a>	Guest portal displays "Error Loading Page" when reason for visit field contains special characters.
<a href="#">CSCwf21960</a>	During upgrade the deregister call fails to remove all the nodes from the database.



Caveat ID	Description
<a href="#">CSCwe18371</a>	Issues with ISE 3.2 admin access restriction.
<a href="#">CSCwe36063</a>	No validation of PBIS reg key configuration on advance tuning page.
<a href="#">CSCwe63873</a>	Qualys adapter is unable to download the knowledge base - Stuck in knowledge download in progress.
<a href="#">CSCwd97551</a>	ISE cannot retrieve OU attributes from client certificate in EAP-TLS session resumption.
<a href="#">CSCwc80574</a>	ISE AD Connector fails during join.
<a href="#">CSCwd68070</a>	Import saml metadata fails.
<a href="#">CSCvx15522</a>	DNSCache enabling command in FQDN syslog popup needs correction.
<a href="#">CSCwe37826</a>	Unable to change the condition operator from AND to OR in posture policy condition.
<a href="#">CSCwe71729</a>	ISE 3.2 : Data Connect password about to expired alarm every minute.
<a href="#">CSCwe57162</a>	Certificate based GUI admin login stuck.
<a href="#">CSCwe39262</a>	Passive D agent sends incorrect time format events.
<a href="#">CSCwd38136</a>	Cisco Identity Services Engine Denial of Service Vulnerability.
<a href="#">CSCwd54844</a>	ERS API schema for network device group creation.
<a href="#">CSCwe49183</a>	ISE SAML destination attribute is missing for signed authentication requests.
<a href="#">CSCwe36788</a>	ISE 3.2 Unable to delete the rules which are added during the time of adding IP access rule.
<a href="#">CSCvz86446</a>	ISE Replication: SyncRequest timeout monitor thread does not kill file transfer after timeout.
<a href="#">CSCwe12618</a>	ISE 3.2 : APIC Integration : com.cisco.cpm.apic.ConfImporter:521 - Failed to get EPs null.
<a href="#">CSCwe71804</a>	ISE 3.1 - Key attributes are missing in SessionCache when third party network device profile is in use.
<a href="#">CSCwe34566</a>	Authentication against ROPC identity store fails with RSA key generation error.
<a href="#">CSCwb79496</a>	WMI status shows progress after mapping from agent protocol to WMI protocol.
<a href="#">CSCwe49504</a>	Passwords with more than 16 characters are not supported in ISE 3.2 for identity-store configuration command.
<a href="#">CSCwe39781</a>	ISE does not remove SXP mapping when SGT is changed after CoA.
<a href="#">CSCwe30606</a>	Unable to download support bundle with size over 1GB from GUI.
<a href="#">CSCvv99093</a>	ISE nodes intermittently trigger Queue Link alarms : Cause=Timeout.

Caveat ID	Description
<a href="#">CSCwf16165</a>	NTP authentication key with more than 15 characters getting % ERROR: bad hashed key.
<a href="#">CSCwd89797</a>	Exception error messages observed when debug log level is enabled on meraki-connector.

## Open Caveats in Cisco ISE Release 3.2 - Cumulative Patch 3

These are open caveats in Cisco ISE Release 3.2 - Cumulative Patch 3.

Caveat ID Number	Description
<a href="#">CSCwf59005</a>	PEAP and EAP-TLS don't work on FIPS mode.
<a href="#">CSCwh92366</a>	In 3.1 Patch 8: Observing Insufficient Virtual Machine Resource Alarm in 3.1 Patch 8 Longevity setup.

## New Features in Cisco ISE, Release 3.2 - Cumulative Patch 2

### Bulk Update and Bulk Delete Support for Context-In API in pxGrid Cloud

From Cisco ISE Release 3.2 Patch 2, you have context-in API support in pxGrid Cloud for bulk updation and bulk deletion of endpoints. For more information, see the [Cisco pxGrid Cloud Onboarding Guide](#) and 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 3.2 Patch 2 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 3.2 Patch 2, 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 3.2*.

### Support for Cisco Secure Network Server 3700 Series Appliance

The Cisco Secure Network Server (SNS) 3700 series appliances are based on the Cisco Unified Computing System (Cisco UCS) C220 Rack Server and are configured specifically to support Cisco ISE. Cisco SNS 3700 series appliances are designed to deliver high performance and efficiency for a wide range of workloads.

The Cisco SNS 3700 series appliances are available in the following models:

- Cisco SNS 3715 (SNS-3715-K9)

- Cisco SNS 3755 (SNS-3755-K9)
- Cisco SNS 3795 (SNS-3795-K9)

Cisco SNS 3715 appliance is designed for small deployments. Cisco SNS 3755 and Cisco SNS 3795 appliances have several redundant components such as hard disks and power supplies and are suitable for larger deployments that require highly reliable system configurations.

For more information, see the [Cisco Secure Network Server 3700 Series Appliance Hardware Installation Guide](#).



**Note** Cisco ISE 3.2 patch 2 and later versions support Cisco SNS 3700 series appliances. You cannot rollback to Cisco ISE 3.2 after installing the first patch (Cisco ISE 3.2 patch 2 or later) on an SNS 3700 series appliance.



**Note** Cisco ISE 3.2 upgrade bundle has been replaced on the [Cisco ISE Software Download](#) site. You must use the new upgrade bundle (ise-upgradebundle-2.7.x-3.1.x-to-3.2.0.542b.SPA.x86\_64.tar.gz) to upgrade from Cisco ISE 3.1 to Cisco ISE 3.2 on SNS 3700 series appliances.

## Resolved Caveats in Cisco ISE Release 3.2 - Cumulative Patch 2

Identifier	Headline
<a href="#">CSCwe25138</a>	Could not create Identity User if the user custom attribute includes \$ or ++
<a href="#">CSCwd45783</a>	pxGrid session publishing stops when reintegrating FMC while P-PIC is down
<a href="#">CSCwd70902</a>	PRRT should be sending unfragmented messages to MnT if IMS is enabled to avoid merge
<a href="#">CSCwd92324</a>	ISE 3.2 ROPC basic serviceability improvements
<a href="#">CSCwd84055</a>	ISE 3.1 Azure AD Autodiscovery for MDM API V3 is incorrect
<a href="#">CSCwd41218</a>	Cisco Identity Services Engine Command Injection Vulnerability
<a href="#">CSCwd27865</a>	Configuration changed is not working when assigning an endpoint to a group
<a href="#">CSCwd39056</a>	ISE 3.1 P4 Passive DC configuration failing to save username correctly
<a href="#">CSCwc91917</a>	Can't add quotation character in TACACS authorization profile
<a href="#">CSCwc62716</a>	IndexRebuild.sql script ran over MnT
<a href="#">CSCwe18371</a>	Issues with ISE 3.2 Admin Access restriction
<a href="#">CSCwd63661</a>	Entering incorrect password on GUI shows end user agreement
<a href="#">CSCwd97353</a>	Automatic backup stops working after 3 - 5 days
<a href="#">CSCwd71574</a>	High CPU utilization when Agentless Posture is configured

Identifier	Headline
<a href="#">CSCwe27146</a>	ISE 3.2 Patch 1: Unable to Parse CLI Admin Username with '-' (hyphen/dash)
<a href="#">CSCwd26845</a>	APIC Integration missing fvIP subscription
<a href="#">CSCwc65821</a>	ERS API doesn't allow for use of minus character in "Network Device Group" name
<a href="#">CSCwc39302</a>	Interface status is showing UP even after shutdown
<a href="#">CSCwd63749</a>	AD Retrieve Groups shows a blank page when loading a huge number of AD groups (400+)
<a href="#">CSCwd71496</a>	ISE not deleting sessions from All SXP Mapping table
<a href="#">CSCwd92835</a>	Network Device Profile shows HTML code as name
<a href="#">CSCwe07406</a>	Error Loading Page error is shown when creating a guest account in the Self-Registered Guest portal
<a href="#">CSCwd79277</a>	Sync status shows as failed when maximum TrustSec objects selected for Sync
<a href="#">CSCwa52678</a>	GUI TCPDUMP gets stuck on Stop_In_Progress
<a href="#">CSCwe00424</a>	ISE- SQLException sent to the Collection Failure Alarm caused by NAS-Port-id length
<a href="#">CSCwe14808</a>	ISE fails to translate AD attribute of msRASSavedFramedIPAddress
<a href="#">CSCwd98296</a>	IP Addresses/Device Groups fields in Network Device Port Conditions page doesn't accept valid port strings
<a href="#">CSCwd57978</a>	All NADs are deleted when you filter network devices by IP and Location
<a href="#">CSCwe37041</a>	Internal CA Certificate Chain becomes invalid when original PPAN is removed
<a href="#">CSCwc64480</a>	ISE fails to establish a secure connection when a new certificate is imported for a portal using same subject and signed by an external CA (without CSR)
<a href="#">CSCwd22790</a>	URI not accepted as Group attribute or as Name in Assertion of attributes for SAML IdP in ISE 3.1/3.2
<a href="#">CSCvy69943</a>	Allow Guest Portal HTTP Requests containing Content-headers with {} characters
<a href="#">CSCwe07354</a>	Radius Token Server config accepts empty host IP for Secondary Server
<a href="#">CSCwd57071</a>	Self-reg portal does not support nodes FQDNs for the Approve/Deny links sent to the sponsors
<a href="#">CSCwd24286</a>	ISE not sending hostname attribute to DNAC
<a href="#">CSCwe44750</a>	Re-profiling result is not saved in Oracle and VCS DB after feed incremental update
<a href="#">CSCwc79321</a>	Unable to change the Identity source from internal to external RSA/RADIUS-token server
<a href="#">CSCwd74560</a>	PUT operation failing with payload via DNAC to ISE (ERS)

