Release Notes for Cisco Identity Services Engine, Release 3.2

First Published: 2022-08-16

Last Modified: 2024-10-30

Introduction to Cisco Identity Services Engine

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

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

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

For detailed Cisco ISE ordering and licensing information, see the *Cisco Identity Services Engine Ordering Guide*.

For information on monitoring and troubleshooting the system, see the "Monitoring and Troubleshooting Cisco ISE" section in the *Cisco Identity Services Engine Administrator Guide*.

What is New in Cisco ISE, Release 3.2?

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 your 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.

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 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 is 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 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 *Cisco Secure Network Server Appliance Hardware Installation Guide*.
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 later 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 center provided by VMware Cloud on AWS.
- Azure VMware Solution: Azure VMware Solution runs VMware workloads natively on Microsoft Azure. You can host Cisco ISE as a VMware virtual machine.
- Google Cloud VMware Engine: Google Cloud VMware Engine runs software defined data center by VMware on the Google Cloud. You can host Cisco ISE as a VMware virtual machine on the software-defined data center provided by the VMware Engine.

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

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

Note Cisco ISE cannot be installed on OpenStack.

- Nutanix AHV 20220304.392

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

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

For information about the virtual machine requirements, see the *Cisco Identity Services Engine Installation Guide* for your version of Cisco ISE.

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 7.2a (Certificate #4036). 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

Validated 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, 123,125, 127, and later
- Google Chrome versions 103, 104, 105, 106, 107, 108, 109, 110, 112, 114, 116, 117, 119, 122, 124, 126, and later
- Microsoft Edge versions 103, 104, 106, 107, 108, 109, 112, 115, and 117, 119, 122, 125, 126, and later
- Safari 18.0, and later

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

Validated External Identity Sources

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

Table 4: Validated External Identity Sources

External Identity Source	Version
Active Directory	
Microsoft Windows Active Directory 2012	Windows Server 2012

External Identity Source	Version
Microsoft Windows Active Directory 2012 R2 [1]	Windows Server 2012 R2
Microsoft Windows Active Directory 2016	Windows Server 2016
Microsoft Windows Active Directory 2019	Windows Server 2019
Microsoft Windows Active Directory 2022	Windows Server 2022 with Patch Windows10.0-KB5025230-x64-V1.006.msu
LDAP Servers	
SunONE LDAP Directory Server	Version 5.2
OpenLDAP Directory Server	Version 2.4.23
Any LDAP v3-compliant server	Any version that is LDAP v3 compliant
AD as LDAP	Windows Server 2022 with Patch Windows10.0-KB5025230-x64-V1.006.msu
Token Servers	
RSA ACE/Server	6.x series
RSA Authentication Manager	7.x and 8.x series
Any RADIUS RFC 2865-compliant token server	Any version that is RFC 2865 compliant
Security Assertion Markup Language (SAML) Single Sign-On (SSO)	
Microsoft Azure MFA	Latest
Oracle Access Manager (OAM)	Version 11.1.2.2.0
Oracle Identity Federation (OIF)	Version 11.1.1.2.0
PingFederate Server	Version 6.10.0.4
PingOne Cloud	Latest
Secure Auth	8.1.1
Any SAMLv2-compliant Identity Provider	Any Identity Provider version that is SAMLv2 compliant
Open Database Connectivity (ODBC) Identity Source	
Microsoft SQL Server	Microsoft SQL Server 2012 Microsoft SQL Server 2022
Oracle	Enterprise Edition Release 12.1.0.2.0
PostgreSQL	9.0

External Identity Source	Version
Sybase	16.0
MySQL	6.3
Social Login (for Guest User Accounts)	
Facebook	Latest

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

Supported Antivirus and Antimalware Products

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

Validated OpenSSL Version

Cisco ISE 3.2 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 that you to enable all disabled pxGrid Direct connectors before restarting Cisco ISE, and disable the connectors again following the restart. Alternatively, you could also edit the attributes of the disabled connector (making it an active connector) prior to the Cisco ISE restart as a workaround to this problem.

This problem has been resolved in Cisco ISE Release 3.2 Cumulative Patch 5 and Cisco ISE Release 3.3 Cumulative Patch 2.

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 is addressed by Microsoft in January 2024. For wired deployments, we recommended that you 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 must 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 the 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 preceding 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 the ClamWin Pty Ltd vendor.

Host Alias Isn't 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 the 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

Cisco ISE Release 3.2 Patch 5 SLR Registered Node Shows SL Registered After 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.

SNMP does not work post upgrade to Cisco ISE Release 3.2 and patches

When you upgrade to Cisco ISE Release 3.2 and its patches, the SNMP functionality is disabled by default. To enable the SNMP functionality, you must run the these CLI commands: `no snmp-server enable` and `snmp-server enable`. If the SNMP is still not enabled, you must log in with root access and run the `systemctl restart snmpd linux` command. You must contact TAC team to get the root access.

Upgrade Information

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

Upgrading to Release 3.2

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.

Upgrade Packages

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

Cisco ISE Release 3.2 upgrade bundle files have been replaced on the Cisco ISE Software Download site.

This entails:

- resolution of bugs CSCwj43362 and CSCwj55392.
- that the filenames of the new files will have "c" appended to the build number (for example, ise-upgradebundle-2.7.x-3.1.x-to-3.2.0.542c.SPA.x86_64.tar.gz).
- that existing Cisco ISE Release 3.2 cumulative patches will continue to work with this new upgrade bundle.

Upgrade Procedure Prerequisites

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

For more information, see the Cisco Identity Services Engine Upgrade Guide.

Cisco ISE Integration with Cisco Catalyst Center

Cisco ISE can integrate with Cisco Catalyst Center. For information about configuring Cisco ISE to work with Catalyst Center, see the *Cisco Catalyst Center documentation*.

For information about Cisco ISE compatibility with Catalyst Center, see the *Cisco SD-Access Compatibility Matrix*.

Install a New Patch

For instructions on how to apply the patch to your system, see the "Cisco ISE Software Patches" section in the Cisco Identity Services Engine Upgrade Journey.

For instructions on how to install a patch using the CLI, see the "Patch Install" section in the *Cisco Identity Services Engine CLI Reference Guide*.

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

Caveats

The Caveats section includes the bug ID and a short description of the bug. For details on the symptoms, conditions, and workaround for a specific caveat, use the Cisco Bug Search Tool (BST).

Note The Open Caveats sections list the open caveats that apply to the current release and might apply to releases earlier than Cisco ISE 3.2. A caveat that is open for an earlier release and is still unresolved applies to all future releases until it is resolved.

New Features in Cisco ISE Release 3.2 - Cumulative Patch 7

Security Identifiers in certificates will not be used for authentication

From Cisco ISE Release 3.2 Patch 7, Cisco ISE supports a new format of certificates with Security Identifiers (SID).

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

For more information, see "SAML-Based Admin Login" in the chapter "Asset Visibility" in the *Cisco ISE Admin Guide, Release 3.2*.

Resolved Caveats in Cisco ISE Release 3.2 - Cumulative Patch 7

Caveat ID	Description
CSCwk94725	In Cisco ISE Release 3.2 Patch 6, the endpoints lose static group assignment.
CSCwj72586	There are OOM killer alerts on the Cisco ISE Admin CLI as a result of an API-gateway memory limitation.
CSCwh01906	Deleted MDM server is still getting listed in MDMServerName attribute allowed values.
CSCwi88583	Handle erl_crash.dump in a better way.
CSCwk07593	Get-All guest user API is not retrieving all accounts.
CSCwj82278	Stale lock file(s) is blocking API gateway and context visibility.
CSCwj76445	Cisco ISE ERS guest documentation should be updated to exclude portal ID from the get calls.
CSCwj97620	pxGrid Direct Sync gets stuck in progress and never goes to completion state.
CSCwk06043	Binding with SGT assigned via MAB policy is not seen in SGT bindings table.

Caveat ID	Description
CSCwj54376	Evaluate configuration validator does not parse all NAD interfaces.
CSCwi57761	The SSH transport protocol with certain OpenSSH extensions allows remote attackers to bypass integrity checks such that client and server may develop a connection for which some security features have been downgraded.
CSCwk25206	Empty (1KB) gpg files are exported if there is no data to purge.
CSCwj68795	Replication error "Error synchronizing object: EDF2EndPoint: Operation: Update".
CSCwh00060	Cisco ISE JoSQL Code Injection Vulnerability was identified.
CSCwi93050	Endpoint import fails for RBAC when using Azure SAML for admin access.
CSCwk13234	Old Cisco ISE nodes get shown in TCP dump and debug profile configuration after restore.
CSCwj83460	Discrepancy in the count of identity groups between the CV and Oracle database.
CSCwf69715	After Cisco ISE Release 3.1 Patch 5 or above installation, TC-NAC adapters will not be reachable and new adapters will not get configured.
CSCwj58727	Cisco ISE should not allow saving allowed protocols with no protocols checked.
CSCwh49351	The ISE admin portal SAML SSO should not redirect to another ISE node, such as the active PSN.
CSCwf18758	Unidentified member user found in super admin administrator group.
CSCwj82240	In Cisco ISE Release 3.2, app counters reports are empty for secondary nodes.
CSCwi67503	Cisco ISE could not find selected authorization profile if created using API.
CSCwd49321	Cisco ISE integration returns an error: "ISE integration error in DNAC GUI: pxGrid not enabled on ISE" even when pxGrid is enabled.
CSCwj32716	NSF should return index-0 (always first URI prefer) SAN-URI to MDM.
CSCwk07454	In Cisco ISE Release 3.2 Patch 6, PSN does not update the DB with the correct posture lease expiry time.
CSCwh95587	Cisco ISE is intermittently not unmounting NFS repositories.
CSCwk46855	Customer with pending account issue isn't reflecting under the sponsor manage account section.
CSCwk30610	Cisco ISE Release 3.2 TACACS+ endstation network condition high step latency while accessing the NAD via console.
CSCwj04197	Cisco ISE stored Cross-Site Scripting Vulnerability.
CSCwj04195	Cisco ISE stored Cross-Site Scripting Vulnerability.
CSCwi20027	Trustsec deploy request failed - CoA request gets stuck while fetching NADs.
CSCvy30859	In Cisco ISE Release 2.6, it is not possible to create static IP-SGT mapping for EPG's imported from ACI.

Caveat ID	Description
CSCwh97876	Cisco ISE Arbitrary File Upload Vulnerability.
CSCwk38279	ea.log file should be included in Support Bundle.
CSCwj84815	Cisco ISE Release 3.3 Patch 2 Error: No session available.
CSCwk31930	Cisco ISE skips authentication against the child DC because the forest is marked as offline.
CSCwj51329	MDM compliance check fails when there are multiple MAC addresses with "VMWare Workspace One" as MDM.
CSCwj39533	RMQforwarder causes high CPU/load average on PSN nodes.
CSCwk73627	Data connect certificate is not getting reflected in trusted certificates store after generating it through CSR.
CSCwc32552	Rate-limiting in Cisco ISE should only be applied to external interfaces.
CSCwj67089	Cisco ISE Release 3.4 BH ISE app server crashes importing large files to secondary node via local disk management.
CSCwf36985	AD group retrieval fails while evaluating authorization policy.
CSCwi79159	Cisco ISE Release 3.2 Patch 4: deleteCertFromStore error: failed to parse certificate.
CSCwk07483	Profiler NetworkDeviceEventHandler Failed to add device error: For input string: "0-255".
CSCwj05508	IP host <ip> <fqdn> command not creating ip-fqdn entry in Cisco ISE.
CSCwj23933	Connector status shows "Not joined" due to AD connector crash.
CSCwj14217	Device network conditions is not loading.
CSCwj48827	Unable to add multiple tasks with quotes ("") in launch program remediation.
CSCwh23986	pxGrid getUserGroups API request return empty list.
CSCwi86762	Right COA to be triggered in VPN flow when posture and MDM flow are configured together.
CSCwj07675	Cisco ISE Release 3.2 sending outgoing RST packets with APIPA IP 169.254.4.X.
CSCwd57846	Convert TACACS AUTHZ to SqlLoader approach to reduce DB transactions.
CSCwj85626	Not able to retrieve endpoint IP address via API calls.
CSCwf79582	AD credentials fail to integrate Cisco ISE with 2.2.1.x and above.
CSCwk13244	Ise-messaging.log is not visible on GUI for download.
CSCwj95818	Maximum concurrent CLI sessions doesn't work.
CSCwk32078	Endpoint check result remains unreachable after passiveID login event.
CSCwk00439	pxGrid Direct service stuck in initializing state due to non-removal of lock file.

