Release Notes for Cisco Identity Services Engine, Release 3.1

First Published: 2021-08-03

Last Modified: 2026-09-21

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 TrustSec solution and supports TrustSec software-defined segmentation.

Cisco ISE is available on secure network server appliances with different performance characterizations, and also as software that can be run on a virtual machines (VMs). Note that you can add more appliances to a deployment for better performance.

Cisco ISE has a scalable architecture with centralized management and control. It supports both standalone with high availability and distributed deployment. 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 3.1?

This section lists the new and changed features in Cisco ISE release 3.1.

Table 1: New and changed information

Date	Description
2026-09-15	General availability of Cisco ISE release 3.1 cumulative patch 12.
2026-04-27	General availability of Cisco ISE release 3.1 cumulative patch 11.
2025-01-29	General availability of Cisco ISE release 3.1 cumulative patch 10.
2024-05-21	General availability of Cisco ISE release 3.1 cumulative patch 9.

Date	Description
2023-12-05	General availability of Cisco ISE release 3.1 cumulative patch 8.
2023-05-26	General availability of Cisco ISE release 3.1 cumulative patch 7.
2023-03-30	General availability of Cisco ISE release 3.1 cumulative patch 6.
2022-12-09	General availability of Cisco ISE release 3.1 cumulative patch 5.
2022-09-22	General availability of Cisco ISE release 3.1 cumulative patch 4.
2022-05-02	General availability of Cisco ISE release 3.1 cumulative patch 3.
2021-12-07	General availability of Cisco ISE release 3.1 cumulative patch 1.
2021-08-03	General availability of Cisco ISE release 3.1.

New features in Cisco ISE release 3.1 cumulative patch 12

There are no new features in Cisco ISE release 3.1 cumulative patch 12.

New features in Cisco ISE release 3.1 cumulative patch 11

Allow server EKU certificates for Cisco pxGrid

Cisco ISE will support using server certificates with only the server authentication EKU for Cisco pxGrid. This update ensures your services remain compatible with new public CA standards.

For more information, refer to Allow server EKU certificates for Cisco pxGrid.

New features in Cisco ISE release 3.1 cumulative patch 10

Blast RADIUS vulnerability fix

To address the Blast RADIUS vulnerability reported in CSCwk67747, the **Message Authenticator Required On Response** check is introduced in **External RADIUS Server**, **RADIUS Token ID Store**, and **Device Profile**.

This check box is not enabled by default after a patch upgrade. Once the check box is enabled, Cisco ISE will not validate any packet that lacks a **Message-Authenticator** attribute in the response, causing the RADIUS flow to fail.

For more information, see the topics "Network Device Profiles Settings" and "External RADIUS Server Settings" in the chapter *Threat Containment* and the topic "Add a RADIUS Token Server" in the chapter *Asset Visibility* in the *Cisco ISE Administrator Guide, Release 3.1*.

Security Identifiers in certificates will not be used for authentication

Cisco ISE supports a new certificate format that includes Security Identifiers (SID) in the Subject Alternative Name (SAN) fields. SIDs in the SAN field will not be used for authentication, helping to prevent authentication failures caused by incorrect SID parsing.

Cisco ISE supports these SAN_URI field formats in certificates:

- SID and ID or GUID separated by a comma (in either order):

- <tag,sid>,<ID><GUID>
- <ID><GUID>,<tag,sid>

- SID and ID or GUID separated by a colon (in either order):
  - <tag,sid>:<ID><GUID>
  - <ID><GUID>:<tag,sid>

- Only SID present:
  - <tag,sid>

- Only ID and GUID present:
  - <ID><GUID>

All newer Microsoft certificates include the SID in the SAN_URI with the format:

tag:microsoft.com,2022-09-14:sid:<SID>.

New features in Cisco ISE release 3.1 cumulative patch 9

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. 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. By using this option, you can reduce the reinstallation time from an average of 5-7 hours, to approximately 1-2 hours.

For more information, see "Localized ISE Installation" in the Chapter "Cisco ISE CLI Commands in EXEC Mode" in the *Cisco Identity Services Engine CLI Reference Guide, Release 3.1*.