Identifier	Headline
<a href="#">CSCwe63320</a>	ISE displays mismatched information on "Get All Endpoints" report
<a href="#">CSCwc57294</a>	Duplicate Manager doesn't remove packet when there is an exception in reading config
<a href="#">CSCwe33360</a>	Anomalous behavior detection is not working as expected
<a href="#">CSCwd82134</a>	Incorrect SLR out of compliance error reported in ISE
<a href="#">CSCwe37018</a>	ISE-DNAC integration fails if there are invalid certificates in ISE Trusted Store
<a href="#">CSCwc48311</a>	ISE vPSN with IMS performance degrades by 30-40% compared to UDP syslog
<a href="#">CSCwe13780</a>	Unable to join node to AD by REST API if we configure a specific OU
<a href="#">CSCwd93002</a>	Getting Null System Error while editing the groups and adding Name in Assertion under SAML
<a href="#">CSCwd31524</a>	16-character passwords are not supported in ISE 3.2 for sftp configuration
<a href="#">CSCwe02315</a>	Online Page level Help IDs for meraki-connector pages in ISE GUI
<a href="#">CSCwd41651</a>	Vertical Scrollbar bug in ISE 3.1
<a href="#">CSCwd69072</a>	Session directory write failed alarm with Cisco NAD using "user defined" NAD profile
<a href="#">CSCwe15576</a>	Not able to configure KRON Job
<a href="#">CSCwc55529</a>	Authentication failed due to missing certificate private key
<a href="#">CSCwc07082</a>	"The phone number is invalid" error message seen when trying to import users from csv file
<a href="#">CSCwd87161</a>	Certificate based login asks for license file if only the Device Admin license is enabled
<a href="#">CSCwe34204</a>	ISE upgrade tab shows upgrade in progress after installing patch
<a href="#">CSCwe22934</a>	ISE Authentication latency from devices with no mac address
<a href="#">CSCwd63717</a>	PKI-enabled SFTP repositories not working in ISE 3.2
<a href="#">CSCwb85502</a>	CIAM: xstream 1.4.17
<a href="#">CSCwc99816</a>	ISE openAPI restore shows Completed_With_Success 25 minutes before CLI command "show restore status" does
<a href="#">CSCwe45245</a>	Smart license registration is not working properly
<a href="#">CSCwd51812</a>	When using certificate based authentication, attempt to access ISE GUI results in access permission error
<a href="#">CSCwe13110</a>	Configuration backup executed on Primary MnT node
<a href="#">CSCvg66764</a>	Session stitching support with ISE PIC agent

Identifier	Headline
<a href="#">CSCwd74898</a>	"Posture Configuration detection" alarms should be "INFO" level and reworded
<a href="#">CSCwd64649</a>	Cisco DNA Center integration issue due to multiple internal CA certificates
<a href="#">CSCwe13947</a>	OpenAPI for EP create/update should work same as ERS API in addition to providing more functionality
<a href="#">CSCwe57764</a>	MDM Connection to Microsoft SCCM fails after Windows DCOM Server Hardening for CVE-2021-26414
<a href="#">CSCvo61351</a>	Live session get stuck at "Authenticated" state
<a href="#">CSCwe74108</a>	Cisco AI Analytics doesn't work with Proxy configured as IP Address
<a href="#">CSCwd97582</a>	ISE 3.1p5 verifies CA certificate EKU leading to "unsupported certificate" error

## Open Caveats in Cisco ISE Release 3.2 - Cumulative Patch 2

These are open caveats in Cisco ISE Release 3.2 - Cumulative Patch 2.

Caveat ID Number	Description
<a href="#">CSCwf25955</a>	A match authorization profile with SGT, VN name, VLAN fields empty causes port to crash.
<a href="#">CSCwf40128</a>	Accept client certificate without KU purpose validation per CiscoSSL rules.
<a href="#">CSCwf02093</a>	In Cisco ISE Release 3.2, hyper-V installations have DHCP enabled.
<a href="#">CSCwe92640</a>	Cisco ISE Releases 3.1 and 3.2: Missing validation for existing routes during CLI configuration.
<a href="#">CSCwf32255</a>	No response received from SNMP server when the "snmp-server host" is configured in Cisco ISE Release 3.2 patch 2.
<a href="#">CSCwe95624</a>	In Cisco ISE Release 3.2, the SNMP is not working following a node restart.
<a href="#">CSCwe69179</a>	The latest IP access restriction configuration removes the previous configuration in Cisco ISE.
<a href="#">CSCwe36788</a>	In Cisco ISE Release 3.2, users are not able to delete the rules which were added during IP access rule addition.
<a href="#">CSCwe41695</a>	In Cisco ISE Releases 3.1 patches 4 and 5, a standalone Cisco ISE node is crashing if it is restarted after removing the admin access restriction.
<a href="#">CSCwf55795</a>	In Cisco ISE Release 3.2 Patch 1, the Cisco ISE GUI and CLI are inaccessible following a configuration restoration with ADE-OS.
<a href="#">CSCwd97551</a>	Cisco ISE cannot retrieve multiple attribute values from the client's certificate in EAP-TLS session.

Caveat ID Number	Description
<a href="#">CSCwh92366</a>	In 3.1 Patch 8: Observing Insufficient Virtual Machine Resource Alarm in 3.1Patch 8 Longevity setup.

## New Features in Cisco ISE, Release 3.2 - Cumulative Patch 1



**Note** The in-app Online Help does not contain information on the features and enhancements in Cisco ISE Release 3.2 Patch 1. For configuration information on the following new features and enhancements, see the [Cisco Identity Services Engine Administrator Guide, Release 3.2](#).

### Extended Support for Cisco Secure Client

Cisco ISE 3.2 Patch 1 supports both AnyConnect and Cisco Secure Client for Windows, macOS, and Linux operating systems. The following Cisco Secure Client versions are supported for these operating systems:

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

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



**Note** Cisco ISE 3.2 supports Cisco Secure Client only for Windows OS.

For more information, see the Chapter "[Compliance](#)" in the *Cisco Identity Services Engine Administrator Guide, Release 3.2*.

### Meraki Connector for Cisco ISE

Cisco ISE and cloud-based Cisco Meraki are TrustSec-enabled systems that are policy administration points for TrustSec policies. If you use both Cisco and Meraki network devices, you can connect one or more Cisco Meraki dashboards to Cisco ISE to replicate TrustSec policies and elements from Cisco ISE to the Cisco Meraki networks belonging to each organization.

For information on configuring Meraki Connectors, see "Connect Cisco Meraki Dashboards with Cisco ISE" in the Chapter "[Segmentation](#)" in the *Cisco Identity Services Engine Administrator Guide, Release 3.2*.

### pxGrid Cloud Support for Context-in

From Cisco ISE Release 3.2 Cumulative Patch 1, pxGrid support for context-in is available. pxGrid Cloud context-in support is provided through ERS and Open APIs. For more information, see the [pxGrid Cloud Onboarding Guide](#).

## Support for Cisco AI Analytics

Cisco ISE 3.2 patch 1 and later releases support Cisco AI Analytics. The Cisco AI Analytics agent queries the endpoints data from Cisco ISE and sends it to AI cloud at regular intervals. This data can be used to reduce the number of unknown endpoints in the network by providing AI-based endpoint groupings, automated custom profiling rules, and crowd-sourced endpoint labels.

For more information, see "Enable Cisco AI Analytics" in the Chapter "[Asset Visibility](#)" in the *Cisco ISE Administrator Guide, Release 3.2*.