Caveat ID	Description
CSCwj35581	Cisco ISE is missing rate limiting protection.
CSCwh39213	Unable to replace SSH key for Cisco ISE AWS EC2 instances.
CSCwi78164	Cisco ISE DNS resolvability health check fails due to a duplicated entry (IP, name and FQDN) on /etc/hosts.
CSCwj12489	Unable to delete network device group.
CSCwk04493	Policy details retrieval method calls the internal method and is not cached.
CSCwj80616	EP details in Cisco ISE context visibility does not match with radius live logs or sessions during MDM workflow.
CSCwk59763	MDM significant attributes triggering the database persistent events.
CSCwj48625	Agentless posture fails for EAP-TLS flows with multiple domains configured for endpoint login.
CSCwj43912	Application remediation disappears after getting modified.
CSCwk04644	System 360 monitoring debug log rotation is not working.
CSCwk14636	Insufficient virtual machine resources alarm not working on AWS.
CSCwf85644	Cisco ISE - Cisco-av-pair throws an error when using % for PSK.
CSCwk21895	Cisco ISE password length shows 127 characters as maximum characters allowed.
CSCwi38377	Unable to trigger COA, stuck at dispatcher queue.
CSCwk09094	Misleading pop-up seen while we set password lifetime for more than 365 days.
CSCwj92369	Registry Condition: Inline creation GUI issue on requirements page.
CSCwi52041	Changes in rank causing authorization rule to commit to the DB table which triggers save call from UI.
CSCwk32104	agentprobeoom.sh & restprobeoom.sh need to clean up their own OOM Heap files.
CSCwk38327	Health check is failing for MDM flow.
CSCwj66951	DOC network access user first name and last name fields doesn't allow for "OR" in the name.
CSCwc64144	TotalAuthenLatency and ClientLatency doesn't work for T+.
CSCwk20019	Attribute name in SMS HTTP URL causes issues with URL updates on editing.
CSCwk35172	DumpClearOnExceed files are filling up the disk on Cisco ISE PSN nodes.
CSCwj35576	Cisco ISE Server-side validation is missing.
CSCwj33447	Cisco ISE Guest Portals Arbitrary File Upload Vulnerability.
CSCwk07789	Getting invalid IP or hostname error when using "_" as first character in the nslookup request.
CSCwj07717	Cisco ISE audit reports log APIPA addresses as the source of API requests.

Caveat ID	Description
CSCwj77501	ODBC advanced attributes does not work if two or more inbound attributes are chosen.
CSCwj35698	Cisco ISE business logic issue - user dictionaries.
CSCwj82298	Assigned logical profile is repeated in context visibility endpoint attributes and reports.
CSCwj83459	Cannot create internal user when there exists a user with same name.
CSCwj72680	HS_err files gets generated on MNT nodes.
CSCvv77007	Cisco ISE constantly requesting internal "Super Admin" users against external RADIUS token server.
CSCwf56826	JStack crash issue is causing the appserver to restart.
CSCwk73315	Cisco ISE 360 Monitoring dashboard displays average CPU time percentage instead of summing the rate.
CSCwj72117	Operational data purging shows only primary monitoring node name.
CSCwk25064	SXP threads storing NULL objects in the Java heap are causing high CPU load and utilization.
CSCvy34255	Extra popup screen appears while viewing Radius/TACACS key after enabling "Require Admin Password".
CSCwj97449	SNMP v3 config does not alert the admin when engineID format is incorrect for SNMP-server host.
CSCwi61950	Cisco ISE is reaching context limit in proxy flow when querying LDAP groups for authorization policy.
CSCwh69267	Post Adeos restore, appserver is stuck at initializing.
CSCwa82035	Cisco ISE serviceability to include GarbageCollector logs, thread dump, and heap dump.
CSCwj06269	No report or alarm for device administration configuration changes.
CSCwj33906	IP/SXP mapping not created for VPN clients.
CSCwj72982	No IPV4 or IPV6 selection seen for passive ID reports for IP address column filter.
CSCwk34825	Cisco ISE internal user lock/suspend on incorrect attempts counter is not working as expected.
CSCwj17975	Cannot assign EAP role on certificate with IMS role.
CSCwj21403	Rest Authorization service will not get enabled when /etc/hosts has multiple entries.
CSCwj89479	When joining multiple Cisco ISE nodes to the domain controller simultaneously, duplicate accounts are being created.
CSCwi74567	Cisco ISE portal is getting corrupt due to inconsistencies in the DB.
CSCwk11836	TACACS livelogs and reports are getting impacted during rollback of P8 to P7.
CSCwk29799	List of installed patches not getting shown under patch management UI due to admin certificate issue.
CSCwi66105	Cisco ISE Release 3.1 Patch 7 CSCvn66106 regression: Custom attribute retention failure.
CSCwj40026	Backup details are showing scheduled number and triggered from CLI, even though they were GUI scheduled.

Caveat ID	Description
CSCwc62131	Cisco ISE is no longer able to query MySQql 8.x due to mysql.proc table no longer implemented.
CSCwh36667	Cisco ISE monitoring GUI page is stuck at "Welcome to Grafana" page.
CSCwk45006	Device admin license is not allowing Cisco ISE admin user to reset first login password.
CSCwk07324	Cisco ISE main thread pool stuck due to ACE 3rd party library.
CSCwj74175	Compress restprobeOOMHeap dumps.
CSCvm56115	Cisco ISE allows policy to be saved when an IDStore is deleted from another browser tab.
CSCwj01310	Longevity3.4: 8 Node Longevity - Intensive GC is observed due to SXP component.
CSCwj80950	Cisco ISE is not sharing posture compliant session properly over pxGrid.
CSCwj77067	Better description for error while modifying internal users.
CSCwk61938	Cisco ISE to evaluate OpenSSH CVE-2024-6387 "regreSSHion".
CSCwj29392	Cisco ISE cross-site request forgery issue.
CSCwi89720	Microsoft Azure AD has been officially renamed as Microsoft Entra ID.
CSCwj12359	Interrupting execution of "show tech-support" is causing services to stop on Cisco ISE.
CSCwj94294	Cisco Identity Services Engine REST API Blind SQL Injection Vulnerabilities.
CSCwj94297	Cisco Identity Services Engine REST API Blind SQL Injection Vulnerabilities.
CSCwj94305	Cisco Identity Services Engine REST API Blind SQL Injection Vulnerabilities.
CSCwj94315	Cisco Identity Services Engine REST API Blind SQL Injection Vulnerabilities.
CSCwj33460	Cisco Identity Services Engine Cross-Site Request Forgery Vulnerability.
CSCwj97491	Cisco Identity Services Engine Command Injection Vulnerability.
CSCwj04194	Cisco Identity Services Engine Information Disclosure Vulnerability.

New Features in Cisco ISE Release 3.2 - Cumulative Patch 6

Support for Transport Gateway Removed

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

- Cisco ISE Smart Licensing

  If you use Transport Gateway as the connection method in your smart licensing configuration, you must edit the setting before you upgrade to Cisco ISE Release 3.2 Patch 6. You must choose a different connection method as Cisco ISE Release does not support Transport Gateway. If you upgrade to Cisco ISE Release 3.2 Patch 6 without updating the connection method, your smart licensing configuration is automatically updated to use the Direct HTTPS connection method during the upgrade process. You can change the connection method at any time after the upgrade.

- Cisco ISE Telemetry

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

Resolved Caveats in Cisco ISE Release 3.2 - Cumulative Patch 6

Caveat ID Number	Description
CSCwf47838	Space characters in Command Arguments are not preserved after CSV Export of TACACS+ Command Set.
CSCwi60778	Endpoint Loses Static Identity Group Assignment after Reauthentication.
CSCwf24553	SR-Insights - Umbrella defect for providing information for terminologies used in Licensing page.
CSCwf24554	SR-Insights - Umbrella defect for displaying more information on SL registration failure.
CSCwi89466	Cisco ISE AD User SamAccountName parameter is null for user session (3.2 P3 or later).
CSCwi58699	CoA is triggered through a Guest Flow when DNAC/EA dictionary attributes are updated on Cisco ISE.
CSCwi62078	[404] Resource Not Found when using the built-in Authorization profile Block_Wireless_Access.
CSCwi58421	PSN node does not update the DB with correct posture expiry time when posture lease is enabled.
CSCwi34405	Unable to enforce IdentityAccesss Restricted attribute during authorization.
CSCwi61491	Application Server Crashes Due to Metaspace exhaustion.
CSCwi29253	Cisco ISE AD Diagnostic Tool stops working upon upgrade, unable to retrieve list of available tests.
CSCwh33160	Cisco ISE does not send SNMPv3 disk traps to configured SNMP server.
CSCwi53104	Export of the report beyond a one-month period yields no data.
CSCwf61673	Cisco ISE CLI Read only users can not run show CPU usage command.
CSCwi54722	Redirect URL use fqdn that ends with IP, IP is replaced by Cisco ISE hostname.
CSCwi15793	Cisco Identity Services Engine custom attribute special characters error.
CSCwa15336	Cisco ISE PIC 3.1: Live Session should not show terminated sessions.
CSCwi59868	Sponsored guest account extension works more than maximum number of days.
CSCwi45090	Cisco ISE: REST API ERS: downloadableacl: The filter field 'name' is not supported.
CSCwi89082	Cisco ISE Portal (default) Deleted from database which is needed to configure SAML.
CSCwi42628	MAR Cache replication failed between peer nodes for both NIC and NON-NIC bonding interfaces.
CSCwi36040	IP access list control in Cisco ISE Release 3.2 is not visible.

Caveat ID Number	Description
CSCwi34117	Grafana UI and Kibana should have RBAC implemented in Identity Services Engine.
CSCwh67500	Cisco ISE 3.2 Could not find selected Authorization Profiles.
CSCvs77939	Errors editing AnyConnect configuration and Posture Agent profiles.
CSCwj21203	1000 DB connections exhausted due to "Dashboard System Status" query.
CSCwj03747	Profiling is not suppressing CoA although we have suppress CoA for specific logical groups.
CSCwi32576	PSN node crashes while assigning the cpmSessionId.
CSCwj16540	Cisco ISE 3.2 Patch 4 Context Visibility does not match Live Logs or Sessions.
CSCwi45879	Unable to select hotspot portal if an existent or duplicated authorization profile is selected.
CSCwi53915	Advanced Filter "Save" option does not work for Client Provisioning Resources filtering.
CSCwf89224	Decryption of Session ticket received from the client fails on Cisco ISE.
CSCwh99772	All network device groups are deleted after removing a child item from any group.
CSCwi86161	[ESXi VA] Functional: mDNAC role UNDEFINED and unable to start ACA migration after Cisco ISE integration.
CSCwj47769	Invalid Request page in Cisco ISE Release 3.2 Patch 5.
CSCwh41977	Cisco ISE 3.2 : Verify existence of Per-User dACL on Cisco ISE configuration.
CSCwh56565	PPAN rest call to MNT nodes (live logs, reports) should not be load balanced.
CSCwj44477	Upgrade Issue -"Database upgrade failed" message.
CSCwi57903	No alarm generated for failed schedule backup.
CSCwj07319	API ers/config/sessionservicenode returns incorrect total.
CSCwi73984	Cisco ISE 3.1P8 Installed Patches menu does not list all the patches.
CSCwi33361	Cisco ISE CLI access problems: Failed to connect to server.
CSCwi21020	Cisco ISE Messaging Certificate generation does not replicate full certificate chain on secondary nodes.
CSCwh72754	Cisco ISE active directory process (lwsmd) stuck at "Updating" and consuming 90-100% CPU.
CSCwi66126	Cisco ISE ERS API - Updating DACL does not modify last update timestamp.
CSCwc85211	Cisco ISE Passive ID Agent error "id to load is required for loading".
CSCwi57950	Cisco ISE 3.2 : Nexpose Rapid 7 : Strict-Transport-Security malformed.
CSCwi98793	Profiler caching mdm attribute with wrong values.
CSCwi17694	Cisco ISE: synflood-limit does not take effect if configured with more than 10000.