New features in Cisco ISE release 3.1 cumulative patch 8

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 3.1 Patch 8, Microsoft Intune only provides the following endpoint details in response to compliance APIs:

- Device compliance status
- Managed by Intune
- MAC address
- Registration status

For more information on these changes, see *Integrate MDM and UEM Servers with Cisco ISE*.

Wi-Fi device analytics data from Cisco Catalyst 9800 wireless LAN controller

You can create profiling policies, authorization conditions, and authentication conditions and policies for Apple, Intel, and Samsung endpoints, using device analytics data from the Cisco Wireless LAN Controllers integrated with your Cisco ISE.

For more information, see "Wi-Fi Device Analytics Data from Cisco Catalyst 9800 Wireless LAN Controller" in the Chapter "Asset Visibility" in the Cisco ISE Administration Guide, Release 3.1.

New features in Cisco ISE release 3.1 cumulative patch 7

Link external LDAP users to Cisco ISE endpoint groups

From Cisco ISE Release 3.1 Patch 7, you can assign external LDAP user groups to Endpoint Identity Groups for guest devices using the **Dynamic** option. For more information, see "Create or Edit Guest Types" in the chapter "Guest and Secure WiFi" in the *Cisco Identity Services Engine Administrator Guide, Release 3.1*.

New features in Cisco ISE release 3.1 cumulative patch 6

Bulk update and bulk delete support for context-in API in pxGrid Cloud

From Cisco ISE Release 3.1 Patch 6, you have context-in API support in pxGrid Cloud for bulk updation and bulk deletion of endpoints. For more information, see the Cisco pxGrid Cloud Onboarding Guide and the Cisco ISE API Reference Guide.

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 3.1 patch 6 and later versions support Cisco SNS 3700 series appliances. Hence, you cannot rollback to ISE 3.1 after installing the first patch (ISE 3.1 patch 6 or later) on an SNS 3700 series appliance. Rollback will fail in this case. You can re-install ISE 3.1 patch 6 or later from the CLI to recover the node.

New features in Cisco ISE release 3.1 cumulative patch 5

Automatically assign logical profiles to endpoints

When an endpoint goes through Cisco ISE profiling workflows, if the endpoint matches an endpoint profiling policy with an associated logical profile, the endpoint is automatically assigned the logical profile.

Support for Cisco Secure Client

Cisco ISE 3.1 Patch 5 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.

pxGrid Cloud support for Context-in

From Cisco ISE release 3.1 cumulative patch 5, 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.

Required URL for smart licensing

Cisco ISE release 3.1cumulative patch 5 uses https://smartreceiver.cisco.com to obtain smart licensing information.

New features in Cisco ISE release 3.1 cumulative patch 4

Changes to IP default gateway require restart

Cisco ISE release 3.1 cumulative patch 4 onwards, when you add or change a gateway, the CLI warns the administrator that service restart may be required, and proceeds to execute the comand only if the Yes option is selected.

For more information, see the Cisco ISE CLI Commands in Configuration Mode chapter in the *Cisco ISE CLI Reference Guide, Release 3.1*

Enhancement to the groups tab in the REST identity store

You can now retrieve, filter, and delete REST identity store groups while configuring Resource Owner Password Credentials in Cisco ISE.

While adding the groups, click **Retrieve Groups** to import the user groups from the connected identity source. Check the check boxes next to the groups that you want to select and click **Save**. You can also select all the groups, if needed. The selected groups are listed in the Groups tab.

You can filter the results using the filter option.

To delete a user group, check the check box next to the group that you want to delete and click Delete.

For more information, see "Configure Resource Owner Password Credentials Flow" in the Chapter "Asset Visibility" in the *Cisco ISE Administrator Guide, Release 3.1*

.

New features in Cisco ISE release 3.1 cumulative patch 3

Microsoft Intune integration changes due to Microsoft Graph updates

Microsoft is deprecating Azure Active Directory (Azure AD) Graph and will not support Azure AD Graph-enabled integrations after June 30, 2022. You must migrate any integrations that use Azure AD Graph to Microsoft Graph. Cisco ISE typically uses the Azure AD Graph for integration with the endpoint management solution Microsoft Intune.