## SGT Reservation using OpenAPI

From Cisco ISE 3.2 patch 1 onwards, SGT reservation through OpenAPI is supported. For more information, see *Cisco Identity Services Engine API Reference Guide*.

## Resolved Caveats in Cisco ISE Release 3.2 - Cumulative Patch 1

Caveat ID	Description
<a href="#">CSCwd13425</a>	Patch install from UI fails
<a href="#">CSCwc74531</a>	ISE hourly cron should cleanup the cached buffers instead of the 95% memory usage
<a href="#">CSCwc80243</a>	ISE TCPDUMP stuck at "COPY_REPO_FAILED" state when no repository is selected
<a href="#">CSCwc85920</a>	ISE TrustSec Logging - SGT create event is not logged to ise-psc.log file
<a href="#">CSCwc33751</a>	ISE 3.1 TFTP copy times out
<a href="#">CSCwc53895</a>	ISE 3.1 patch 3 SAML SSO doesn't work if active PSN is down
<a href="#">CSCwc65802</a>	Save button for SAML configuration grayed out
<a href="#">CSCwc99178</a>	Not able to add too many Authorization Profiles with active session alarm setting
<a href="#">CSCwd10997</a>	Node syncup fails to replicate wildcard certificate with the portal role
<a href="#">CSCwc69492</a>	Metaspace exhaustion causes crashes on ISE node
<a href="#">CSCwb62192</a>	Scheduled backup failure when ISE indexing engine backup failed
<a href="#">CSCwd05697</a>	Guest locations do not load in the ISE Guest Portal
<a href="#">CSCwc62415</a>	Cisco Identity Services Engine Unauthorized File Access Vulnerability
<a href="#">CSCwa37580</a>	ISE 3.0 NFS share stuck
<a href="#">CSCwb77915</a>	Toggle to enable/disable RSA PSS cipher based on policy under Allowed Protocols
<a href="#">CSCvv10712</a>	Sec_txnlog_master table should be truncated post 2 million record count
<a href="#">CSCwc62413</a>	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
<a href="#">CSCwc76720</a>	Error with SNMPv3 privacy password in ISE 3.1



Caveat ID	Description
<a href="#">CSCwd35608</a>	ISE is sending old Audit Session ID in reauthentication CoA after successful port-bounce CoA
<a href="#">CSCwc62419</a>	Cisco Identity Services Engine Insufficient Access Control Vulnerability
<a href="#">CSCwc44580</a>	ISE 3.1 creates cni-podman0 interface with IP 10.88.0.1 and ip route for 10.88.0.0/16
<a href="#">CSCwc61320</a>	Slowness in the Support Bundle page due to Download Logs page loading in the background
<a href="#">CSCwc98833</a>	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
<a href="#">CSCwc98831</a>	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability
<a href="#">CSCwc95878</a>	Intermittent issues with App activation or App not receiving events
<a href="#">CSCwd13555</a>	ISE abruptly stops consuming passive-id session from a third party Syslog server
<a href="#">CSCwd32591</a>	ISE 3.2 SFTP repositories not operational from GUI after clicking "generate key pairs"
<a href="#">CSCwd51409</a>	ISE cannot retrieve repositories and scan policies of Tenable Security Center
<a href="#">CSCwd24304</a>	ISE 3.2 ERS POST /ers/config/networkdevicegroup fails due to broken attribute othername/type/ndgtype
<a href="#">CSCwd03009</a>	RMQForwarder thread to control based on hardware Appliance in platform.properties
<a href="#">CSCwc81729</a>	"All devices were successfully deleted" message displayed while trying to delete a NAD by filtering
<a href="#">CSCwb16640</a>	ISE 3.2 Authorization Profile does not persist VLAN name string for SDA SG-VN-VLAN use case
<a href="#">CSCwc42712</a>	ISE RADIUS and PassiveID session merging
<a href="#">CSCwd15888</a>	Not able to access Time Settings Configuration Export on ERS API
<a href="#">CSCwc15013</a>	Add serviceability and fix "Could not get a resource since the pool is exhausted" error in ISE 3.0
<a href="#">CSCwc87670</a>	ISE 3.1 patch 3 unable to import endpoints from csv file if SAML is used
<a href="#">CSCwa55233</a>	"Unknown CA" Queue Link error when using third-party signed certificate for IMS
<a href="#">CSCwd73787</a>	CLI password change doesn't persist in Confd DB after "password" command
<a href="#">CSCwd42311</a>	Unable to download rest-id-store from Download Logs on GUI
<a href="#">CSCwc50392</a>	ROPC AD groups retrieval is not working with 53k and above groups
<a href="#">CSCwc50944</a>	The change of profiling policy name is not reflected in the policy set conditions
<a href="#">CSCwc95075</a>	"File path field must contain a valid file name" error when configuring file conditions for posture.

Caveat ID	Description
<a href="#">CSCwc75572</a>	PPAN application server stuck at initializing state
<a href="#">CSCwd22790</a>	ISE 3.2 can't save Group Membership attribute for SAML service provider
<a href="#">CSCwd27506</a>	ISE 3.0 patch 6 missing scheduled reports
<a href="#">CSCwc74206</a>	ISE 3.0 not saving SCCM MDM server object with new password, works when new instance is used
<a href="#">CSCwd31405</a>	Latency observed during query of Session.PostureStatus
<a href="#">CSCwd45843</a>	Authentication step latency for policy evaluation due to GC activity
<a href="#">CSCwc60997</a>	SAML flow with load balancer is failing due to incorrect token handling
<a href="#">CSCwc49580</a>	ANC CoA is sent to the NAS IP address instead of the Device IP address
<a href="#">CSCwb26965</a>	Getting error while creating network device groups via REST API
<a href="#">CSCwc23593</a>	LSD is causing high CPU usage
<a href="#">CSCwc48509</a>	Windows Server 2022 is actually working as the target domain controller to be monitored
<a href="#">CSCwb72948</a>	ISE 3.0 patch 4 unable to access system certificates page for the registered node
<a href="#">CSCwc93451</a>	Profiler should ignore non-positive RADIUS syslog messages for forwarding from default RADIUS probe
<a href="#">CSCwc98828</a>	Cisco Identity Services Engine Interface Feature Insufficient Access Control Vulnerability
<a href="#">CSCwd24089</a>	ISE 3.2 Safe mode not enabled
<a href="#">CSCwd16837</a>	ISE openAPI HTTP repo patch install fails when dir listing is disabled
<a href="#">CSCwd31137</a>	ISE scheduled radius authentication reports failed while exporting to SFTP repository
<a href="#">CSCwc98824</a>	Posture Requirements only show the default entry
<a href="#">CSCwd30994</a>	Static default route with gateway of interfaces other than Gig 0 breaks network connectivity
<a href="#">CSCwc98823</a>	Cisco Identity Services Engine Command Injection Vulnerability
<a href="#">CSCwd41773</a>	Application server crashes if CRL of size 5 MB or more is downloaded frequently
<a href="#">CSCwc88848</a>	ISE 3.1 patch 1 does not create Rest ID/ROPC folder logs

## Open Caveats in Cisco ISE Release 3.2 - Cumulative Patch 1

Caveat ID	Description
<a href="#">CSCwd79277</a>	Sync status shows as failed when maximum TrustSec objects are selected for sync.
<a href="#">CSCwd89797</a>	Exception error messages seen when Debug log level is enabled on meraki-connector.
<a href="#">CSCwd93002</a>	System Error : Null while editing the groups and adding Name in Assertion under SAML.
<a href="#">CSCwd93209</a>	Sync Cycle does not end when meraki-connection is deleted from ISE.
<a href="#">CSCwe02315</a>	Page level online help for Meraki Connector is not available.
<a href="#">CSCwe01771</a>	Dashboards created using the changed Time fields:acs_timestamp would not show up after patch install.
<a href="#">CSCwh92366</a>	In 3.1 Patch 8: Observing Insufficient Virtual Machine Resource Alarm in 3.1Patch 8 Longevity setup.

## Known Limitations in Cisco ISE Release 3.2 - Cumulative Patch 1

### Custom Log Analytics Dashboards are not Displayed After Patch Install

Custom Log Analytics dashboards that are created in Cisco ISE Release 3.2 are not displayed after you install Cisco ISE Release 3.2 Patch 1. To view those dashboards, you must export all the custom dashboards from Kibana (as json files) before upgrading to Cisco ISE 3.2 patch 1, and import those dashboards on the MnT node after installing Cisco ISE 3.2 patch 1.

These dashboards will not be displayed even if you restore Cisco ISE 3.2 operational backup on an Cisco ISE 3.2 patch 1 node. As mentioned earlier, you must export the dashboards from Kibana and import them after patch install.