Caveat ID Number	Description
CSCwd67833	ERS API takes several seconds to update single endpoint.
CSCwi67639	Command show cpu usage does not display information on Cisco ISE 3.X.
CSCwi30707	Cisco ISE 3.1 patch 7 : Removed Device Types remain selectable in Policy Set.
CSCwi73981	Cannot remove identity store from CLI that was added using uppercase FQDN.
CSCwi89689	Cisco ISE - Invalid IP or hostname error.
CSCwi94938	Cisco ISE 3.2 guest user API gives incorrect results when filter used.
CSCwi59216	Sponsor Portal returns 400 Bad Request when clicking (Contact Support).
CSCwi59567	Issues with updating the CoA retry count to "0" .
CSCwi52264	Cisco ISE SAML ID provider Configuration Attributes are deleted though they are referenced.
CSCvt75833	Cisco ISE should do nslookup again when the token server is FQDN.
CSCwi17200	Cisco ISE: TROUBLESHOOTING.EncryptionOffPeriod causes RPC netlogon failure.
CSCwi48806	Authorization policy takes time to load, causes duplicate portal entries.
CSCwi96581	Upgrade CXF Version as 3.4.2 is vulnerable.
CSCwi88504	Cisco ISE Release 3.2P5 : missing step and resolution text in live logs for attribute.
CSCwi59230	Non super-admin users cannot edit or delete endpoints when Cisco ISE has more than 1k identity groups.
CSCwf80386	Current value of Disable_RSA_PSS environmental value is not preserved upon patch installation.
CSCwi63725	SNMPD process causing memory leak on Cisco ISE.
CSCwi25755	From Cisco ISE 3.2 or higher. Cannot Add SAML Provider.
CSCwh25160	Swap cleanup script to drop the swap area and program the cron.
CSCwf51766	Cisco ISE cannot create a Authentication Policy with DenyAccess Identity Source through OpenAPI.
CSCwj06401	Endpoints has null key value pair in the attributes section is interrupting the purge flow.
CSCwd14523	'accountEnabled' attribute causes authentication issues for EAP-TLS with Azure AD.
CSCwh61339	Export of more than 90k Network Devices time out.
CSCwa32407	ENH : resend the user account details for all or specific guest users to the sponsor.
CSCwh92366	3.1P8: Observing Insufficient Virtual Machine Resource Alarm in 3.1P8 Longevity setup.
CSCwf17714	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 "Localized ISE Installation" in the chapter "Cisco ISE CLI Commands in EXEC Mode" in the *Cisco ISE 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
CSCwb57672	GCMP256 authentication for SHA384 with RSA4096 certificate failed.
CSCwh36544	PxGrid not showing topic registration details.
CSCwh42683	Read-Only permissions for SAML users.
CSCwh64195	Data corruptions causing FailureReason=11007 or FailureReason=15022.
CSCwh99534	Endpoint Probe does not clean up SXP mappings.
CSCwh24823	When non-mandatory attributes are not included in the PUT requests, those values are reset to empty or default.
CSCwd48787	ISE - SSL buffer is not cleared and affects PAC decryption.
CSCwh90691	Show CLI commands throws exception after configuring log level to 5.
CSCwh83323	SMS not sent in "Reset Password" flow when a custom "SMTP API Destination Address" is used.
CSCwe25050	Wildcard certificate imported on PPAN not replicated to other nodes in deployment.

Caveat ID	Description
CSCwi18005	External RADIUS server list does not show up after upgrading to Cisco ISE 3.2.
CSCwd21798	Cisco ISE-PIC license expiration alarms.
CSCvj75157	Cisco ISE API does not recognize identity groups while creating user accounts.
CSCwh63501	Vulnerabilities in log4net 2.0.8.0.
CSCwi37249	Endpoints profiled incorrectly as Android devices.
CSCvz86688	Aruba-MPSK-Passphrase needs encryption support.
CSCwh58768	Unable to delete existing devices in My Device portal after restoring from ISE 2.7 version.
CSCwh47601	Unable to create SNMPv3 user with auth and priv passwords equal to 40 characters.
CSCwh18899	Need support for system certificate import for multi-node cluster in ISE OpenAPI.
CSCwc04447	Unable to filter the TACACS Live Logs via Network Device IP.
CSCwh17285	Portals fail to initialize if IPv6 enable is the only IPv6 command on interface.
CSCwh70696	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability.
CSCwi04514	Posture client provisioning resources HTTP error when dictionary attribute contains "-".
CSCwh24754	Excess number of AD groups mapped to sponsor groups causing latency in sponsor login.
CSCwh81035	PAN missing non-significant attribute updates of endpoints from PSNs.
CSCwh10401	Cannot generate pxGrid client certificate leveraging CSR.
CSCwh60726	ISE lwsm decodes are not done properly.
CSCwh77574	Cisco ISE does not allow special characters for password while importing certificate.
CSCwh55667	Posture failure due to expired or invalid license reported as Internal System Error in AnyConnect ISE posture reports.
CSCwh88801	0.0.0.0 default static routes configured on all interfaces get deleted post reload.
CSCwf10516	Authorization policy search feature is not working.
CSCwi45131	Apache Struts Vulnerability Affecting Cisco Products: December 2023.
CSCwi27497	REST Auth service not running on ISE node.
CSCwh52589	Acs.Username is not being updated with guest username in first device connection.
CSCwh30723	ISE Context Visibility doesn't validate static MAC entries if they miss a separator like colon.
CSCwh92185	Radius Authentication report exported from the Operational Data Purging page are empty.
CSCwh83482	ISE database not updating the email field for Sponsor Accounts.

Caveat ID	Description
CSCwh96018	Failure due to case sensitive check when new MDMs are created with the same name but different case.
CSCwh99772	All network device groups are deleted when a child item is removed from any group.
CSCwh93498	Endpoints purging rule automatically created when duplicate option is used for My Devices portal.
CSCwh90610	ISE Abandoned Jedis connections not being sent back to the threadPool.
CSCvo60450	Enhancement for encryption to only send AES256 for MS-RPC calls.
CSCwi03961	Location group information is missing from policy sets.
CSCwh41977	Verify existence of Per-User dACL on ISE configuration.
CSCwh79938	Cannot set PreferredDCs registry value in advanced tuning.
CSCwh30893	Profiling not processing the Calling Station ID values with the following format "xxxxxxxxxxx".
CSCwh84446	Guest Type save doesn't work when Account Expiration Notification has special or newline character.
CSCwh45472	Operational Backups from the GUI fail to SFTP Repositories if the PKI key pair passphrase contains +.
CSCwh38464	ISE CLI admin user unable to login after 2 months of inactive period.
CSCwi06794	RADIUS Live log delay Regression for CSCwe00424.
CSCwh71117	Enabling only "User Services" enables Admin GUI Access as well.
CSCwh95022	Sponsor portal shows wrong days of week information from [Setting date] tab when using Japanese UI.
CSCwf25955	Matching authorization profile with SGT, VN name, Vlan empty causes prrt to crash.
CSCwf61657	Gig0 always involved in TCP Handshake of Sponsor FQDN.
CSCwd34467	Authorization rule evaluation broken for attempts using eap-chaining and Azure AD groups.
CSCwi15914	Additional IPV6-SGT session binding created for IPv6 link local address from SXP Add operation.
CSCwh70275	Registering node with left over certificates from deregistration can delete in use certificates.
CSCwh69045	Few internal users password not expiring after configured global password expiry days.
CSCwh26698	Add a mechanism to fetch user data for pxGrid connector.
CSCwf98849	Critical Error displayed while saving changes made to Client Provisioning portal.
CSCwh71273	Limited GUI access/Inability to regenerate Root CA when essentials licenses are disabled.
CSCwi23166	Unable to save changes in the patch management condition.
CSCwh51156	Corrupted NAD profiles are not loaded and authentication failed with FailureReasons 11007 and 15022.
CSCwi59555	Search for MAC Address in xx:xx:xx:xx:xx:xx format ignored.
CSCwh47299	Cisco ISE Alarm and dashboard summary does not load.

Caveat ID	Description
CSCwf64662	SXP can create inconsistent mapping between IP address and SGT.
CSCwh26288	pxGrid Direct: Premier license is required to add a connector, feature should only need advantage.
CSCwc53824	ISE limits connection to AMP AMQP service to TLSv1.0.
CSCwi05905	ISE ERS API - /ers/config/deploymentinfo/getAllInfo returns different data on multi-node deployments.
CSCwh23367	ISE 3.2 Self-Reg Email Subject line truncates everything after "=" sign on Sponsor-Guest Portal.
CSCwh53159	Unable to change admin password if it contains "$".
CSCwh71435	Enable password of the internal users is created even when this is not specified through ERS API.
CSCwf38083	ISE services stuck in initializing state with secure syslog.
CSCwh93925	ISE incorrectly routes RADIUS Traffic when multiple static default routes are configured.
CSCwi28131	Endpoints with custom attributes used in Never Purge rule are still purged.
CSCwf55795	After ADE-OS restore, ISE UI and CLI not accessible in 3.2P1 and above.
CSCwi36954	When MnT database usage exceeds threshold,database purge done based on retention days set for RADIUS.
CSCwf72037	Administrator Login Report shows "Administrator authentication failed" every 5 minutes.
CSCwh21038	Session information is not stored in the timed session cache during third party posture flow.
CSCwi19099	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
CSCwh92366	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 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 Identity Services Engine Administration Guide, *Release 3.2*.

Resolved Caveats in Cisco ISE Release 3.2 - Cumulative Patch 4

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

Caveat ID	Description
CSCwh06338	Cisco ISE GUI does not load when you edit Client Provisioning Portal configuration.
CSCwf68108	'Asset' attributes and pxGrid context-in through OpenAPI.
CSCwe54318	SXP service gets stuck at initializing state due to H2 DB delay in querying bindings.
CSCwd12453	Cisco ISE Release 3.1 portal tag with special character validation issues.
CSCwb63834	MNT log processor runs on a non-management admin Cisco ISE node.
CSCwf27484	Unable to match Azure AD group in authorization due to lack of paging in the query to Azure.
CSCwf19811	Cisco ISE 3.1 SXP bindings report shows no data found.
CSCwf22794	Inconsistency in VLAN ID and Name 'Error: Not a valid ODBC dictionary'.
CSCvq79397	UI pages do not load properly with custom admin menu workcenter permissions.
CSCuz65708	Mozilla Firefox 45 and Google Chrome 72: Incorrect line numbering for DACL.
CSCwf59005	Cisco ISE Release 3.2 Patch 3: PEAP and EAP-TLS do not work in FIPS mode.
CSCwh51548	Cisco ISE 3.2.0.542: Hotpatches don't install when both patch and hotpatches are in ZTP Configuration.
CSCwc26835	RADIUS server sequence configuration is corrupted.
CSCwf44906	Reconfiguring repositories with credentials is necessary after restoration of configuration backup.
CSCwf39620	Windows agentless posture does not work if the username starts with $ (dollar sign).
CSCwh17448	Cisco ISE Release 3.1 - Agentless posture flows fail when domain user is configured for endpoint login.
CSCwf72918	In Cisco ISE Release 3.2, the order of IP name-servers in the running configuration is incorrect.
CSCwd57628	Cisco ISE Release 3.1 NAD radius shares a secret key incorrectly when it starts with an apostrophe symbol.
CSCwh46669	After the admin certificate change, Cisco ISE does not restart services if the bond interface is configured.
CSCwh26288	pxGrid Direct: A premier license is required to add a connector. The feature should only need advantage license.
CSCwe10898	The endpoint MAC address is not added to Endpoint Identity Group when using grace access in guest portal.
CSCwh42009	Cisco ISE Release 3.2 Patch 3 : Adapter log issue.
CSCwf22527	Context Visibility: Endpoint custom attributes cannot be filtered with special characters.
CSCwf88944	Guest portal FQDN is mapped with the IP address of node in database.
CSCwd38766	Deleting SNMPv3 username with a "-" or "_" character does not delete the hexadecimal username from Cisco ISE.