For more information on the migration from Azure AD graph to microsoft graph, see the following resources:

- Migrate Azure AD Graph apps to Microsoft Graph
- Azure AD Graph to Microsoft Graph migration FAQ
- Update your applications to use Microsoft Authentication Library and Microsoft Graph API

Cisco ISE release 3.1 patch 3 supports Microsoft Intune integrations that use Microsoft Graph. To avoid any disruption in the integration between Cisco ISE and Microsoft Intune, update your Cisco ISE to Cisco ISE Release 3.1 Patch 3. Then, update your Cisco ISE integration in Microsoft Azure to use Microsoft Graph instead of Azure AD Graph, before June 30, 2022. In Cisco ISE, you must update your Microsoft Intune integrations to update the **Auto Discovery URL** field—Replace **https://graph.windows.net<*Directory (tenant) ID*>** with **https://graph.microsoft.com**.

See Connect Microsoft Intune to Cisco ISE as a Mobile Device Management Server for more information on the configuration steps.

Opening TAC support cases in Cisco ISE

You can now open TAC Support Cases for Cisco ISE and other Cisco products 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 3.1*.

SHA1 ciphers disabled by default

From Cisco ISE relase 3.1 patch 2, SHA1 ciphers on port 443 are disabled by default.

Support for Cisco pxGrid Cloud

Cisco ISE release 3.1 patch 3 supports Cisco pxGrid Cloud. Cisco pxGrid Cloud is a new Cisco cloud offer that extends pxGrid, ERS and OpenAPI access to cloud-based applications. To allow connectivity between a Cisco ISE deployment and Cisco pxGrid Cloud, pxGrid Cloud service must be enabled on one or more pxGrid nodes in the Cisco ISE deployment. For more information on Cisco pxGrid Cloud, see Cisco pxGrid Cloud Solution Guide.

Update of OCSP responder certificates

From Cisco ISE release 3.1 cumulative patch 3 onwards, the following rules are applicable for the renewal of OCSP certificates:

- For a multi-node Cisco ISE deployment, OCSP certificates are renewed automatically if you install the patch through the Cisco ISE GUI. If you install the patch through the Cisco ISE CLI, we recommend you to renew the OCSP certificate manually.
- For a standalone Cisco ISE deployment, OCSP certificates are renewed automatically irrespective of whether you install the patch through the Cisco ISE GUI or the Cisco ISE CLI.
- If you uninstall Cisco ISE release 3.1 patch 3, you have to renew the OCSP certificate manually.

  This one-time OCSP certificate renewal process is because of the change in certificate hierarchy. For more information, see Update of OCSP Responder Certificates in the "Basic Setup" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 3.1*.

New features in Cisco ISE release 3.1 cumulative patch 1

Cisco ISE on AWS

- The software version Cisco ISE release 3.1 patch 1 is available on Amazon Web Services (AWS).
- You can now install Cisco ISE in evaluation mode in the AWS instance named t3.xlarge. For more information about using Cisco ISE in evaluation mode in AWS, see the section "Cisco ISE Evaluation Instance on AWS" in the *Cisco ISE Installation Guide, Release 3.1*.

  t3.xlarge instances only support Cisco ISE release 3.1 patch 1 and later releases.

OpenAPI service

The following OpenAPIs have been introduced in Cisco ISE Release 3.1 Cumulative Patch 1:

- License
- Generate Self-Signed Certificate
- Patch and Hot Patch
- Deployment

For more information, see "Enable API Service" in the Chapter "Basic Setup" in *Cisco ISE Administrator Guide, Release 3.1*.

Signed SAML authentication request for Cisco ISE

Cisco ISE now only accepts signed SAML requests and assertions for authentication.

For more information, see "Configure SAML ID Provider" in the Chapter "Asset Visibility" in *Cisco ISE Administrator Guide, Release 3.1*.

New features in Cisco ISE release 3.1

Cisco ISE on AWS

- The software version Cisco ISE release 3.1 patch 1 is available on Amazon Web Services (AWS).
- You can now install Cisco ISE in evaluation mode in the AWS instance named t3.xlarge. For more information about using Cisco ISE in evaluation mode in AWS, see the section "Cisco ISE Evaluation Instance on AWS" in the *Cisco ISE Installation Guide, Release 3.1*.

t3.xlarge instances only support Cisco ISE release 3.1 patch 1 and later releases.