After installing Cisco ISE 3.2 patch 1, the Log Analytics dashboards with visualization created using the following attributes might show an error:

- acs\_timestamp
- acsview\_timestamp (for all indices except TACACS)
- generated\_time for TACACS indices
- IP address field in all indices

Do the following to fix this error:

- Replace acs\_timestamp with logged\_at\_timezone
- Replace acsview\_timestamp with logged\_at
- Replace generated\_time with logged\_at\_timezone
- Consider ipaddress as a text field

## Cisco ISE 3.2 Files Replaced on Software Download Site

Cisco ISE 3.2 OVA, ISO, and upgrade bundle files have been replaced on the [Cisco ISE Software Download](#) site.

### What Changes Are Made?

The following bug is resolved in this build:

- [CSCwd13425](#): Patch installation on the ISE 3.2 GUI fails.



**Note** The filenames of the new files have "a" appended to the build number (for example, ise-3.2.0.542a.SPA.x86\_64.iso).

## Open Caveats in Cisco ISE Release 3.2

The following table lists the open caveats in Release 3.2

Caveat ID	Description
<a href="#">CSCwc75986</a>	The endpoint debug report in Cisco ISE Release 3.2 shows the error "No Data Available".
<a href="#">CSCwb16640</a>	In Cisco ISE Release 3.2, the authorization profile does not persist with the VLAN name string for SDA SG-VN-VLAN use case.
<a href="#">CSCwc54812</a>	Upgrade preparation results in a thread dump due to a high load.
<a href="#">CSCwc73330</a>	The last name of the internal user is not added properly while creating a user in Cisco ISE Release 3.2.
<a href="#">CSCwc83059</a>	After a full upgrade, the VCS information is missing.
<a href="#">CSCwc41697</a>	Legacy split upgrade fails on PSN from when upgrading from Cisco ISE Release 3.1 Patch 3 to Cisco ISE Release 3.2.0.483 after the secondary PAN upgrade.
<a href="#">CSCwc74251</a>	PRRT - A Response signature verification failure issue occurs for pxGrid clients when performing an OCSP check.
<a href="#">CSCwe99609</a>	Timestamps need readjustment whenever the timezone is changed.
<a href="#">CSCwe99666</a>	Live logs and live sessions pages are displayed in an incorrect sorting order when the timezone is changed on the PSN and MnT nodes.
<a href="#">CSCwe99706</a>	Session data is shown at the bottom when PSNs are in different timezones.
<a href="#">CSCwh18731</a>	An upgrade to Cisco ISE Release 3.2 with LSD disabled prior to the upgrade causes an EP profiler exception.
<a href="#">CSCwh36667</a>	Cisco ISE Monitoring GUI page is stuck at "Welcome to Grafana".
<a href="#">CSCwh92366</a>	In 3.1 Patch 8: Observing Insufficient Virtual Machine Resource Alarm in 3.1 Patch 8 Longevity setup.

## Resolved Caveats in Cisco ISE Release 3.2

Bug ID	Reason
<a href="#">CSCwd13425</a>	Patch install from the Cisco ISE GUI fails.
<a href="#">CSCvz91603</a>	Unable to fetch the attributes from ODBC after upgrading Cisco ISE to Cisco ISE Release 3.0 patch 3.
<a href="#">CSCvy75191</a>	Cisco ISE XML external entity injection vulnerability.
<a href="#">CSCvz55293</a>	The secondary administrative Cisco ISE node is causing services to restart on the primary administration node. This causes a mismatch in the documentation.
<a href="#">CSCvq53373</a>	/ers/config/<obj>/bulk/submit returning invalid Location URI /ers/config/<obj>/bulk/submit/<bulkID>;
<a href="#">CSCvz87476</a>	Unsupported message code 91104 and 91105 alarms.
<a href="#">CSCwa12273</a>	AD users in Super Admin group can't create or edit admin user. The error "Operation is not permitted" is displayed.
<a href="#">CSCvz66279</a>	RADIUS reports older than 7 days are empty (regression of CSCvw78289).
<a href="#">CSCvz37623</a>	NTP (' - ') source state description missing in Cisco ISE CLI.
<a href="#">CSCwa25539</a>	Vulnerability assessment for CVE-2021-35599 on Oracle DB.
<a href="#">CSCwc12303</a>	PGA memory used by the instance exceeds PGA_AGGREGATE_LIMIT on the monitoring node.
<a href="#">CSCwc33751</a>	Cisco ISE Release 3.1 TFTP copy times out.
<a href="#">CSCwb29357</a>	Cisco ISE AD User SamAccountName parameter is null for user sessions.
<a href="#">CSCvw09460</a>	Updated fields list for PUT on /erc/config/authorizationprofile/{id} usually empty.
<a href="#">CSCvx48922</a>	Memory leak on TACACS flow.
<a href="#">CSCvz85074</a>	Fix for CSCvu35802 breaks AD group retrieval with certificate attribute as identity in EAP-chaining.
<a href="#">CSCwb64656</a>	When the Essential license is disabled on the Cisco ISE GUI, smart licensing portal is not reporting license consumption.
<a href="#">CSCwa07580</a>	Could not create Identity User if username includes \$.
<a href="#">CSCwa56934</a>	Inconsistent sorting on Cisco ISE ERS API(s) for endpoint group.
<a href="#">CSCwb55232</a>	Create a nested endpoint group using Cisco ISE ERS API.
<a href="#">CSCwb77915</a>	Toggle to enable/disable RSA PSS cipher based on policy under Allowed Protocols.
<a href="#">CSCvz85117</a>	Cisco ISE Health Check I/O bandwidth performance check false alarm.

Bug ID	Reason
<a href="#">CSCwb29140</a>	Threads getting exhausted post moving to the latest patches where the nss rpm is updated.
<a href="#">CSCwb59357</a>	Cisco ISE ova ztp attempts HTTP directs listing of contents.
<a href="#">CSCvz18848</a>	Agentless posture breaks for locale.
<a href="#">CSCwb82814</a>	Cisco ISE Release 3.1 OpenAPI giving a 400 error when fetching Nested Conditions.
<a href="#">CSCwa61347</a>	Cisco ISE-PIC not forwarding live sessions beginning with special characters.
<a href="#">CSCvz13747</a>	SystemTest: Cisco ISE primary administration node GUI page not opening after PAN failover.
<a href="#">CSCvz66577</a>	SMS Javascript customization is not working for SMS email gateway.
<a href="#">CSCvy81435</a>	Cisco ISE Guest SAML authentication fails with "Access rights validated" HTML page.
<a href="#">CSCwb23853</a>	Unable to add SAML ID provider on Cisco ISE 3.1 patch 1 when doing a configuration restore from an older Cisco ISE release.
<a href="#">CSCvy99582</a>	When upgrading from Cisco ISE Release 2.4 patch 13 to Cisco ISE 2.7 if external RADIUS server configuration upgrade will fail.
<a href="#">CSCwa96229</a>	Cisco ISE is allowing user to change admin password without validating the current password.
<a href="#">CSCwb36849</a>	Cisco ISE must avoid sending empty Cisco AV-Pairs in access-accept packets.
<a href="#">CSCwa20152</a>	CoA was not initiated on Cisco ISE for switches for which matrix wasn't changed, hence the policy sync failed.
<a href="#">CSCvy94553</a>	TACACS authentication report shows duplicate entries.
<a href="#">CSCvv54351</a>	Device administration using RADIUS does not consume base license.
<a href="#">CSCvz50059</a>	Cisco ISE GC_APP Logs are not auto-rotating or deleting from the local disk.
<a href="#">CSCwc99178</a>	Unable to add many authorization profiles with active session alarm setting.
<a href="#">CSCvu21809</a>	TEAP (EAP-TLS) with EAP-chaining is not using the configured CN for AD lookups.
<a href="#">CSCvz79665</a>	Microsoft Intune graph URL change from graph.windows.net/tenant to graph.microsoft.com.
<a href="#">CSCwc39320</a>	Upgraded Cisco ISE nodes via CLI method gets stuck in "Upgrading" status on the primary administration node GUI.
<a href="#">CSCwa35293</a>	Cisco ISE 2.7: Authentication success settings shows success/success URL.
<a href="#">CSCwb92006</a>	Having single quote in middle of the password on proxy settings causes page to become un-editable.