Caveat ID	Description
CSCwe74135	Cisco ISE Release ISE 3.1 Patch 5 : Guest portal removal failure : ORA-02292: integrity constraint.
CSCwf10773	"no ip name-server" restarts services directly without prompt.
CSCvw81130	Cisco ISE Release 2.7 - Unable to disable active directory diagnostic tool scheduled tests.
CSCwd34685	Cisco ISE messaging service oscillating between "Not running" and "Initializing".
CSCwf30570	Agentless script does not run if the computer is not on AC power.
CSCwf24158	The 'terms and conditions' checkbox disappears when Portal Builder is used for Cisco ISE Release 3.0 and later releases.
CSCwf94289	Cisco ISE Release 3.0 Patch 6: Policy export does not export policies.
CSCwa08802	Cisco ISE Release 3.1 on AWS shows a false negative on the DNS check for health checks.
CSCwe15945	Guest account cannot be seen by sponsors in a specific sponsor group.
CSCwf34391	Cisco ISE Easyconnect stitching does not work if PassiveID happens before active authentication.
CSCwh42442	Cisco ISE Release 3.2 Patch 3: CRL download failure.
CSCvy88380	Unable to select Cisco ISE messaging usage (grayed out) for an existing certificate.
CSCwf21585	Using potentially insecure methods - HTTP PUT method is accepted.
CSCwh14249	There is a Cisco ISE 3.x spelling mistake in API gateway settings.
CSCwf09364	User & endpoint identity groups description field is not editable for long text.
CSCwf47038	Trash All or Selected at pxGrid policy should not touch entries for internal group.
CSCwh04251	Cisco ISE agentless posture does not support a password containing the ":" character.
CSCvu56500	Cisco ISE exports all network devices and gives an empty file.
CSCwf66237	The Cisco ISE "Get All Endpoints" request takes time to execute since Cisco ISE Release 2.7.
CSCwf59058	RBAC policy with custom permissions does not work when the administration menu is hidden.
CSCwd97984	Meraki Sync Service does not run immediately after Cisco ISE application server restarts.
CSCwf66880	Endpoint .csv file import displays "No file chosen" after selecting a file.
CSCwf26951	Profiler CoA sent with the wrong session ID.
CSCwd17322	Cisco ISE in AWS - health check input and output bandwidth performance and check false alarm.
CSCwe27438	Launch page level help does not work with patch management, upgrade, and health checks.
CSCwf40265	The Cisco ISE maximum session counter time limit does not work.
CSCwb18744	SG and contracts with multiple backslash characters in a row in the description cannot sync with Cisco ISE.

Caveat ID	Description
CSCwh48026	pxGrid direct-connector.log discrepancy between the actual clock and the time it prints the logs.
CSCwf37679	Sponsor permissions are disabled on the sponsor portal when accessed from the primary PAN.
CSCwf96294	Cisco ISE Release 3.0: Connection attempt to disallowed domains.
CSCwf23981	Cisco ISE Authorization Profile shows the wrong Security Group and VN value.
CSCwf61939	Using an apostrophe in the First Name and Last name fields presents an invalid name error.
CSCwd36753	AnyConnect posture script does not run when the script condition name includes a period.
CSCwc36589	Cisco ISE Intune MDM integration might be disrupted due to the End of Support for MAC address-based APIs from Intune.
CSCwh18731	Upgrading to Cisco ISE Release 3.2 with LSD disabled before upgrade causes EP profiler exception.
CSCwc53824	Cisco ISE limits connection to AMP AMQP service to TLSv1.0.
CSCwf36285	Row of "Manage SXP Domain filters" only displays maximum 25.
CSCwf07855	Cisco ISE SXP bindings API call returns 2xx response when the call fails.
CSCwf82055	Unable to disable SHA1 for ports associated with passive ID agents.
CSCwf62744	ENH: Add "Disable EDR Internet Check" tag.
CSCwh28098	Cisco ISE Release 3.2 Patch 3: CoA Disconnect is sent instead of CoA Push during posture assessment with RSD disabled.
CSCwf14365	"Configuration Missing" warning is seen on the Log Analytics page.
CSCwe82004	TCP socket exhaustion.
CSCwe53550	Cisco ISE and CVE-2023-24998.
CSCwf71870	TACACS deployment with 0 days evaluation will not work after registering for smart licensing.
CSCwh46877	Need CoA Port-Bounce while removing ANC Policy with PORT_BOUNCE.
CSCwf62987	Vulnerabilities present in antisamy 1.5.9.
CSCwh32290	There is a mismatch between the FQDN value in the GUI and CLI after performing reset-configuration.
CSCwf42496	Attempting to delete "Is IPSEC Device" NDG causes all subsequent RADIUS/T+ authentications to fail.
CSCwc44622	Session gets stuck indefinitely until it restarts when NAD (Meraki) misbehaves.
CSCwh51136	Cisco ISE drops RADIUS request with the message "Request from a non-wireless device was dropped".
CSCwf33018	A fix to the bug CSCwd35608 is causing CoA calls from UI to be sent to the wrong IP address.
CSCwf44942	TACACS:PSN crashes during max user session authentication flow.
CSCwf19039	Cisco ISE Release 3.1 Patch 5: Agentless posture failures cause /tmp/ folder to increase in size.

Caveat ID	Description
CSCwf31477	Profiler triggers port bounce when multiple sessions exist on a switch port.
CSCwf55641	German and Italian emails are not saved under Account Expiration Notification in Guest Types.
CSCwh28528	TopN Device administration reports don't work when TACACS incoming messages exceed 40 million records per day.
CSCwe96739	TLS 1.0 and TLS 1.1 accept Cisco ISE Release 3.0 admin portal.
CSCwe95624	Cisco ISE Release 3.2 SNMP does not work after node restarts.
CSCwe03624	Smart license registration fails with "communication send error" alarms intermittently.
CSCwf81550	Cisco ISE changes the MAC address format according to the selected MAC address format even when it is unnecessary.
CSCwf54680	Unable to edit or delete authorization profiles with parentheses in their names.
CSCwh38484	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.
CSCwf35760	Ct_engine uses 100% CPU.
CSCwh39008	Unable to schedule or edit the schedule for configuration backup.
CSCwf60904	ANC remediation does not function with AnyConnect VPN.
CSCwh03227	Cisco ISE does not use a license when authorized with no authorization profile rule.
CSCwf80951	Unable to edit or create admin user due to "xwt.widget.repeater.DataRepeater" error.
CSCwe98676	Vulnerable JavaScript library issue found while executing ZAP.
CSCwd20521	Active Directory connector does not stop.
CSCwf59310	Cisco ISE Release 3.1 Patch 7 : Context Visibility : pxGrid ContextIn : Missing Custom Attributes.
CSCwh05647	Static IPv6 routes are removed after a reload in Cisco ISE Release 3.2.
CSCwh41693	Cisco ISEaaS: AWS - Support IMDS v2 issue.
CSCwh00049	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
CSCwh92366	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 Wi-Fi" 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
CSCwe61215	SFTP and FTP validation fails through CLI when password is configured with more than 16 characters.
CSCwf15717	ISE 3.2 - System 360 is not available only with Device Admin license.
CSCvr79992	Session.CurrentDate attribute is not calculated correctly during authentication.
CSCwe68336	Posture Assessment By Condition generates ORA-00904: "SYSTEM_NAME": invalid identifier.
CSCwe15315	TrustSec PAC Information Field attribute values are lost when network device CSV template file is imported.
CSCwf14957	TrustSec status cannot be changed if using Japanese UI in ISE.
CSCwe69085	PSN GUI is not accessible when only device administration license is enabled
CSCwd97022	ISE-PIC 3.2 p3 Smart Licensing Disabled PIC Upgrade is out of compliance.
CSCwd46505	ISE-PIC does not show Queue Link errors.
CSCwe24932	Agentless posture fails when using multiple domain users in the endpoint login configuration.
CSCwe54318	SXP service gets stuck into initializing due to H2 DB delay in querying bindings.
CSCvt62460	Unable to retrieve groups or attributes from different LDAPs when defined per node.
CSCwe49261	ISE PassiveID Agent probes the status of all domains even the ones without passiveID configuration.
CSCwd47111	ISE is unable to save the subnet or IP address pool name for voice vlans.

Caveat ID	Description
CSCwd79277	Sync status shows as failed when maximum trustsec objects are selected for sync.
CSCwf26973	Network Device Group information is missing when admin account is Read-Only.
CSCwd97606	Multiple requests for same IP+VN+VPN combinations with different session IDs creates duplicate records.
CSCwe07822	ISE date of last purge has wrong timestamp.
CSCwd90613	Radius Server Sequence page shows "no data available".
CSCwf28229	VLAN detection interval should not be more than 30 seconds.
CSCwd12357	SXP service gets stuck in initializing due to an exception on port 9644.
CSCwe59587	Some items are displayed as [Test] in Japanese display.
CSCwe37978	Scheduled report with huge size comes up as empty on the repository when exported.
CSCwe92640	ISE 3.1 and 3.2 - Validation is missing for existing routes during CLI configuration.
CSCwe43002	"Read-only Admin" is not available for ISE admin SAML authentication.
CSCwc93253	ISE - Network device captcha prompts only when filter matches one network device.
CSCwe64558	Admin account created from network access users cannot change dark mode setting.
CSCwf19463	Conditions Studio drag and drop layering.
CSCwc64346	ISE ERS SDK network device bulk request documentation is not correct.
CSCwe85828	Trust store does not update admin certificate after generating new admin certificate.
CSCwc47015	Fix for CSCvz85074 breaks AD group retrieval in ISE.
CSCwe52296	ISE MNT Auth Status API query should be optimized.
CSCwf33128	Radius used space reports incorrect usage as it also takes into account a few TACACS tables.
CSCwb83304	ISE upgrade fails because of custom security group.
CSCwc47799	ISE does not show any error when importing a certificate and private key when the password has % .
CSCwe11676	Data lost when accessing Total Compromised Endpoints in Cisco ISE dashboard Threat for TC-NAC.
CSCwe41695	ISE 3.1P4 and P5: Standalone ISE crashes if restarted after removing admin access restriction.
CSCwe80760	Unable to save launch program remediation when the parameter contains double quote ("").
CSCwe17954	Cisco Identity Services Engine Information Disclosure Vulnerability.
CSCwe70402	ISE 3.2 cannot handle portal customization scripts that include single-line JavaScript comments.
CSCwf40128	Accept client certificate without KU purpose validation as per CiscoSSL rules.
CSCwe52461	Unable to enable the firewall condition in ISE 3.1.

Caveat ID	Description
CSCwe96633	Support bundle does not contain tterrors.log and times.log.
CSCwf22799	Deferred Update condition does not work if compliance module is not compatible with Secure Client.
CSCwd39746	For SCCM integration with ISE need MSAL support as MS is deprecating ADAL.
CSCwe97989	ISE 3.2 crashes with VN in authorization profile.
CSCwe38800	Vulnerabilities in hibernate-validator - multiple versions.
CSCwe49167	ISE 3.2 SAML sign authentication request setting gets unchecked on being saved.
CSCwf33881	ISE 3.2 P1 establishes connections to servers not listed in ISE ports or resources reference guides.
CSCwf13630	Mnt Log Processor service stops every night.
CSCwe12098	ISE 3.2: Ports for Guest Portal configuration do not open on ISE nodes installed on AWS node.
CSCwe86793	ISE filter of REST ID Store Groups displays: Error Processing this request.
CSCwe40577	Failed to handle API resource request: Failed to convert condition.
CSCwe70975	In ISE the SMS Javascript Customization does not work for SMS email gateway.
CSCwe69179	ISE - latest IP access restriction configuration removes previous configuration.
CSCwf31073	ISE 3.1 OpenAPI Error 400 when device admin network conditions are fetched.
CSCwf33421	Update warning message while changing timezone.
CSCwe49422	From ISE 3.2, clear text passwords must be entered in the identity-store command.
CSCwf09393	Cisco ISE 3.1 services fail to start after restoring backup from old ISE version 2.7.
CSCwc70197	Cisco ISE Certificate API fails to return trusted certificate with hash character in friendly name.
CSCwf15130	Permission for collector.log file is set as root automatically.
CSCwe38610	Make MDM API V3 certificate string case insensitive.
CSCwc57240	GUI does not validate default value while adding custom attributes.
CSCwe55215	ISE smart licensing now uses smart transport.
CSCwf05309	ISE SAML certificate does not replicate to other nodes.
CSCwe83868	Vulnerabilities in spring-framework 5.1.3.
CSCwf34596	User Custom Attributes are stuck on rendering.
CSCwe78540	IotAsset information is missing when Get All Endpoints is invoked.
CSCwe43468	Static IP-SGT mapping with VN reference causes DNAC Group-Based Policy sync to fail.
CSCwc13859	Unable to create Scheduled backup with admin user from "System Admin" AdminGroup.