OpenAPI service

The following OpenAPIs have been introduced in Cisco ISE Release 3.1 Cumulative Patch 1:

- License
- Generate Self-Signed Certificate
- Patch and Hot Patch
- Deployment

For more information, see "Enable API Service" in the Chapter "Basic Setup" in *Cisco ISE Administrator Guide, Release 3.1*.

Signed SAML authentication request for Cisco ISE

Cisco ISE now only accepts signed SAML requests and assertions for authentication.

For more information, see "Configure SAML ID Provider" in the Chapter "Asset Visibility" in *Cisco ISE Administrator Guide, Release 3.1*.

Android settings for native supplicant profile

Android settings are added for native supplicant profile. You can select one of the following options for Certificate Enrollment Protocol:

- Enrollment over Secure Transport (EST)
- Simple Certificate Enrollment Protocol (SCEP)

If you choose the EST protocol, Cisco ISE will ask for additional password inputs from Android users while issuing certificates.

For more information, see "Native Supplicant Profile Settings" in the Chapter "Compliance" in the *Cisco ISE Administrator Guide, Release 3.1*.

Enhancements in audit logs

The following audit logs have been enhanced to include more details about relevant events:

- Posture audit logs now include information regarding:
  - Creation and deletion of posture policies.
  - Changes made to existing posture policies, such as changes in fields such as **Conditions**, **Rule Name**, and so on.
  - Addition, deletion, or modification in posture configurations such as **Conditions**, **Remediation Actions**, **Requirements**, and so on.
- RBAC audit logs now include information regarding creation and deletion of existing menu access and data access content.
- Network Access and Admin Users audit logs now include information regarding creation, edition, and deletion of Network Access and Admin Users.

Posture state synchronization

You can configure AnyConnect to probe Cisco ISE at specified intervals when the posture status is not compliant. This helps prevent a client from being stuck in pending state.

The posture state synchronization is supported for Windows, Linux, and MacOS clients.

For more information, see "Posture State Synchronization" in the Chapter "Compliance" in the *Cisco ISE Administrator Guide, Release 3.1*.

Obtain configuration backup using Cisco support diagnostics connector

You can use Cisco support diagnostics connector to trigger configuration backup and upload the backup files to the Cisco support diagnostics folder. After uploading the backup files to the Cisco support diagnostics folder, you can delete the backup files from the Cisco ISE local disk. To use this feature, you must enable smart licensing and Cisco Support Diagnostics in Cisco ISE.

For more information, see "Obtain Configuration Backup Using Cisco Support Diagnostics Connector" in the Chapter "Troubleshoot" in the *Cisco ISE Administrator Guide, Release 3.1*.

Configuration of authorization result alarm

You can configure alarms based on the results of authorization policies. This allows you to monitor the impact of any networking, infrastructure, or application changes on endpoint authorizations. You can define the scope of your alarms by choosing specific Network Device Groups (NDGs). For each NDG you choose, a new Authorization Result alarm is created.

You can filter the authorization logs to be monitored for an alarm by choosing specific authorization profiles and Security Group Tags (SGTs). Only endpoints that have met authorization policy sets with the specified authorization profiles and SGTs are monitored by the alarm.

For more information, see "Configure Authorization Result Alarm" in the Chapter "Troubleshoot" in the *Cisco ISE Administrator Guide, Release 3.1*.

Configuration of preferred domain controllers

You can specify the domain controllers that you want to use in case of domain failover. If a domain fails, Cisco ISE compares the priority scores of the domain controllers that are added to the preferred list and selects the one with the highest priority score. If that domain controller is offline or is not reachable because of an issue, the next one in the preferred list with the highest priority score is used. If all the domain controllers in the preferred list are down, a domain controller outside the list is selected based on the priority score. When the domain controller that was used before the failover is restored, Cisco ISE switches back to that domain controller.

For more information, see "Configure Preferred Domain Controllers" in the Chapter "Asset Visibility" in the *Cisco ISE Administrator Guide, Release 3.1*.

Context visibility enhancements

- In the **Export Endpoints** dialog box, you can now check the **Importable Only** check box if you want to export only the attributes that can be imported to Cisco ISE without any modification to the CSV file. Using this option prevents the need to modify the columns or metadata in the exported CSV file before importing it to Cisco ISE.
- While using the **Quick Filter** or **Advanced Filter** option, you can use the **Export Filtered** option to export only the filtered endpoints.