Bug ID	Reason
<a href="#">CSCvz88188</a>	TACACS authorization policy querying for username fails because username from session cache is null.
<a href="#">CSCwc50944</a>	The change of profiling policy name is not reflected on the policy set conditions automatically.
<a href="#">CSCvw58039</a>	Cisco ISE does not show report for client provisioning when AC is updated on the endpoint through Cisco ISE.
<a href="#">CSCwb33727</a>	Cisco ISE 3.1: Special character in attributes not supported.
<a href="#">CSCwa26210</a>	The next page field is missing from the JSON response of API 'GET /ers/config/radiusserversequence'.
<a href="#">CSCwc18751</a>	Unable to download a created support bundle from the Cisco ISE GUI if we login using format DomainName\UserName.
<a href="#">CSCwb24002</a>	The authentication settings of the Cisco ISE ERS SDK is not disabled via API call.
<a href="#">CSCwa88845</a>	Device port network conditions does not validate interface ID.
<a href="#">CSCvy66496</a>	REST ID cannot filter groups based on name or SID for Azure AD groups.
<a href="#">CSCwa94984</a>	Cisco ISE API add user operation with long custom attribute string takes 4min using Curl
<a href="#">CSCvz44655</a>	Cisco ISE manage account selection issue.
<a href="#">CSCwb56878</a>	The Replication Stopped alarm is triggered in Cisco ISE.
<a href="#">CSCvz77905</a>	Cisco ISE RADIUS service denial of service vulnerability.
<a href="#">CSCwa11653</a>	CIAM: linux-kernel 4.18.0.
<a href="#">CSCwa78479</a>	Cisco Identity Services Engine Assessment of CVE-2021-4034 Polkit
<a href="#">CSCwa20354</a>	Operational data purging and database utilization node information does not show intermittently.
<a href="#">CSCvv87286</a>	Fail to import Internal CA and key from Cisco ISE Release 2.7 Patch 2 to Cisco ISE Release 3.0.
<a href="#">CSCvz08813</a>	Unable to scroll to different pages in the Issued Certificates page.
<a href="#">CSCvz07191</a>	Cisco ISE GUI is stuck at loading if the AD group does not exist when using certificate based authentication for Cisco GUI access.
<a href="#">CSCwb92643</a>	Cisco ISE ADE-OS CLI TCP params fail to make changes and are no longer relevant.
<a href="#">CSCvz28133</a>	User unable to generate support bundle.
<a href="#">CSCwa55996</a>	New objects do not exist in the conditions studio.
<a href="#">CSCwc09435</a>	Error handling or messaging for the mobile number format is not clear.

Bug ID	Reason
<a href="#">CSCvx59893</a>	Inconsistency between Cisco ISE syslog level and message level.
<a href="#">CSCwa16401</a>	Get-By-ID server sequence, returns empty server list after first change made on the sequence via Cisco ISE GUI.
<a href="#">CSCwc40959</a>	In dark mode of Cisco ISE Release 3.2, the Internal Users have a color that is difficult to read.
<a href="#">CSCwc26241</a>	Cisco ISE Release 3.2 displays the error: "TypeError: Cannot read properties of undefined (reading 'attr')".
<a href="#">CSCwa48465</a>	Reports are unusable due to mishandling fields with multiple values.
<a href="#">CSCwb01843</a>	DST/TZ update should happen automatically.
<a href="#">CSCvx54894</a>	Sponsor Portal admin unable to create random guest accounts for 60 minutes or 1 hour duration or less.
<a href="#">CSCwb75964</a>	Cisco ISE Release 3.0: Unable to edit primary administration node auto failover alarms.
<a href="#">CSCwb32244</a>	No possibility to edit certificate imported to Cisco ISE Trusted Certificate.
<a href="#">CSCwa89443</a>	Cisco DNA Center - Cisco ISE Integration: Cisco ISE shows an old Cisco DNA Center certificate for pxGrid endpoint.
<a href="#">CSCvz27791</a>	Cisco ISE: Application server stuck initializing after backup restore due to MDM configuration.
<a href="#">CSCwa14268</a>	Vulnerability assessment for CVE-2021-35619 on Oracle DB.
<a href="#">CSCwa97123</a>	NTP sync failure alarms with more than 2 NTP servers configured.
<a href="#">CSCvy51210</a>	Cisco ISE Release 2.7 should display an error when attempting to delete the IP default label of network access devices on Cisco ISE GUI.
<a href="#">CSCvz37241</a>	Move queue link error from WARN to Critical and Restart if there is a timeout.
<a href="#">CSCwa40040</a>	Session Directory Write failed, SQLException: String Data right truncation on Cisco ISE 3.0 Patch 4.
<a href="#">CSCvy53842</a>	Certificate validation syslog message sent during specific certificate audits in Cisco ISE.
<a href="#">CSCvz01485</a>	In Cisco ISE 2.7 patch 4, users are unable to upload .json file for Umbrella security profile.
<a href="#">CSCwc23997</a>	Cisco ISE is showing incorrect VLAN assignment information in authorization profile and attributes details.
<a href="#">CSCwb95433</a>	"File path field must contain a valid file name" error when configuring file conditions for posture.
<a href="#">CSCvz78841</a>	CIAM: openssh 7.6.



Bug ID	Reason
<a href="#">CSCvz90468</a>	Internal users using external password store are getting disabled if we create users using API flow.
<a href="#">CSCwa06912</a>	High latency observed for TACACS+ requests with date and time condition in authorization policies.
<a href="#">CSCwb01568</a>	Cisco ISE on AWS: Operational DB not sized properly based on a larger OS disk.
<a href="#">CSCvy76328</a>	IPV6 changes the Subnet to /128 when using the duplicate option from Network device tab.
<a href="#">CSCvz56358</a>	Cisco ISE Release 3.0 checks only the first SAN entry.
<a href="#">CSCwc85920</a>	Cisco ISE TrustSec Logging - SGT create event is not logged to ise-psc.log file.
<a href="#">CSCwc61320</a>	Slowness on support bundle page due to the Download Logs page loading in the background.
<a href="#">CSCvw93570</a>	Cisco ISE Release 2.4 patch 8 is unable to edit, duplicate or delete guest portals.
<a href="#">CSCwa20309</a>	Unknown NAD and misconfigured network device detected alarms.
<a href="#">CSCwc21890</a>	Passive easy connect does not work in Cisco ISE with dedicated monitoring nodes.
<a href="#">CSCwb29498</a>	High operations DB usage alarm percentage need to be configurable.
<a href="#">CSCwc69492</a>	Cisco ISE 3.1: Metaspace exhaustion causes crashes on Cisco ISE node.
<a href="#">CSCwb48707</a>	Unable to load the Endpoint Purge tab.
<a href="#">CSCvz44488</a>	Cisco ISE 3.0 geantless posture does not use domain authentication if same local user exists.
<a href="#">CSCvt25277</a>	Cisco ISE 2.4 patch 12 install is stuck.
<a href="#">CSCvz68091</a>	Configuration changes to guest types is not updated in audit reports.
<a href="#">CSCwa32312</a>	RCM and MDM flows getting failed because of session cache not populated.
<a href="#">CSCwa37040</a>	Backup-logs using public key encryption on the Cisco ISE CLI does not allow for capture of core files.
<a href="#">CSCwb61614</a>	Guest users (AD or internal) cannot delete or add their own devices on specific node.
<a href="#">CSCvs95495</a>	Reauthorization issue in Aruba third party device.
<a href="#">CSCwb27894</a>	EAP-TEAP with EAP-TLS unable to match condition that has "CERTIFICATE.Issuer - Common Name".
<a href="#">CSCvz49871</a>	Cisco ISE GUI: net::ERR_ABORTED 404: /admin/ng/nls/fr-fr/.
<a href="#">CSCwa33462</a>	CSV NAD import is rejected due to special symbol @ at the beginning of RADIUS shared secret.