Caveat ID	Description
CSCwf26226	CPU spike due memory leak with EP purge call.
CSCwc20314	ISE-PIC 3.1 : PIC License : Consumption 0.
CSCwf40861	UI shows HTML hexadecimal code for the characters in the command set.
CSCwd55061	ERS API internal error seen while creating existing NDG.
CSCwe86494	ISE displays tomcat stacktrace when using a specific URL.
CSCwd41098	Getting pxGrid error logs in ise-psc.log after disabling pxGrid.
CSCwe41824	ISE 3.2 Missing S-PAN Key for PKI-based SFTP.
CSCwd82119	EAP-TLS authentication with ECDSA certificates fails on ISE 3.1.
CSCwf26482	REST AUTH services not running after upgrade from ISE 3.1 to version 3.2.
CSCwd05040	Unable to import certificates on secondary node post registration to the deployment.
CSCwf10004	ISE IP SGT static mapping is not sent to SXP domain on moving it to another mapping group.
CSCwe36242	TACACS Command Accounting report export does not work.
CSCwc85867	ISE Change Configuration Audit Report does not clearly indicate SGT create and delete events.
CSCwd70658	Unable to add Network Access Device. Reason: "There is an overlapping IP Address in your device" .
CSCwe99961	Sponsored Portal in Germany - Calendar shows Thursday (Donnerstag) as Di not Do.
CSCwf23981	ISE Authorization Profile displays wrong Security Group and VN value.
CSCwd73282	ISE 3.1 Patch 3 : Sponsor Portal : Session Cookie SameSite value set to none.
CSCwf09674	Registered Endpoint Report shows unregistered guest devices.
CSCwc85546	ISE 3.1 ENH "Illegal hex characters in escape (%) pattern ? for input string: ^F".
CSCwf17490	Post SL update, ISE licensing page shows evaluation compliance status for consumed licenses.
CSCwe30235	Vulnerabilities in jszip 3.0.0.
CSCwe84210	Authorization policy evaluation fails due to NullPointerException in LicenseConsumptionUtil.java.
CSCwe69189	LSD causes high bandwidth utilization.
CSCwb44638	Enhancement: To have separate log file with MNT DB metrics.
CSCwd31414	Guest portal displays "Error Loading Page" when reason for visit field contains special characters.
CSCwf21960	During upgrade the deregister call fails to remove all the nodes from the database.
CSCwe18371	Issues with ISE 3.2 admin access restriction.
CSCwe36063	No validation of PBIS reg key configuration on advance tuning page.

Caveat ID	Description
CSCwe63873	Qualys adapter is unable to download the knowledge base - Stuck in knowledge download in progress.
CSCwd97551	ISE cannot retrieve OU attributes from client certificate in EAP-TLS session resumption.
CSCwc80574	ISE AD Connector fails during join.
CSCwd68070	Import saml metadata fails.
CSCvx15522	DNSCache enabling command in FQDN syslog popup needs correction.
CSCwe37826	Unable to change the condition operator from AND to OR in posture policy condition.
CSCwe71729	ISE 3.2 : Data Connect password about to expired alarm every minute.
CSCwc57162	Certificate based GUI admin login stuck.
CSCwe39262	Passive D agent sends incorrect time format events.
CSCwd38136	Cisco Identity Services Engine Denial of Service Vulnerability.
CSCwd54844	ERS API schema for network device group creation.
CSCwe49183	ISE SAML destination attribute is missing for signed authentication requests.
CSCwe36788	ISE 3.2 Unable to delete the rules which are added during the time of adding IP access rule.
CSCvz86446	ISE Replication: SyncRequest timeout monitor thread does not kill file transfer after timeout.
CSCwe12618	ISE 3.2 : APIC Integration : com.cisco.cpm.apic.ConfImporter:521 - Failed to get EPs null.
CSCwe71804	ISE 3.1 - Key attributes are missing in SessionCache when third party network device profile is in use.
CSCwe34566	Authentication against ROPC identity store fails with RSA key generation error.
CSCwb79496	WMI status shows progress after mapping from agent protocol to WMI protocol.
CSCwe49504	Passwords with more than 16 characters are not supported in ISE 3.2 for identity-store configuration command.
CSCwe39781	ISE does not remove SXP mapping when SGT is changed after CoA.
CSCwe30606	Unable to download support bundle with size over 1GB from GUI.
CSCvv99093	ISE nodes intermittently trigger Queue Link alarms : Cause=Timeout.
CSCwf16165	NTP authentication key with more that 15 characters getting % ERROR: bad hashed key.
CSCwd89797	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
CSCwf59005	PEAP and EAP-TLS don't work on FIPS mode.
CSCwh92366	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 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 update 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 Identity Services Engine 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
CSCwe25138	Could not create Identity User if the user custom attribute includes $ or ++.
CSCwd45783	pxGrid session publishing stops when reintegrating FMC while P-PIC is down.
CSCwd70902	PRRT should be sending unfragmented messages to MnT if IMS is enabled to avoid merge.
CSCwd92324	ISE 3.2 ROPC basic serviceability improvements.
CSCwd84055	ISE 3.1 Azure AD Autodiscovery for MDM API V3 is incorrect.
CSCwd41218	Cisco Identity Services Engine Command Injection Vulnerability.
CSCwd27865	Configuration changed is not working when assigning an endpoint to a group.
CSCwd39056	ISE 3.1 P4 Passive DC configuration failing to save username correctly.
CSCwc91917	Can't add quotation character in TACACS authorization profile.
CSCwc62716	IndexRebuild.sql script ran over MnT.
CSCwe18371	Issues with ISE 3.2 Admin Access restriction.
CSCwd63661	Entering incorrect password on GUI shows end user agreement.
CSCwd97353	Automatic backup stops working after 3 - 5 days.
CSCwd71574	High CPU utilization when Agentless Posture is configured.
CSCwe27146	ISE 3.2 Patch 1: Unable to Parse CLI Admin Username with '-' (hyphen/dash).
CSCwd26845	APIC Integration missing fvIP subscription.
CSCwc65821	ERS API does not allow for use of minus character in "Network Device Group" name.
CSCwc39302	Interface status is showing UP even after shutdown.
CSCwd63749	AD Retrieve Groups shows a blank page when loading a huge number of AD groups (400+).
CSCwd71496	ISE not deleting sessions from All SXP Mapping table.

Identifier	Headline
CSCwd92835	Network Device Profile shows HTML code as name.
CSCwe07406	Error Loading Page error is shown when creating a guest account in the Self-Registered Guest portal.
CSCwd79277	Sync status shows as failed when maximum TrustSec objects selected for Sync.
CSCwa52678	GUI TCPDUMP gets stuck on Stop_In_Progress.
CSCwe00424	ISE- SQLException sent to the Collection Failure Alarm caused by NAS-Port-id length.
CSCwe14808	ISE fails to translate AD attribute of msRASSavedFramedIPAddress.
CSCwd98296	IP Addresses/Device Groups fields in Network Device Port Conditions page doesn't accept valid port strings.
CSCwd57978	All NADs are deleted when you filter network devices by IP and Location.
CSCwe37041	Internal CA Certificate Chain becomes invalid when original PPAN is removed.
CSCwc64480	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).
CSCwd22790	URI not accepted as Group attribute or as Name in Assertion of attributes for SAML IdP in ISE 3.1/3.2.
CSCvy69943	Allow Guest Portal HTTP Requests containing Content-headers with {} characters.
CSCwe07354	Radius Token Server config accepts empty host IP for Secondary Server.
CSCwd57071	Self-reg portal does not support nodes FQDNs for the Approve/Deny links sent to the sponsors.
CSCwd24286	ISE not sending hostname attribute to DNAC.
CSCwe44750	Re-profiling result is not saved in Oracle and VCS DB after feed incremental update.
CSCwc79321	Unable to change the Identity source from internal to external RSA/RADIUS-token server.
CSCwd74560	PUT operation failing with payload via DNAC to ISE (ERS).
CSCwe63320	ISE displays mismatched information on "Get All Endpoints" report.
CSCwc57294	Duplicate Manager does not remove packet when there is an exception in reading config.
CSCwe33360	Anomalous behavior detection is not working as expected.
CSCwd82134	Incorrect SLR out of compliance error reported in ISE.
CSCwe37018	ISE-DNAC integration fails if there are invalid certificates in ISE Trusted Store.
CSCwc48311	ISE vPSN with IMS performance degrades by 30-40% compared to UDP syslog.
CSCwe13780	Unable to join node to AD by REST API if we configure a specific OU.
CSCwd93002	Getting Null System Error while editing the groups and adding Name in Assertion under SAML.
CSCwd31524	16-character passwords are not supported in ISE 3.2 for sftp configuration.

Identifier	Headline
CSCwe02315	Online Page level Help IDs for meraki-connector pages in ISE GUI.
CSCwd41651	Vertical Scrollbar bug in ISE 3.1.
CSCwd69072	Session directory write failed alarm with Cisco NAD using "user defined" NAD profile.
CSCwe15576	Not able to configure KRON Job.
CSCwc55529	Authentication failed due to missing certificate private key.
CSCwc07082	"The phone number is invalid" error message seen when trying to import users from csv file.
CSCwd87161	Certificate based login asks for license file if only the Device Admin license is enabled.
CSCwe34204	ISE upgrade tab shows upgrade in progress after installing patch.
CSCwe22934	ISE Authentication latency from devices with no mac address.
CSCwd63717	PKI-enabled SFTP repositories not working in ISE 3.2.
CSCwb85502	CIAM: xstream 1.4.17.
CSCwc99816	ISE openAPI restore shows Completed_With_Success 25 minutes before CLI command "show restore status" does.
CSCwe45245	Smart license registration is not working properly.
CSCwd51812	When using certificate based authentication, attempt to access ISE GUI results in access permission error.
CSCwe13110	Configuration backup executed on Primary MnT node.
CSCvg66764	Session stitching support with ISE PIC agent.
CSCwd74898	"Posture Configuration detection" alarms should be "INFO" level and reworded.
CSCwd64649	Cisco DNA Center integration issue due to multiple internal CA certificates.
CSCwe13947	OpenAPI for EP create/update should work same as ERS API in addition to providing more functionality.
CSCwe57764	MDM Connection to Microsoft SCCM fails after Windows DCOM Server Hardening for CVE-2021-26414.
CSCvo61351	Live session get stuck at "Authenticated" state.
CSCwe74108	Cisco AI Analytics doesn't work with Proxy configured as IP Address.
CSCwd97582	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
CSCwf25955	A match authorization profile with SGT, VN name, VLAN fields empty causes port to crash.
CSCwf40128	Accept client certificate without KU purpose validation per CiscoSSL rules.
CSCwf02093	In Cisco ISE Release 3.2, hyper-V installations have DHCP enabled.
CSCwe92640	Cisco ISE Releases 3.1 and 3.2: Missing validation for existing routes during CLI configuration.
CSCwf32255	No response received from SNMP server when the "snmp-server host" is configured in Cisco ISE Release 3.2 patch 2.
CSCwe95624	In Cisco ISE Release 3.2, the SNMP is not working following a node restart.
CSCwe69179	The latest IP access restriction configuration removes the previous configuration in Cisco ISE.
CSCwe36788	In Cisco ISE Release 3.2, users are not able to delete the rules which were added during IP access rule addition.
CSCwe41695	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.
CSCwf55795	In Cisco ISE Release 3.2 Patch 1, the Cisco ISE GUI and CLI are inaccessible following a configuration restoration with ADE-OS.
CSCwd97551	Cisco ISE cannot retrieve multiple attribute values from the client's certificate in EAP-TLS session.
CSCwh92366	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
CSCwd13425	Patch install from UI fails.
CSCwc74531	ISE hourly cron should cleanup the cached buffers instead of the 95% memory usage.
CSCwc80243	ISE TCPDUMP stuck at "COPY_REPO_FAILED" state when no repository is selected.
CSCwc85920	ISE TrustSec Logging - SGT create event is not logged to ise-psc.log file.
CSCwc33751	ISE 3.1 TFTP copy times out.
CSCwc53895	ISE 3.1 patch 3 SAML SSO doesn't work if active PSN is down.
CSCwc65802	Save button for SAML configuration grayed out.