For more information, see "Export Endpoints Using CSV File" in the Chapter "Asset Visibility" in the *Cisco ISE Administrator Guide, Release 3.1*.

Full upgrade and split upgrade options added to Cisco ISE GUI

In the **Administration > System > Upgrade > Upgrade Selection** window, you can choose one of the following options based on your requirements:

- **Full Upgrade**: Full upgrade is a multistep process that enables a complete upgrade of your Cisco ISE deployment sequentially. This upgrades all the nodes in parallel and in lesser time compared to the split upgrade process. Because all the nodes are upgraded parallelly, services will be down during the upgrade process.
- **Split Upgrade**: Split upgrade is a multistep process that enables the upgrade of your Cisco ISE deployment while allowing services to remain available during the upgrade process for users. With the split upgrade option, you will be able to choose the nodes to be upgraded.

For more information, see "Upgrade a Cisco ISE Deployment from the GUI" in the Chapter "Upgrade Method" in *Cisco Identity Services Engine Upgrade Journey, Release 3.1*.

Cisco ISE on Amazon Web Services

You can launch a Cisco ISE instance on the Amazon Web Services (AWS) platform using a Cloud Formation Template (CFT) or an Amazon Machine Image (AMI).

For more information, see the Chapter "Install Cisco ISE with AmazonWeb Services" in *Cisco ISE Installation Guide, Release 3.1*.

Virtual appliance licenses

Cisco ISE release 3.1 and later supports the Cisco ISE VM license. This license replaces the VM Small, VM Medium, and VM Large licenses from earlier releases. The new Cisco ISE VM license covers Cisco ISE VM nodes for both on-premises and cloud deployments.

For more information, refer to "Cisco ISE Licenses" in the chapter "Licensing" in the *Cisco ISE Administrator Guide, Release 3.1*.

Download or upload files from local disk

You can easily add, download, or delete the files that are used for local disk management.

For more information, see "Download and Upload Files from Local Disk" in the Chapter "Maintain and Monitor" in the *Cisco ISE Administrator Guide, Release 3.1*.

MacOS versions in posture policy configurations

In Cisco ISE 3.0 and earlier, you could configure posture policies and requirements with minor MacOS versions such as MacOS 11.1, MacOS 11.2, and so on. In Cisco ISE 3.1, you can only choose major MacOS versions such as MacOS 11 (All) to configure posture policies and requirements.

When you upgrade to Cisco ISE 3.1, any posture condition that includes a minor MacOS version is automatically updated to the corresponding major MacOS version. For example, a posture condition that was configured for MacOS 11.1 will be updated to MacOS 11 (All).

OpenAPI service

OpenAPIs are REST APIs based on HTTPS operating over port 443. From Cisco ISE 3.1 onwards, newer APIs are available in the OpenAPI format. For more information on Cisco ISE OpenAPIs, see https://<*ise-ip*>/api/swagger-ui/index.html.

The following OpenAPIs have been introduced in Cisco ISE 3.1:

- Repository Management
- Configuration Data Backup and Restore
- Certificate Management
- Policy Management
  - RADIUS Policy
  - TACACS+ Policy

For more information, see "Enable API Service" in the Chapter "Basic Setup" in *Cisco ISE Administrator Guide, Release 3.1*.

Posture support for Linux operating system

Posture is a service in Cisco ISE that allows you to check the state of all the endpoints that are connecting to a network for compliance with corporate security policies. Cisco ISE release 3.1 supports the following Linux operating system versions, in addition to Windows and Mac operating systems:

- Ubuntu
  - 18.04
  - 20.04
- Red Hat
  - 7.5
  - 7.9
  - 8.1
  - 8.2
  - 8.3
  - 8.4
  - 8.5
  - 8.6
  - 8.7
  - 8.8
  - 8.9
  - 9.0

- 9.1
- 9.2
- 9.3

- SUSE
  - 12.3
  - 12.4
  - 12.5
  - 15.0
  - 15.1
  - 15.2

The following posture conditions are supported for Linux operating system:

- File Condition
- Application Condition
- Antimalware Condition
- Patch Management Condition

You can configure agent profiles for Linux clients. You can add client-provisioning resources for AnyConnect Linux clients.