Bug ID	Reason
<a href="#">CSCwc44580</a>	Cisco ISE 3.1 creates cni-podman0 interface with IP 10.88.0.1 and IP route for 10.88.0.0/16.
<a href="#">CSCvx23375</a>	Cisco ISE authorization profiles option get truncated during editing or saving (in Google Chrome only).
<a href="#">CSCwb41741</a>	Cisco ISE - Invalid character error in Admin Groups.
<a href="#">CSCwb27857</a>	Cisco ISE Release 3.0 Patch 5: Unable to login into the Cisco ISE GUI of MnT nodes using RSA 2FA in distributed deployment.
<a href="#">CSCwa09060</a>	Unable to assign the role to externally signed system cert binded by CSR in Cisco ISE 3.1 Patch 1.
<a href="#">CSCvz72225</a>	Adding FQDN in discovery host- Discovery host: invalid IP address or host name.
<a href="#">CSCwa13696</a>	Cisco ISE Release 3.1 Guest Username or Password Policy is not modifiable.
<a href="#">CSCwb39638</a>	Unable to import Network Device configured with SNMPv3 SHA2 authorization.
<a href="#">CSCwa23207</a>	Multiple runtime crashes seen due to memory allocation inconsistency.
<a href="#">CSCwb52396</a>	Cisco ISE PRA failover.
<a href="#">CSCvy94511</a>	TACACS report showing duplicate entries due to EPOCH time being null.
<a href="#">CSCvz77482</a>	Cisco ISE Release 3.0 can't deselect the 'location' settings as part of the guest self registration portal.
<a href="#">CSCwb59170</a>	Cisco ISE Release 3.1 SHA-2 option is not available for NAD creation via REST API.
<a href="#">CSCwc62415</a>	Cisco Identity Services Engine Unauthorized File Access Vulnerability.
<a href="#">CSCwc76720</a>	Error with SNMPv3 Privacy Password on Cisco ISE Release 3.1 only.
<a href="#">CSCwb42924</a>	Unable to get message option in Posture remediation actions.
<a href="#">CSCwb35304</a>	Cisco ISE Release 3.1: Race condition causes registration/sync failure.
<a href="#">CSCwa47190</a>	AD security groups cannot have their OU end with dot character on Posture Policy.
<a href="#">CSCvz57222</a>	Cisco ISE Release 3.0: Admin access is allowed for Cisco ISE GUI with secondary interfaces GigabitEthernet 1 and Bond 1.
<a href="#">CSCwb52092</a>	AWS Cloud Formation stack for Cisco ISE Release 3.1 fails with very strong admin password.
<a href="#">CSCwa18443</a>	Need to handle Posture expiry when 8 octet MAC is present in endpoint on the deployment node.
<a href="#">CSCwa83517</a>	Guest portal registration page gives "error loading page" when email address contains apostrophe.

Bug ID	Reason
<a href="#">CSCvi35653</a>	Bi-directional communication/UDP heart-beat between Cisco ISE and AnyConnect Cisco ISE Posture.
<a href="#">CSCwb19256</a>	Pingnode call causing app server to crash (OOM exception) during CRL validation.
<a href="#">CSCwc31482</a>	NetworkSetupAssistance.exe digital signature certificate expired in BYOD flow using Windows SPW.
<a href="#">CSCwa57955</a>	Posture firewall remediation action unchangeable.
<a href="#">CSCwb48388</a>	Licensing only displays one reserved count if licenses reserved in CSSM have multiple expiry dates.
<a href="#">CSCwa25731</a>	Last 7 days filter not working in Reports.
<a href="#">CSCwb97579</a>	Cisco ISE Release 3.1 compatibility problems with Hyper-V Gen-2.
<a href="#">CSCwc74206</a>	Cisco ISE Release 3.0 not saving SCCM MDM server object with new password, works when new instance is use.
<a href="#">CSCvy33393</a>	Cisco ISE 3.1 BH Context visibility shows \\ in username where as live logs show correct single \.
<a href="#">CSCwb26965</a>	Cisco ISE Release 3.1: Getting error while creating network device groups via REST API.
<a href="#">CSCvz18627</a>	PEAP session timeout value restricted to max 604800.
<a href="#">CSCwa78042</a>	Cisco ISE Release 3.1 is requesting ISE-PIC licenses from smart account.
<a href="#">CSCwa91335</a>	Default domain configuration in Passive-Syslog provider does not work in Cisco ISE Release 3.1.
<a href="#">CSCvz73445</a>	Agentless Posture not passing AntiMalware check.
<a href="#">CSCvz63643</a>	Cisco ISE Release 2.7: EndpointPersister thread getting stopped.
<a href="#">CSCwb21669</a>	Unable to enter IPV6 address for on-prem SSM server.
<a href="#">CSCwa17470</a>	Cisco ISE Release 3.1 SAML admin authentication failing with Access Denied if 2+ groups in the group claim.
<a href="#">CSCwa49859</a>	Attribute value dc-opaque causing issues with Live Logs.
<a href="#">CSCvz72034</a>	Cisco ISE Release 3.1: When updating network device from Cisco DNA Center shared secret/password is empty or masked.
<a href="#">CSCvz83204</a>	Cisco ISE unable to fetch the URL attribute value from improper index during posture flow.
<a href="#">CSCwc53577</a>	Parent user identity group can be created via CSV file.
<a href="#">CSCwb71505</a>	Cisco ISE Release 3.1: Application server stuck in initializing state due to ACE library error.

Bug ID	Reason
<a href="#">CSCvz74457</a>	Cisco ISE ERS API doesn't allow for use of dot character in "Network Device Group" name or create or update.
<a href="#">CSCwc07283</a>	Context visibility endpoint authentication tab is not showing data in Cisco ISE Release 3.1.
<a href="#">CSCvy94427</a>	Posture lease breaks for EAP chaining from Cisco ISE Release 2.7.
<a href="#">CSCvy71690</a>	Customer fields in the guest portal contains & - \$ #.
<a href="#">CSCwa95889</a>	Cisco ISE: SSH/SFTP to Hosts w/ Newer HostKey algorithms (e.g. rsa-sha2-512).
<a href="#">CSCvy91805</a>	Maximum sessions are not being enforced with EAP-FAST-Chaining in Cisco ISE.
<a href="#">CSCwd05697</a>	Guest locations do not load in Cisco ISE Guest Portal.
<a href="#">CSCwc88848</a>	Cisco ISE Release 3.1 Patch 1 does not create the Rest ID/ROPC folder logs.
<a href="#">CSCvy69539</a>	CIAM: openjdk - multiple versions.
<a href="#">CSCwb34910</a>	Multi-line issues for Guest SMS notification under Cisco ISE portal.
<a href="#">CSCvy92536</a>	Cisco ISE Release 3.0: Device Admin license alone should allow access to Administration > System > Logging menu.
<a href="#">CSCwb02129</a>	SSH to Cisco ISE failing on any SSH public keys manually imported.
<a href="#">CSCwb32466</a>	Cisco ISE Release 3.1: Unable to delete endpoint identity group created via REST API when setting no description.
<a href="#">CSCvy86859</a>	Mac OS Beta Monterey (MacOS 12 beta 2) failing NSP MacOSXSPWizard v3.1.0.2.
<a href="#">CSCwa04454</a>	Cisco ISE Releases 3.0 & 3.1: Device Admin License alone should allow access to all TACACS required menus.
<a href="#">CSCwc08484</a>	Disabling Open TAC case leads to Cisco ISE Integrity Check failure on Cisco ISE service restart.
<a href="#">CSCvz07823</a>	Cisco ISE Release 2.7 failed to add endpoint to group.
<a href="#">CSCwc49580</a>	ANC COA is sent to the NAS IP address instead of the Device IP address.
<a href="#">CSCwc87670</a>	Cisco ISE Release 3.1 patch 3 is unable to import endpoints from .csv file if SAML is used.
<a href="#">CSCwd31405</a>	Latency observed during query of Session.PostureStatus.
<a href="#">CSCwb30941</a>	CVE-2022-0778 - Cisco ISE Release 3.1 and above is affected.
<a href="#">CSCwb85456</a>	CIAM: OpenSSL upgrade to 1.0.2ze and 1.1.1o.
<a href="#">CSCwc65802</a>	Save button for SAML configuration grayed out.