Caveat ID	Description
CSCwc99178	Not able to add too many Authorization Profiles with active session alarm setting.
CSCwd10997	Node syncup fails to replicate wildcard certificate with the portal role.
CSCwc69492	Metaspace exhaustion causes crashes on ISE node.
CSCwb62192	Scheduled backup failure when ISE indexing engine backup failed.
CSCwd05697	Guest locations do not load in the ISE Guest Portal.
CSCwc62415	Cisco Identity Services Engine Unauthorized File Access Vulnerability.
CSCwa37580	ISE 3.0 NFS share stuck.
CSCwb77915	Toggle to enable/disable RSA PSS cipher based on policy under Allowed Protocols.
CSCvv10712	Sec_txnlog_master table should be truncated post 2 million record count.
CSCwc62413	Cisco Identity Services Engine Cross-Site Scripting Vulnerability.
CSCwc76720	Error with SNMPv3 privacy password in ISE 3.1.
CSCwd35608	ISE is sending old Audit Session ID in reauthentication CoA after successful port-bounce CoA.
CSCwc62419	Cisco Identity Services Engine Insufficient Access Control Vulnerability.
CSCwc44580	ISE 3.1 creates cni-podman0 interface with IP 10.88.0.1 and ip route for 10.88.0.0/16.
CSCwc61320	Slowness in the Support Bundle page due to Download Logs page loading in the background.
CSCwc98833	Cisco Identity Services Engine Cross-Site Scripting Vulnerability.
CSCwc98831	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability.
CSCwc95878	Intermittent issues with App activation or App not receiving events.
CSCwd13555	ISE abruptly stops consuming passive-id session from a third party Syslog server.
CSCwd32591	ISE 3.2 SFTP repositories not operational from GUI after clicking "generate key pairs".
CSCwd51409	ISE cannot retrieve repositories and scan policies of Tenable Security Center.
CSCwd24304	ISE 3.2 ERS POST /ers/config/networkdevicegroup fails due to broken attribute othername/type/ndgtype.
CSCwd03009	RMQForwarder thread to control based on hardware Appliance in platform.properties.
CSCwc81729	"All devices were successfully deleted" message displayed while trying to delete a NAD by filtering.
CSCwb16640	ISE 3.2 Authorization Profile does not persist VLAN name string for SDA SG-VN-VLAN use case.
CSCwc42712	ISE RADIUS and PassiveID session merging.
CSCwd15888	Not able to access Time Settings Configuration Export on ERS API.
CSCwc15013	Add serviceability and fix "Could not get a resource since the pool is exhausted" error in ISE 3.0.

Caveat ID	Description
CSCwc87670	ISE 3.1 patch 3 unable to import endpoints from csv file if SAML is used.
CSCwa55233	"Unknown CA" Queue Link error when using third-party signed certificate for IMS.
CSCwd73787	CLI password change doesn't persist in Confd DB after "password" command.
CSCwd42311	Unable to download rest-id-store from Download Logs on GUI.
CSCwc50392	ROPC AD groups retrieval is not working with 53k and above groups.
CSCwc50944	The change of profiling policy name is not reflected in the policy set conditions.
CSCwc95075	"File path field must contain a valid file name" error when configuring file conditions for posture.
CSCwc75572	PPAN application server stuck at initializing state.
CSCwd22790	ISE 3.2 can't save Group Membership attribute for SAML service provider.
CSCwd27506	ISE 3.0 patch 6 missing scheduled reports.
CSCwc74206	ISE 3.0 not saving SCCM MDM server object with new password, works when new instance is used.
CSCwd31405	Latency observed during query of Session.PostureStatus.
CSCwd45843	Authentication step latency for policy evaluation due to GC activity.
CSCwc60997	SAML flow with load balancer is failing due to incorrect token handling.
CSCwc49580	ANC CoA is sent to the NAS IP address instead of the Device IP address.
CSCwb26965	Getting error while creating network device groups via REST API.
CSCwc23593	LSD is causing high CPU usage.
CSCwc48509	Windows Server 2022 is actually working as the target domain controller to be monitored.
CSCwb72948	ISE 3.0 patch 4 unable to access system certificates page for the registered node.
CSCwc93451	Profiler should ignore non-positive RADIUS syslog messages for forwarding from default RADIUS probe.
CSCwc98828	Cisco Identity Services Engine Interface Feature Insufficient Access Control Vulnerability.
CSCwd24089	ISE 3.2 Safe mode not enabled.
CSCwd16837	ISE openAPI HTTP repo patch install fails when dir listing is disabled.
CSCwd31137	ISE scheduled radius authentication reports failed while exporting to SFTP repository.
CSCwc98824	Posture Requirements only show the default entry.
CSCwd30994	Static default route with gateway of interfaces other than Gig 0 breaks network connectivity.
CSCwc98823	Cisco Identity Services Engine Command Injection Vulnerability.

Caveat ID	Description
CSCwd41773	Application server crashes if CRL of size 5 MB or more is downloaded frequently.
CSCwc88848	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
CSCwd79277	Sync status shows as failed when maximum TrustSec objects are selected for sync.
CSCwd89797	Exception error messages seen when Debug log level is enabled on meraki-connector.
CSCwd93002	System Error : Null while editing the groups and adding Name in Assertion under SAML.
CSCwd93209	Sync Cycle does not end when meraki-connection is deleted from ISE.
CSCwe02315	Page level online help for Meraki Connector is not available.
CSCwe01771	Dashboards created using the changed Time fields:acs_timestamp would not show up after patch install.
CSCwh92366	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.

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

Caveat ID	Description
CSCwm05210	Getting '500 internal error' when sending ISE 9060/ers/config/endpoint/{MAC address}/releaserejectedendpoint.

Resolved Caveats in Cisco ISE Release 3.2

The resolved caveats in Cisco ISE Release 3.2, have parity with these Cisco ISE patch releases: 2.7 Patch 7, 3.0 Patch 6, and 3.1 Patch 3.

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

Caveat ID Number	Description
CSCwb77915	Toggle to enable/disable RSA PSS cipher based on policy under Allowed Protocols.
CSCvz85117	Cisco ISE Health Check I/O bandwidth performance check false alarm.
CSCwb29140	Threads getting exhausted post moving to the latest patches where the nss rpm is updated.
CSCwb59357	Cisco ISE ova ztp attempts HTTP directs listing of contents.
CSCvz18848	Agentless posture breaks for locale.
CSCwb82814	Cisco ISE Release 3.1 OpenAPI giving a 400 error when fetching Nested Conditions.
CSCwa61347	Cisco ISE-PIC not forwarding live sessions beginning with special characters.
CSCvz13747	SystemTest: Cisco ISE primary administration node GUI page not opening after PAN failover.
CSCvz66577	SMS Javascript customization is not working for SMS email gateway.
CSCvy81435	Cisco ISE Guest SAML authentication fails with "Access rights validated" HTML page.
CSCwb23853	Unable to add SAML ID provider on Cisco ISE 3.1 patch 1 when doing a configuration restore from an older Cisco ISE release.
CSCvy99582	When upgrading from Cisco ISE Release 2.4 patch 13 to Cisco ISE 2.7 if external RADIUS server configuration upgrade will fail.
CSCwa96229	Cisco ISE is allowing user to change admin password without validating the current password.
CSCwb36849	Cisco ISE must avoid sending empty Cisco AV-Pairs in access-accept packets.
CSCwa20152	CoA was not initiated on Cisco ISE for switches for which matrix wasn’t changed, hence the policy sync failed.
CSCvy94553	TACACS authentication report shows duplicate entries.
CSCvv54351	Device administration using RADIUS does not consume base license.
CSCvz50059	Cisco ISE GC_APP Logs are not auto-rotating or deleting from the local disk.
CSCwc99178	Unable to add many authorization profiles with active session alarm setting.
CSCvu21809	TEAP (EAP-TLS) with EAP-chaining is not using the configured CN for AD lookups.
CSCvz79665	Microsoft Intune graph URL change from graph.windows.net/tenant to graph.microsoft.com.
CSCwc39320	Upgraded Cisco ISE nodes via CLI method gets stuck in "Upgrading" status on the primary administration node GUI.
CSCwa35293	Cisco ISE 2.7: Authentication success settings shows success/success URL.
CSCwb92006	Having single quote in middle of the password on proxy settings causes page to become un-editable.
CSCvz88188	TACACS authorization policy querying for username fails because username from session cache is null.

Caveat ID Number	Description
CSCwc50944	The change of profiling policy name is not reflected on the policy set conditions automatically.
CSCvw58039	Cisco ISE does not show report for client provisioning when AC is updated on the endpoint through Cisco ISE.
CSCwb33727	Cisco ISE 3.1: Special character in attributes not supported.
CSCwa26210	The next page field is missing from the JSON response of API 'GET /ers/config/radiusserversequence'.
CSCwc18751	Unable to download a created support bundle from the Cisco ISE GUI if we login using format DomainName\UserName.
CSCwb24002	The authentication settings of the Cisco ISE ERS SDK is not disabled via API call.
CSCwa88845	Device port network conditions does not validate interface ID.
CSCvy66496	REST ID cannot filter groups based on name or SID for Azure AD groups.
CSCwa94984	Cisco ISE API add user operation with long custom attribute string takes 4min using Curl
CSCvz44655	Cisco ISE manage account selection issue.
CSCwb56878	The Replication Stopped alarm is triggered in Cisco ISE.
CSCvz77905	Cisco ISE RADIUS service denial of service vulnerability.
CSCwa11653	CIAM: linux-kernel 4.18.0.
CSCwa78479	Cisco Identity Services Engine Assessment of CVE-2021-4034 Polkit
CSCwa20354	Operational data purging and database utilization node information does not show intermittently.
CSCvv87286	Fail to import Internal CA and key from Cisco ISE Release 2.7 Patch 2 to Cisco ISE Release 3.0.
CSCvz08813	Unable to scroll to different pages in the Issued Certificates page.
CSCvz07191	Cisco ISE GUI is stuck at loading if the AD group does not exist when using certificate based authentication for Cisco GUI access.
CSCwb92643	Cisco ISE ADE-OS CLI TCP params fail to make changes and are no longer relevant.
CSCvz28133	User unable to generate support bundle.
CSCwa55996	New objects do not exist in the conditions studio.
CSCwc09435	Error handling or messaging for the mobile number format is not clear.
CSCvx59893	Inconsistency between Cisco ISE syslog level and message level.
CSCwa16401	Get-By-ID server sequence, returns empty server list after first change made on the sequence via Cisco ISE GUI.
CSCwc40959	In dark mode of Cisco ISE Release 3.2, the Internal Users have a color that is difficult to read.