For more information, see the Chapter "Compliance" in *Cisco ISE Administrator Guide, Release 3.1*.

ERS service auto enabled on VMware cloud environment

The External RESTful Services (ERS) API service is enabled by default when the Amazon Machine Image (AMI) version of Cisco ISE is deployed on a VMware cloud environment. This helps in easy integration of Cisco ISE with other Cisco products and third-party applications, without the need to enable the ERS service from the Cisco ISE GUI.

For more information, see "Enable API Service" in the Chapter "Basic Setup" in the *Cisco ISE Administrator Guide, Release 3.1*.

pxGrid client auto approval API

pxGrid can be used to share context-sensitive information from the Cisco ISE session directory with other network systems such as Cisco ISE ecosystem partner systems and other Cisco platforms. The pxGrid client auto approval API can be used to:

- Enable automatic approval of certificate-based connection requests from new pxGrid clients. Enable this option only when you trust all the clients in your environment.
- Enable username or password-based authentication for the pxGrid clients. When this option is enabled, pxGrid clients cannot be automatically approved. A pxGrid client can register itself with the pxGrid controller by sending the username through a REST API. The pxGrid controller generates a password

for the pxGrid client during client registration. An administrator can approve or deny the connection request.

For more information about the PxGrid Client Auto Approval API, see the “pxGrid Settings” section in the ERS SDK. You can access the ERS SDK with the following URL:

https://<*ISE-Admin-Node*>:9060/ers/sdk



Note Only users with ERS Admin role can access the ERS SDK.

Configuration of maximum password attempts for Active Directory account

You can configure the badPwdCount attribute to prevent active directory account lockout due to too many bad password attempts. Before authenticating the user, Cisco ISE compares the maximum bad password attempts configured in Cisco ISE with the current value of the badPwdCount attribute on active directory. When the maximum bad password attempts configured in Cisco ISE is equal to the value of the badPwdCount attribute, the authentication is dropped and not sent to active directory.

For more information, see "Configure Maximum Password Attempts for AD Account" in the Chapter "Asset Visibility" in the *Cisco ISE Administrator Guide, Release 3.1*.

Handle random and changing MAC addresses with mobile device management servers

As a privacy measure, mobile devices and some desktop operating systems increasingly use random and changing MAC addresses for each SSID that they connect to. In Cisco ISE, you can now work around this problem by configuring Cisco ISE to use a unique device identifier called GUID instead of MAC addresses. When an endpoint enrolls with a Mobile Device Management (MDM) server, the MDM server sends a certificate with a GUID value to the endpoint. The endpoint uses this certificate for authentication with Cisco ISE. Cisco ISE receives the GUID for the endpoint from the certificate. All communications between Cisco ISE and the MDM server now use the GUID to identify the endpoint, ensuring accuracy and consistency between the two systems.

For more information, see "Handle Random and Changing MAC Addresses With Mobile Device Management Servers" in the Chapter "Secure Wired Access" in *Cisco ISE Administrator Guide, Release 3.1*

MAC randomization for BYOD

Android and iOS devices increasingly use random and changing MAC addresses for each SSID that they connect to. Cisco ISE and MDM systems see different MAC addresses for the same device depending on which SSID they use to connect to the service. Therefore, a unique identifier is generated by the Cisco ISE Provisioning service to identify these endpoints.

For more information, see "MAC Randomization for BYOD" in the Chapter "Basic Setup" in *Cisco ISE Administrator Guide, Release 3.1*.

Endpoint API enhancement

The **logicalProfileName** filter can be used to get endpoints that belong to a specific Logical Profile. The supported operator for logicalProfileNamefilter is EQ (equal to). The syntax to invoke the API with this filter is:

/ers/config/endpoint?filter={filter name}.{operator}.{logical profile name}

For more information, see Cisco ISE API Reference Guide.

Posture script remediation

You can create and upload posture remediation scripts to Cisco ISE to resolve non-compliance issues in endpoints.

For more information, see "Add a Script Remediation" in the Chapter "Compliance" in *Cisco ISE Administrator Guide, Release 3.1*.