Bug ID	Reason
<a href="#">CSCvy84989</a>	Enabling cookies for POST /ers/config/internaluser/ causes Identity Group(s) does not exist error.
<a href="#">CSCwc12693</a>	Cisco ISE ERS Validation Error- Mandatory fields missing: [validDays].
<a href="#">CSCvz33839</a>	Menu access customization is not working.
<a href="#">CSCwb91392</a>	Health check and full upgrade precheck timesout when third party CA certificate is used for the admin.
<a href="#">CSCvz75902</a>	Cisco ISE replacing pxGrid cert when generating Cisco ISE internal CA.
<a href="#">CSCvz65182</a>	If we set MTU greater than 1500 then the MTU value is not setting persistently across reboot.
<a href="#">CSCvu94544</a>	Cisco ISE 3.0 BH: TACACS live logs do not give an option select Network Device IP.
<a href="#">CSCwc09104</a>	Guest redirect with Auth vlan no longer works on Cisco ISE Release 3.1.
<a href="#">CSCvz17020</a>	Cisco ISE GUI shows all the licenses as Out of Compliance - Smart Licensing.
<a href="#">CSCwa45316</a>	MDM intune integration broken for vpn user on Cisco ISE Release 3.1.
<a href="#">CSCwd10840</a>	Cisco ISE CLI is stuck.
<a href="#">CSCwb88851</a>	Inconsistent IP to SGT mapping after several re-authentications when VN value is changing.
<a href="#">CSCvz63405</a>	Cisco ISE client pxGrid certificate is not delivered to Cisco DNA Center.
<a href="#">CSCwb75093</a>	CIAM: linux-kernel 4.18.0
<a href="#">CSCvy92040</a>	Cisco ISE restore popup menu displays wrong text.
<a href="#">CSCvz72208</a>	Cisco ISE Release 3.1: Authentication tab shows blank result in Context Visivility.
<a href="#">CSCwc21400</a>	HTTP 400 response in Repo OpenAPI when an SFTP/FTP repo user password contains ! (exclamation mark).
<a href="#">CSCwa79799</a>	Missing PermSize attribute on sysodbcini file.
<a href="#">CSCvn27270</a>	Cisco ISE: Cannot create network device group with name Location or Device Type.
<a href="#">CSCvz43183</a>	Sponsor permissions are not passed to guest REST API for "By Name" calls.
<a href="#">CSCwc59570</a>	Cisco ISE sending SXP MSG size > 4096 bytes in SXP version 4.
<a href="#">CSCwa67433</a>	Cannot export SAML provider info xml file from the Cisco ISE GUI.
<a href="#">CSCwc24126</a>	Profiler condition not displaying the attribute value.
<a href="#">CSCwa97357</a>	Cisco ISE is not sending "mobilenumber" value in the SMTP API body.

Bug ID	Reason
<a href="#">CSCvz61191</a>	Cisco ISE Release 3.1: No response when click "choose file" on import endpoints from CSV file page.
<a href="#">CSCwb94890</a>	Key Performance Metrics report has no entries for 8 AM and 9 AM every day.
<a href="#">CSCwb09045</a>	Cisco ISE policy service nodes crashing due to incorrect cryptoLib initialization.
<a href="#">CSCwb11147</a>	Improvement to logs needed with conflict handling SGT-IP mapping w/VN.
<a href="#">CSCwa46758</a>	Deleted root network device groups are still referenced in the network devices exported CSV report.
<a href="#">CSCwc81729</a>	"All devices were successfully deleted" after trying to delete one particular NAD by filtering.
<a href="#">CSCvz20851</a>	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerability.
<a href="#">CSCvu94025</a>	Cisco ISE should either allow IP only for syslog targets or provide DNS caching.
<a href="#">CSCvz71284</a>	SNMPv3 COA request is not issued by Cisco ISE Release 2.7.
<a href="#">CSCwa90930</a>	Need hard Q cap on RMQ.
<a href="#">CSCvx85675</a>	Cisco ISE can't handle deletion/addition of SXP-IP mappings propagation due to race condition.
<a href="#">CSCwb04898</a>	Unable to restore CFG backup from linux SFTP repository if the file owned by a group name w/ space.
<a href="#">CSCwb57665</a>	Cisco ISE evaluation for Struts2 CVE-2021-31805.
<a href="#">CSCwc48509</a>	Windows Server 2022 is actually working as the target domain controller to be monitored.
<a href="#">CSCvz94133</a>	Configuration backup fails due to "EDF_DB_LOG".
<a href="#">CSCvw90586</a>	Unable to change network device group name and description at the same time.
<a href="#">CSCwa51150</a>	WLC failed to validate EAPOL Key M2 with Cisco ISE Release 3.1.
<a href="#">CSCwb82141</a>	Context visibility endpoints and NADs from an existing deployment are not removed after restore.
<a href="#">CSCvs55875</a>	Existing routes are not installed in routing table after MTU change.
<a href="#">CSCwa47566</a>	Cisco ISE Conditions Studio: Identity Groups drop-down limited to 1000.
<a href="#">CSCwb91645</a>	Cisco ISE TrustSec Dashboard Refresh Call causing high CPU on MnT.
<a href="#">CSCvz34849</a>	DELETE /ers/config/networkdevicegroup/{id} not working; CRUD exception.
<a href="#">CSCvz65945</a>	"Invalid Length" TACACS authorization failures within live logs for non-TACACS traffic.

Bug ID	Reason
<a href="#">CSCwb38069</a>	Cisco ISE Release 3.1: Services failed to start after restoring backup from old Cisco ISE Release 2.6.
<a href="#">CSCvy16894</a>	Authorization profile will throw an error if we use some symbols.
<a href="#">CSCwa13877</a>	Cisco ISE Smart Licensing Authorization Renewal Failure: Details=Invalid response from licensing cloud.
<a href="#">CSCwa76896</a>	Duplicated culomn "Failure Reasons" in RADIUS Authentications Report.
<a href="#">CSCwa47133</a>	Cisco ISE Evaluation log4j CVE-2021-44228.
<a href="#">CSCvy66598</a>	MAR feature should be ignored in case of MAB authentication.
<a href="#">CSCwa17718</a>	Session service unavailable for pxGrid Session Directory with dedicated MnT.
<a href="#">CSCwc05718</a>	Cisco ISE Debug Wizard Posture profile does not contain client-webapp component to DEBUG.
<a href="#">CSCwb05532</a>	Location of "Location" and "Device Type" exchanging every time clicking Network Devices > Add.
<a href="#">CSCwb22662</a>	64-character limit is too small to accommodate external user identities, such as user principal name.
<a href="#">CSCvz83753</a>	Empty user custom attribute included in AuthZ advanced attributes settings results in incorrect AVP.
<a href="#">CSCwa75348</a>	ODBC behavior failover issues.
<a href="#">CSCwb81416</a>	Cisco ISE Release 3.1 GUI not loading post login.
<a href="#">CSCwb40349</a>	Cisco ISE 3.X: Invalid characters in external RADIUS token shared secret.
<a href="#">CSCvz67073</a>	Cisco Identity Services Engine Authentication Bypass Vulnerability.
<a href="#">CSCwb62192</a>	Scheduled backup failure when Cisco ISE indexing engine backup failed.
<a href="#">CSCwb01854</a>	Upgrade External RADIUS server list not showing up after upgrading to Cisco ISE Release 3.0 or later.
<a href="#">CSCvz05704</a>	Platform check fails for Cisco ISE having disk size more than 1TB.
<a href="#">CSCwa43187</a>	Cisco ISE Queue Link Error: Message=From Node1 To Node2; Cause=Timeout in NAT'ed deployment.
<a href="#">CSCwb47255</a>	Supported HTTP methods are visible.
<a href="#">CSCvz00258</a>	SessionCache not cleared for TACACS AuthZ failures results in high heap usage and authentication latency.
<a href="#">CSCwb86283</a>	Cisco ISE Deployment: All nodes thrown OUT_OF_SYNC as a result of incorrect certificate expiry check.

Bug ID	Reason
<a href="#">CSCwa19573</a>	Catalina.out file is huge because of SSL audit events.
<a href="#">CSCwb82469</a>	Windows 11 Pro for Workstations is indeed not supported yet in the latest posture feed update.
<a href="#">CSCvw90778</a>	T+ ports (49) are still open if disable device admin process under deployment page.
<a href="#">CSCvz55258</a>	Cisco:cisco-av-pair AuthZ conditions stopped working.
<a href="#">CSCwa52110</a>	SNMP config set on the N/w device, a delay of 20 seconds is introduced while processing SNMP record.
<a href="#">CSCvz00659</a>	Special characters in Banner blocking SFTP repository.
<a href="#">CSCwc65711</a>	MAC - CSC 5.0554 web deployment pkgs are failed to upload to ISE->CP->resources[100MB].
<a href="#">CSCvz45150</a>	Cisco ISE Release 3.1 requests a traditional license.
<a href="#">CSCwc27765</a>	Cisco ISE configuration backup fails due to SYS_EXPORT_SCHEMA_01.
<a href="#">CSCwa59237</a>	Deployment-RegistrationPoller causing performance issues on PAN node with 200+ internal certificates.
<a href="#">CSCwa38023</a>	Cisco ISE Release 3.1: Unable to generate pxGrid certificates with Active Directory super admin.
<a href="#">CSCwb57675</a>	Cannot disable "Dedicated Mnt" option from the Cisco ISE GUI once it is enabled.
<a href="#">CSCwa82553</a>	Cisco ISE Release 3.1 default route is on the incorrect interface if bonding is configured.
<a href="#">CSCwa04370</a>	Cisco ISE Release 3.1: Default route removed or tied to wrong interface after upgrading.
<a href="#">CSCwa32814</a>	Cisco ISE Configured with 15 Collection Filters Hides the 15th Filter.
<a href="#">CSCwa60873</a>	Optimize bouncy-castle class to improve performance on primary administration node.
<a href="#">CSCwc42712</a>	Cisco ISE RADIUS and PassiveID session merging.
<a href="#">CSCvz46560</a>	Cisco ISE using jquery v1.10.2 is vulnerable.
<a href="#">CSCwc53895</a>	Cisco ISE Release 3.1 Patch 3 SAML SSO doesn't work if active policy service node goes down.
<a href="#">CSCvz79518</a>	Serviceability: "DNS Resolution Failure" alarm should show Cisco ISE server.
<a href="#">CSCvz08319</a>	Cisco ISE application server process is restarting during Dot1X due to buffer length = 0 for EAP TLS.
<a href="#">CSCwa08484</a>	Missing IPv4 mappings if sessions have both IPv4 and IPv6 addresses
<a href="#">CSCwb23028</a>	Inaccurate dictionary word evaluation for passwords.
<a href="#">CSCvy45345</a>	EAP-chaining authz failure due to machine authentication flag set to true incorrectly.