Caveat ID Number	Description
CSCwc26241	Cisco ISE Release 3.2 displays the error: "TypeError: Cannot read properties of undefined (reading 'attr')".
CSCwa48465	Reports are unusable due to mishandling fields with multiple values.
CSCwb01843	DST/TZ update should happen automatically.
CSCvx54894	Sponsor Portal admin unable to create random guest accounts for 60 minutes or 1 hour duration or less.
CSCwb75964	Cisco ISE Release 3.0: Unable to edit primary administration node auto failover alarms.
CSCwb32244	No possibility to edit certificate imported to Cisco ISE Trusted Certificate.
CSCwa89443	Cisco DNA Center - Cisco ISE Integration: Cisco ISE shows an old Cisco DNA Center certificate for pxGrid endpoint.
CSCvz27791	Cisco ISE: Application server stuck initializing after backup restore due to MDM configuration.
CSCwa14268	Vulnerability assessment for CVE-2021-35619 on Oracle DB.
CSCwa97123	NTP sync failure alarms with more than 2 NTP servers configured.
CSCvy51210	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.
CSCvz37241	Move queue link error from WARN to Critical and Restart if there is a timeout.
CSCwa40040	Session Directory Write failed, SQLException: String Data right truncation on Cisco ISE 3.0 Patch 4.
CSCvy53842	Certificate validation syslog message sent during specific certificate audits in Cisco ISE.
CSCvz01485	In Cisco ISE 2.7 patch 4, users are unable to upload .json file for Umbrella security profile.
CSCwc23997	Cisco ISE is showing incorrect VLAN assignment information in authorization profile and attributes details.
CSCwb95433	"File path field must contain a valid file name" error when configuring file conditions for posture.
CSCvz78841	CIAM: openssh 7.6.
CSCvz90468	Internal users using external password store are getting disabled if we create users using API flow.
CSCwa06912	High latency observed for TACACS+ requests with date and time condition in authorization policies.
CSCwb01568	Cisco ISE on AWS: Operational DB not sized properly based on a larger OS disk.
CSCvy76328	IPV6 changes the Subnet to /128 when using the duplicate option from Network device tab.
CSCvz56358	Cisco ISE Release 3.0 checks only the first SAN entry.
CSCwc85920	Cisco ISE TrustSec Logging - SGT create event is not logged to ise-psc.log file.
CSCwc61320	Slowness on support bundle page due to the Download Logs page loading in the background.
CSCvw93570	Cisco ISE Release 2.4 patch 8 is unable to edit, duplicate or delete guest portals.

Caveat ID Number	Description
CSCwa20309	Unknown NAD and misconfigured network device detected alarms.
CSCwc21890	Passive easy connect does not work in Cisco ISE with dedicated monitoring nodes.
CSCwb29498	High operations DB usage alarm percentage need to be configurable.
CSCwc69492	Cisco ISE 3.1: Metaspace exhaustion causes crashes on Cisco ISE node.
CSCwb48707	Unable to load the Endpoint Purge tab.
CSCvz44488	Cisco ISE 3.0 agentless posture does not use domain authentication if same local user exists.
CSCvt25277	Cisco ISE 2.4 patch 12 install is stuck.
CSCvz68091	Configuration changes to guest types is not updated in audit reports.
CSCwa32312	RCM and MDM flows getting failed because of session cache not populated.
CSCwa37040	Backup-logs using public key encryption on the Cisco ISE CLI does not allow for capture of core files.
CSCwb61614	Guest users (AD or internal) cannot delete or add their own devices on specific node.
CSCvs95495	Reauthorization issue in Aruba third party device.
CSCwb27894	EAP-TEAP with EAP-TLS unable to match condition that has "CERTIFICATE.Issuer - Common Name".
CSCvz49871	Cisco ISE GUI: net::ERR_ABORTED 404: /admin/ng/nls/fr-fr/.
CSCwa33462	CSV NAD import is rejected due to special symbol @ at the beginning of RADIUS shared secret.
CSCwc44580	Cisco ISE 3.1 creates cni-podman0 interface with IP 10.88.0.1 and IP route for 10.88.0.0/16.
CSCvx23375	Cisco ISE authorization profiles option get truncated during editing or saving (in Google Chrome only).
CSCwb41741	Cisco ISE - Invalid character error in Admin Groups.
CSCwb27857	Cisco ISE Release 3.0 Patch 5: Unable to login into the Cisco ISE GUI of MnT nodes using RSA 2FA in distributed deployment.
CSCwa09060	Unable to assign the role to externally signed system cert bound by CSR in Cisco ISE 3.1 Patch 1.
CSCvz72225	Adding FQDN in discovery host- Discovery host: invalid IP address or host name.
CSCwa13696	Cisco ISE Release 3.1 Guest Username or Password Policy is not modifiable.
CSCwb39638	Unable to import Network Device configured with SNMPv3 SHA2 authorization.
CSCwa23207	Multiple runtime crashes seen due to memory allocation inconsistency.
CSCwb52396	Cisco ISE PRA failover.
CSCvy94511	TACACS report showing duplicate entries due to EPOCH time being null.
CSCvz77482	Cisco ISE Release 3.0 can't deselect the 'location' settings as part of the guest self registration portal.

Caveat ID Number	Description
CSCwb59170	Cisco ISE Release 3.1 SHA-2 option is not available for NAD creation via REST API.
CSCwc62415	Cisco Identity Services Engine Unauthorized File Access Vulnerability.
CSCwc76720	Error with SNMPv3 Privacy Password on Cisco ISE Release 3.1 only.
CSCwb42924	Unable to get message option in Posture remediation actions.
CSCwb35304	Cisco ISE Release 3.1: Race condition causes registration/sync failure.
CSCwa47190	AD security groups cannot have their OU end with dot character on Posture Policy.
CSCvz57222	Cisco ISE Release 3.0: Admin access is allowed for Cisco ISE GUI with secondary interfaces GigabitEthernet 1 and Bond 1.
CSCwb52092	AWS Cloud Formation stack for Cisco ISE Release 3.1 fails with very strong admin password.
CSCwa18443	Need to handle Posture expiry when 8 octet MAC is present in endpoint on the deployment node.
CSCwa83517	Guest portal registration page gives "error loading page" when email address contains apostrophe.
CSCvi35653	Bi-directional communication/UDP heart-beat between Cisco ISE and AnyConnect Cisco ISE Posture.
CSCwb19256	Pingnode call causing app server to crash (OOM exception) during CRL validation.
CSCwc31482	NetworkSetupAssistance.exe digital signature certificate expired in BYOD flow using Windows SPW.
CSCwa57955	Posture firewall remediation action unchangeable.
CSCwb48388	Licensing only displays one reserved count if licenses reserved in CSSM have multiple expiry dates.
CSCwa25731	Last 7 days filter not working in Reports.
CSCwb97579	Cisco ISE Release 3.1 compatibility problems with Hyper-V Gen-2.
CSCwc74206	Cisco ISE Release 3.0 not saving SCCM MDM server object with new password, works when new instance is use.
CSCvy33393	Cisco ISE 3.1 BH Context visibility shows \\ in username whereas live logs show correct single \.
CSCwb26965	Cisco ISE Release 3.1: Getting error while creating network device groups via REST API.
CSCvz18627	PEAP session timeout value restricted to max 604800.
CSCwa78042	Cisco ISE Release 3.1 is requesting ISE-PIC licenses from smart account.
CSCwa91335	Default domain configuration in Passive-Syslog provider does not work in Cisco ISE Release 3.1.
CSCvz73445	Agentless Posture not passing AntiMalware check.
CSCvz63643	Cisco ISE Release 2.7: EndpointPersister thread getting stopped.
CSCwb21669	Unable to enter IPV6 address for on-prem SSM server.

Caveat ID Number	Description
CSCwa17470	Cisco ISE Release 3.1 SAML admin authentication failing with Access Denied if 2+ groups in the group claim.
CSCwa49859	Attribute value dc-opaque causing issues with Live Logs.
CSCvz72034	Cisco ISE Release 3.1:When updating network device from Cisco DNA Center shared secret/password is empty or masked.
CSCvz83204	Cisco ISE unable to fetch the URL attribute value from improper index during posture flow.
CSCwc53577	Parent user identity group can be created via CSV file.
CSCwb71505	Cisco ISE Release 3.1: Application server stuck in initializing state due to ACE library error.
CSCvz74457	Cisco ISE ERS API does not allow for use of dot character in "Network Device Group" name or create or update.
CSCwc07283	Context visibility endpoint authentication tab is not showing data in Cisco ISE Release 3.1.
CSCvy94427	Posture lease breaks for EAP chaining from Cisco ISE Release 2.7.
CSCvy71690	Customer fields in the guest portal contains & - $ #.
CSCwa95889	Cisco ISE: SSH/SFTP to Hosts w/ Newer HostKey algorithms (e.g. rsa-sha2-512).
CSCvy91805	Maximum sessions are not being enforced with EAP-FAST-Chaining in Cisco ISE.
CSCwd05697	Guest locations do not load in Cisco ISE Guest Portal.
CSCwc88848	Cisco ISE Release 3.1 Patch 1 does not create the Rest ID/ROPC folder logs.
CSCvy69539	CIAM: openjdk - multiple versions.
CSCwb34910	Multi-line issues for Guest SMS notification under Cisco ISE portal.
CSCvy92536	Cisco ISE Release 3.0: Device Admin license alone should allow access to Administration > System > Logging.
CSCwb02129	SSH to Cisco ISE failing on any SSH public keys manually imported.
CSCwb32466	Cisco ISE Release 3.1: Unable to delete endpoint identity group created via REST API when setting no description.
CSCvy86859	Mac OS Beta Monterey (MacOS 12 beta 2) failing NSP MacOsXSPWizard v3.1.0.2.
CSCwa04454	Cisco ISE Releases 3.0 & 3.1: Device Admin License alone should allow access to all TACACS required menus.
CSCwc08484	Disabling Open TAC case leads to Cisco ISE Integrity Check failure on Cisco ISE service restart.
CSCvz07823	Cisco ISE Release 2.7 failed to add endpoint to group.
CSCwc49580	ANC COA is sent to the NAS IP address instead of the Device IP address.

Caveat ID Number	Description
CSCwc87670	Cisco ISE Release 3.1 patch 3 is unable to import endpoints from .csv file if SAML is used.
CSCwd31405	Latency observed during query of Session.PostureStatus.
CSCwb30941	CVE-2022-0778 - Cisco ISE Release 3.1 and above is affected.
CSCwb85456	CIAM: OpenSSL upgrade to 1.0.2ze and 1.1.1o.
CSCwc65802	Save button for SAML configuration grayed out.
CSCvy84989	Enabling cookies for POST /ers/config/internaluser/ causes Identity Group(s) does not exist error.
CSCwc12693	Cisco ISE ERS Validation Error- Mandatory fields missing: [validDays].
CSCvz33839	Menu access customization is not working.
CSCwb91392	Health check and full upgrade precheck time out when third party CA certificate is used for the admin.
CSCvz75902	Cisco ISE replacing pxGrid cert when generating Cisco ISE internal CA.
CSCvz65182	If we set MTU greater than 1500 then the MTU value is not setting persistently across reboot.
CSCvu94544	Cisco ISE 3.0 BH: TACACS live logs do not give an option select Network Device IP.
CSCwc09104	Guest redirect with Auth vlan no longer works on Cisco ISE Release 3.1.
CSCvz17020	Cisco ISE GUI shows all the licenses as Out of Compliance - Smart Licensing.
CSCwa45316	MDM intune integration broken for vpn user on Cisco ISE Release 3.1.
CSCwd10840	Cisco ISE CLI is stuck.
CSCwb88851	Inconsistent IP to SGT mapping after several re-authentications when VN value is changing.
CSCvz63405	Cisco ISE client pxGrid certificate is not delivered to Cisco DNA Center.
CSCwb75093	CIAM: linux-kernel 4.18.0
CSCvy92040	Cisco ISE restore popup menu displays wrong text.
CSCvz72208	Cisco ISE Release 3.1: Authentication tab shows blank result in Context Visibility.
CSCwc21400	HTTP 400 response in Repo OpenAPI when an SFTP/FTP repo user password contains ! (exclamation mark).
CSCwa79799	Missing PermSize attribute on sysodbcini file.
CSCvn27270	Cisco ISE: Cannot create network device group with name Location or Device Type.
CSCvz43183	Sponsor permissions are not passed to guest REST API for "By Name" calls.
CSCwc59570	Cisco ISE sending SXP MSG size > 4096 bytes in SXP version 4.
CSCwa67433	Cannot export SAML provider info xml file from the Cisco ISE GUI.

Caveat ID Number	Description
CSCwc24126	Profiler condition not displaying the attribute value.
CSCwa97357	Cisco ISE is not sending "mobilenumber" value in the SMTP API body.
CSCvz61191	Cisco ISE Release 3.1: No response when click "choose file" on import endpoints from CSV file page.
CSCwb94890	Key Performance Metrics report has no entries for 8 AM and 9 AM every day.
CSCwb09045	Cisco ISE policy service nodes crashing due to incorrect cryptoLib initialization.
CSCwb11147	Improvement to logs needed with conflict handling SGT-IP mapping w/VN.
CSCwa46758	Deleted root network device groups are still referenced in the network devices exported CSV report.
CSCwc81729	"All devices were successfully deleted" after trying to delete one particular NAD by filtering.
CSCvz20851	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerability.
CSCvu94025	Cisco ISE should either allow IP only for syslog targets or provide DNS caching.
CSCvz71284	SNMPv3 COA request is not issued by Cisco ISE Release 2.7.
CSCwa90930	Need hard Q cap on RMQ.
CSCvx85675	Cisco ISE can't handle deletion/addition of SXP-IP mappings propagation due to race condition.
CSCwb04898	Unable to restore CFG backup from linux SFTP repository if the file owned by a group name w/ space.
CSCwb57665	Cisco ISE evaluation for Struts2 CVE-2021-31805.
CSCwc48509	Windows Server 2022 is actually working as the target domain controller to be monitored.
CSCvz94133	Configuration backup fails due to "EDF_DB_LOG".
CSCvw90586	Unable to change network device group name and description at the same time.
CSCwa51150	WLC failed to validate EAPOL Key M2 with Cisco ISE Release 3.1.
CSCwb82141	Context visibility endpoints and NADs from an existing deployment are not removed after restore.
CSCvs55875	Existing routes are not installed in routing table after MTU change.
CSCwa47566	Cisco ISE Conditions Studio: Identity Groups drop-down limited to 1000.
CSCwb91645	Cisco ISE TrustSec Dashboard Refresh Call causing high CPU on MnT.
CSCvz34849	DELETE /ers/config/networkdevicegroup/{id} not working; CRUD exception.
CSCvz65945	"Invalid Length" TACACS authorization failures within live logs for non-TACACS traffic.
CSCwb38069	Cisco ISE Release 3.1: Services failed to start after restoring backup from old Cisco ISE Release 2.6.
CSCvy16894	Authorization profile will throw an error if we use some symbols.

Caveat ID Number	Description
CSCwa13877	Cisco ISE Smart Licensing Authorization Renewal Failure: Details=Invalid response from licensing cloud.
CSCwa76896	Duplicated column "Failure Reasons" in RADIUS Authentications Report.
CSCwa47133	Cisco ISE Evaluation log4j CVE-2021-44228.
CSCvy66598	MAR feature should be ignored in case of MAB authentication.
CSCwa17718	Session service unavailable for pxGrid Session Directory with dedicated MnT.
CSCwc05718	Cisco ISE Debug Wizard Posture profile does not contain client-webapp component to DEBUG.
CSCwb05532	Location of "Location" and "Device Type" exchanging every time clicking Network Devices > Add.
CSCwb22662	64-character limit is too small to accommodate external user identities, such as user principal name.
CSCvz83753	Empty user custom attribute included in AuthZ advanced attributes settings results in incorrect AVP.
CSCwa75348	ODBC behavior failover issues.
CSCwb81416	Cisco ISE Release 3.1 GUI not loading post login.
CSCwb40349	Cisco ISE 3.X: Invalid characters in external RADIUS token shared secret.
CSCvz67073	Cisco Identity Services Engine Authentication Bypass Vulnerability.
CSCwb62192	Scheduled backup failure when Cisco ISE indexing engine backup failed.
CSCwb01854	Upgrade External RADIUS server list not showing up after upgrading to Cisco ISE Release 3.0 or later.
CSCvz05704	Platform check fails for Cisco ISE having disk size more than 1TB.
CSCwa43187	Cisco ISE Queue Link Error: Message=From Node1 To Node2; Cause=Timeout in NAT'ed deployment.
CSCwb47255	Supported HTTP methods are visible.
CSCvz00258	SessionCache not cleared for TACACS AuthZ failures results in high heap usage and authentication latency.
CSCwb86283	Cisco ISE Deployment: All nodes thrown OUT_OF_SYNC as a result of incorrect certificate expiry check.
CSCwa19573	Catalina.out file is huge because of SSL audit events.
CSCwb82469	Windows 11 Pro for Workstations is indeed not supported yet in the latest posture feed update.
CSCvw90778	T+ ports (49) are still open if disable device admin process under deployment page.
CSCvz55258	Cisco:cisco-av-pair AuthZ conditions stopped working.
CSCwa52110	SNMP config set on the N/w device, a delay of 20 seconds is introduced while processing SNMP record.
CSCvz00659	Special characters in Banner blocking SFTP repository.

Caveat ID Number	Description
CSCwc65711	MAC - CSC 5.0554 web deployment packages fails to upload to ISE > CP > resources[100MB].
CSCvz45150	Cisco ISE Release 3.1 requests a traditional license.
CSCwc27765	Cisco ISE configuration backup fails due to SYS_EXPORT_SCHEMA_01.
CSCwa59237	Deployment-RegistrationPoller causing performance issues on PAN node with 200+ internal certificates.
CSCwa38023	Cisco ISE Release 3.1: Unable to generate pxGrid certificates with Active Directory super admin.
CSCwb57675	Cannot disable "Dedicated MnT" option from the Cisco ISE GUI once it is enabled.
CSCwa82553	Cisco ISE Release 3.1 default route is on the incorrect interface if bonding is configured.
CSCwa04370	Cisco ISE Release 3.1: Default route removed or tied to wrong interface after upgrading.
CSCwa32814	Cisco ISE Configured with 15 Collection Filters Hides the 15th Filter.
CSCwa60873	Optimize bouncy-castle class to improve performance on primary administration node.
CSCwc42712	Cisco ISE RADIUS and PassiveID session merging.
CSCvz46560	Cisco ISE using jquery v1.10.2 is vulnerable.
CSCwc53895	Cisco ISE Release 3.1 Patch 3 SAML SSO doesn't work if active policy service node goes down.
CSCvz79518	Serviceability: "DNS Resolution Failure" alarm should show Cisco ISE server.
CSCvz08319	Cisco ISE application server process is restarting during Dot1X due to buffer length = 0 for EAP TLS.
CSCwa08484	Missing IPv4 mappings if sessions have both IPv4 and IPv6 addresses
CSCwb23028	Inaccurate dictionary word evaluation for passwords.
CSCvy45345	EAP-chaining authorization failure due to machine authentication flag set to true incorrectly.
CSCvz38266	ADFS SAML login to work with FQDN same as Okta.
CSCwd10997	Node syncup fails to replicate wildcard certificate with the portal role.
CSCwb98854	Cisco ISE does not update expiry date after updating SLR license.
CSCvy96761	Session cache needs to be updated during EAP chaining flow to handle relevant identities.
CSCvy69900	CIAM: linux-kernel 4.18.0.
CSCwa37580	Cisco ISE Release 3.0 NFS share stuck.
CSCwb84779	Changing Parent Identity Group name breaks authorization references.
CSCwb00530	Android VPN and InTune MDM integration not working on Cisco ISE Release 3.1.
CSCvx85064	Enable ability to modify SMS content when sponsornet guest self-reset password.
CSCwa16291	Guest Portal's Button's text element is causing words to be repeated for Apple VoiceOver.

Caveat ID Number	Description
CSCwa03126	Cisco ISE CPP not loading correctly in some languages.
CSCwa36350	Hotpatch API details have blank timestamp.
CSCvz90852	Hotspot Guest Portals in CNA with blank Success and not switched to done on iDevices.
CSCwc57939	Cisco ISE detects large VMs as unsupported.
CSCwa57705	IP-SGT mapping does not link with new network access device group.
CSCvz92898	SCM js files browser download during admin login.
CSCwa05404	Stale sessions observed for TACACS could not find selected service error.
CSCwb37760	Sponsor Portal getting error 500 when enabling "Allow kerberos SSO" portal setting.
CSCvz72069	pxGrid shown disabled on Summary page for Cisco ISE-PIC.
CSCwd13555	Cisco ISE abruptly stops consuming passive-id session from a third party syslog server.
CSCvz95326	Unable to add more than one ACI IP address/hostname when trying to enable ACI integration in Cisco ISE.
CSCwa08018	Cisco ISE Release 3.1 - The Cisco ISE GUI is not working when IPV6 is disabled globally.
CSCvy76622	SystemTest: Android BYOD flow with EST and StaticIP/Hostname/FQDN fails.
CSCwb03479	Hotpatch.log needs to be included in support-bundle.
CSCvv43120	Cisco ISE 2.x: Intune MDM Alarm for connectivity || 401 Unauthorized.
CSCwb84440	Sponsor portal breaks after removing endpoint groups.
CSCwa00729	All NADs are deleted due to one particular NAD deletion.
CSCwa82247	Cisco ISE Queue Link Error: Cause=Timeout due to 169.254.2.0/25 in Cisco ISE IPtables.
CSCwb39964	Cisco ISE can login to the Cisco ISE GUI with disabled shadow admin accounts with external identity source.
CSCwb07504	Sorting internal users based on User Identity Groups does not work in Identity Management > Identities.
CSCvz93230	Guest portal does not load if hosted on a different interface from Gig0.
CSCwa53499	REST ID is fetching the groups from cloud once the connector settings page is opened.
CSCwa56771	Cisco ISE Release 3.0 patch 2- Monitor all setting displays incorrectly with multiple matrices and different views.
CSCwa60903	ISE is adding extra 6 hours to nextUpdate date for CRL
CSCwa41166	Unsafe characters in T+ commands stored in Hex Numeric Character References.
CSCwa55866	TACACS responses are not sent sometimes with single connect enabled.

Caveat ID Number	Description
CSCvo39514	MnT log processor is not running because collector log permission.
CSCwb40942	From address to send email is invalid if it does not end with .com or .net.
CSCvk25808	Unable to edit or remove Scheduled Reports if admin who created them is no longer available
CSCwb53455	RMQ TLS syslogs related to internal docker IP 169.254.2.2 are sent to audit logs.
CSCvz57267	Inability to import Cisco ISE certificates issued for primary administration node to other nodes in spite of the SAN field FQDN.
CSCvz20020	Okta redirection fails for first ID store and works when second ID store is assigned.
CSCwc51219	CSV NAD import is rejected if += characters are at the beginning of the RADIUS shared secret.
CSCvz60870	High Active Directory latency during high TPS causes HOL Blocking on ADRT.
CSCwb02346	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerability.
CSCvy43246	User unable to create a guest SSID during Portal Creation step - Cisco ISE is busy is the error displayed.
CSCwb93156	TrustCertQuickView giving the same info for all trusted certificates.
CSCvz86020	Live log/session not showing latest data due to "too many files open" error.
CSCwa95892	ui_time_left variable showing wrong duration
CSCwc33850	Unable to export certificate with private key using API.
CSCwc11613	Certificate signing request should not be case sensitive.
CSCwc60997	Cisco ISE: SAML flow with loadbalancer is failing due to incorrect token handling on Cisco ISE.
CSCwb40131	Getting 400 Bad Request while enabling the Internal User with external password type using Rest API.
CSCwa11633	Cisco ISE Release 3.0: APIC Integration: Failed to create secGroup.
CSCwb32492	Application server restart on all nodes after changing the Primary Administration certificate.
CSCwc00162	Certificate based admin login not working when client/browser send more than one certificate.
CSCwb79056	Cisco ISE Release 3.1 ERS call /ers/config/sgmapping/{id} doesn't return SGT value for custom SGTs.
CSCwc62413	Cisco Identity Services Engine Cross-Site Scripting Vulnerability.
CSCvv02086	Add ability to disable TLS 1.0 and 1.1 on Cisco ISE PIC node.
CSCvy94818	EP's incorrectly profiled as "cisco-router" due to NMAP performing aggressive guesses.
CSCvz35550	Cisco ISE Health Check MDM Validation false alarm.
CSCwc03220	Removing an IP Access list from Cisco ISE destroys the distributed deployment.
CSCwc30811	Underscore is vulnerable in Guest Portals.

Caveat ID Number	Description
CSCvz05966	In Cisco ISE Release 2.6 patch 9, default permissions can't go back to default group Internal after adding a new group.
CSCwc30643	My Devices Portal doesn't open after reloading the node unless we do CRUD.
CSCwa47221	AD security groups cannot have their OU end with dot character on client provisioning policy.
CSCwa59621	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.

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)