Bug ID	Reason
<a href="#">CSCvz38266</a>	ADFS SAML login to work with FQDN same as Okta.
<a href="#">CSCwd10997</a>	Node syncup fails to replicate wildcard certificate with the portal role.
<a href="#">CSCwb98854</a>	Cisco ISE not update expiry date after updating SLR license.
<a href="#">CSCvy96761</a>	Session cache needs to be update dduring EAP chaining flow to handle relevant identities.
<a href="#">CSCvy69900</a>	CIAM: linux-kernel 4.18.0.
<a href="#">CSCwa37580</a>	Cisco ISE Release 3.0 NFS share stuck.
<a href="#">CSCwb84779</a>	Changing Parent Identity Group name breaks authorization references.
<a href="#">CSCwb00530</a>	Android VPN and InTune MDM integration not working on Cisco ISE Release 3.1.
<a href="#">CSCvx85064</a>	Enable ability to modify SMS content when sponsornet guest self-reset password.
<a href="#">CSCwa16291</a>	Guest Portal's Button's text element is causing words to be repeated for Apple VoiceOver.
<a href="#">CSCwa03126</a>	Cisco ISE CPP not loading correctly in some languages.
<a href="#">CSCwa36350</a>	Hotpatch API details have blank timestamp.
<a href="#">CSCvz90852</a>	Hotspot Guest Portals in CNA with blank Success and not switched to done on iDevices.
<a href="#">CSCwc57939</a>	Cisco ISE detects large VMs as unsupported.
<a href="#">CSCwa57705</a>	IP-SGT mapping does not link with new network access device group.
<a href="#">CSCvz92898</a>	SCM js files browser download during admin login.
<a href="#">CSCwa05404</a>	Stale sessions observed for TACACS could not find selected service error.
<a href="#">CSCwb37760</a>	Sponsor Portal getting error 500 when enabling "Allow kerberos SSO" portal setting.
<a href="#">CSCvz72069</a>	pxGrid shown disabled on Summary page for Cisco ISE-PIC.
<a href="#">CSCwd13555</a>	Cisco ISE abruptly stops consuming passive-id session from a third party syslog server.
<a href="#">CSCvz95326</a>	Unable to add more than one ACI IP address/hostname when trying to enable ACI integration in Cisco ISE.
<a href="#">CSCwa08018</a>	Cisco ISE Release 3.1 - The Cisco ISE GUI is not working when IPV6 is disabled globally.
<a href="#">CSCvy76622</a>	SystemTest: Android BYOD flow with EST and StaticIP/Hostname/FQDN fails.
<a href="#">CSCwb03479</a>	Hotpatch.log needs to be included in support-bundle.
<a href="#">CSCvv43120</a>	Cisco ISE 2.x: Intune MDM Alarm for connectivity    401 Unauthorized.

Bug ID	Reason
<a href="#">CSCwb84440</a>	Sponsor portal breaks after removing endpoint groups.
<a href="#">CSCwa00729</a>	All NADs are deleted due to one particular NAD deletion.
<a href="#">CSCwa82247</a>	Cisco ISE Queue Link Error: Cause=Timeout due to 169.254.2.0/25 in Cisco ISE IPtables.
<a href="#">CSCwb39964</a>	Cisco ISE can login to the Cisco ISE GUI with disabled shadow admin accounts with external identity source.
<a href="#">CSCwb07504</a>	Sorting internal users based on User Identity Groups doesn't work in Identity Management->Identities.
<a href="#">CSCvz93230</a>	Guest portal does not load if hosted on a different interface from Gig0.
<a href="#">CSCwa53499</a>	REST ID is fetching the groups from cloud once the connector settings page is opened.
<a href="#">CSCwa56771</a>	Cisco ISE Release 3.0 patch 2- Monitor all setting displays incorrectly with multiple matrices and different views.
<a href="#">CSCwa60903</a>	ISE is adding extra 6 hours to nextUpdate date for CRL
<a href="#">CSCwa41166</a>	Unsafe characters in T+ commands stored in Hex Numeric Character References.
<a href="#">CSCwa55866</a>	TACACS responses are not sent sometimes with single connect enabled.
<a href="#">CSCvo39514</a>	MnT log processor is not running because collector log permission.
<a href="#">CSCwb40942</a>	From address to send email is invalid if it does not end with .com or .net.
<a href="#">CSCvk25808</a>	Unable to edit or remove Scheduled Reports if admin who created them is no longer available
<a href="#">CSCwb53455</a>	RMQ TLS syslogs related to internal docker IP 169.254.2.2 are sent to audit logs.
<a href="#">CSCvz57267</a>	Inability to import Cisco ISE certificates issued for primary administration node to other nodes in spite of the SAN field FQDN.
<a href="#">CSCvz20020</a>	Okta redirection fails for first ID store and works when second ID store is assigned.
<a href="#">CSCwc51219</a>	CSV NAD import is rejected if += characters are at the beginning of the RADIUS shared secret.
<a href="#">CSCvz60870</a>	High Active Directory latency during high TPS causes HOL Blocking on ADRT.
<a href="#">CSCwb02346</a>	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerability.
<a href="#">CSCvy43246</a>	User unable to create a guest SSID during Portal Creation step - Cisco ISE is busy is the error displayed.
<a href="#">CSCwb93156</a>	TrustCertQuickView giving the same info for all trusted certificates.
<a href="#">CSCvz86020</a>	Live log/session not showing latest data due to "too many files open" error.

Bug ID	Reason
<a href="#">CSCwa95892</a>	\$sui_time_left\$ variable showing wrong duration
<a href="#">CSCwc33850</a>	Unable to export certificate with private key using API.
<a href="#">CSCwc11613</a>	Certificate signing request should not be case sensitive.
<a href="#">CSCwc60997</a>	Cisco ISE: SAML flow with loadbalancer is failing due to incorrect token handling on Cisco ISE.
<a href="#">CSCwb40131</a>	Getting 400 Bad Request while enabling the Internal User with external password type using Rest API.
<a href="#">CSCwa11633</a>	Cisco ISE Release 3.0: APIC Integration: Failed to create secGroup.
<a href="#">CSCwb32492</a>	Application server restart on all nodes after changing the Primary Administration certificate.
<a href="#">CSCwc00162</a>	Certificate based admin login not working when client/browser send more than one certificate.
<a href="#">CSCwb79056</a>	Cisco ISE Release 3.1 ERS call /ers/config/sgmapping/{id} doesn't return SGT value for custom SGTs.
<a href="#">CSCwc62413</a>	Cisco Identity Services Engine Cross-Site Scripting Vulnerability.
<a href="#">CSCvv02086</a>	Add ability to disable TLS 1.0 and 1.1 on Cisco ISE PIC node.
<a href="#">CSCvy94818</a>	EP's incorrectly profiled as "cisco-router" due to NMAP performing aggressive guesses.
<a href="#">CSCvz35550</a>	Cisco ISE Health Check MDM Validation false alarm.
<a href="#">CSCwc03220</a>	Removing an IP Access list from Cisco ISE destroys the distributed deployment.
<a href="#">CSCwc30811</a>	Underscore is vulnerable in Guest Portals.
<a href="#">CSCvz05966</a>	In Cisco ISE Release 2.6 patch 9, default permissions can't go back to default group Internal after adding a new group.
<a href="#">CSCwc30643</a>	My Devices Portal doesn't open after reloading the node unless we do CRUD.
<a href="#">CSCwa47221</a>	AD security groups cannot have their OU end with dot character on client provisioning policy.
<a href="#">CSCwa59621</a>	Inconsistent sorting on Cisco ISE ERS API(s) for identity group.

## 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](http://www.cisco.com/go/offices).

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

© 2022 Cisco Systems, Inc. All rights reserved.