RHEL 8.2 support

Cisco ISE runs on the Cisco Application Deployment Engine Operating System (ADEOS), which is based on Red Hat Enterprise Linux (RHEL). For Cisco ISE 3.1, ADEOS is based on RHEL 8.2.

RHEL 8.2 supports the following VMware ESXi versions:

- VMware ESXi 6.5
- VMware ESXi 6.5 U1
- VMware ESXi 6.5 U2
- VMware ESXi 6.5 U3
- VMware ESXi 6.7
- VMware ESXi 6.7 U1
- VMware ESXi 6.7 U2
- VMware ESXi 6.7 U3
- VMware ESXi 7.0
- VMware ESXi 7.0 U1
- VMware ESXi 7.0 U2
- VMware ESXi 8.0

For more information, see the Chapter "Overview" in *Cisco Identity Services Engine Upgrade Journey, Release 3.1*.

SAML-based admin login

SAML-based admin login adds a single sign on capability to Cisco ISE using the SAML 2.0 standard. You can use an external Identity Provider such as Okta or any identity provider that implements SAML 2.0.

For more information, see "SAML-based Admin Login" in the Chapter "‘Asset Visibility" in *Cisco ISE Administrator Guide, Release 3.1*.

Specific license reservation

Specific license reservation is a smart licensing method for managing licenses in situations where security requirements prevent a persistent connection between Cisco ISE and the Cisco Smart Software Manager (CSSM). Specific license reservation allows you to reserve licenses on a Cisco ISE node.

You can create a specific license reservation by defining the type and number of licenses you need to reserve. Then, activate the reservation on a Cisco ISE node. The Cisco ISE node, where you register and enable the reservation, tracks license usage and enforces license compliance.

For more information, refer to "Specific license reservation" in the chapter "Licensing" in the *Cisco ISE Administrator Guide, Release 3.1*.

Upgrade to pxGrid 2.0

From Cisco ISE release 3.1, all pxGrid connections must be based on pxGrid 2.0. pxGrid 1.0-based (XMPP-based) integrations will cease to work on Cisco ISE from release 3.1 onwards.

pxGrid Version 2.0, which is based on WebSockets, was introduced in Cisco ISE Release 2.4. We recommend that you plan and upgrade your other systems to pxGrid 2.0-compliant versions in order to prevent potential disruptions, if any, to integrations.

For more information, see the Chapter "pxGrid" in *Cisco ISE Administrator Guide, Release 3.1*.

Note The output of **show application status ise** command reflects only the status of pxGrid 1.0 services.

Zero touch provisioning

Zero Touch Provisioning (ZTP) refers to the uninterrupted provisioning mechanism that helps to automate Cisco ISE installation, infrastructure service enablement, patching, and hot patching without manual intervention.

For more information, see "Zero Touch Provisioning" in the Chapter "Additional Installation Information" in *Cisco ISE Installation Guide, Release 3.1*.

Cisco Secure Access Control System-to-Cisco ISE migration tool

The Cisco Secure Access Control System-to-Cisco ISE Migration Tool is not supported for Cisco ISE 3.1 and later. End-of-life dates have been announced for Cisco Secure Access Control System. For more information, see End-of-Life Notice.

New and changed APIs in Cisco ISE

For detailed information on new, changed, and deprecated APIs, see the Cisco ISE API Guide on Cisco DevNet.

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*.

Verified Hardware

Cisco ISE 3.1 can be installed on the following platforms:

Table 2: Verified 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)	

Note

- Cisco ISE 3.1 Patch 6 and later versions support Cisco SNS 3700 series appliances.
- Cisco ISE 3.1 does not support the Cisco Secured Network Server (SNS) 3515 appliance.
- Memory allocation of less than 16 GB is not supported for VM appliance configurations. In the event of a Cisco ISE behavior issue, all the users are required to change the allocated memory to at least 16 GB before opening a case with the Cisco Technical Assistance Center.

After installation, you can configure Cisco ISE with specific component personas such as Administration, Monitoring, or pxGrid on the platforms that are listed in the above table. In addition to these personas, Cisco ISE contains other types of personas within Policy Service, such as Profiling Service, Session Services, Threat-Centric NAC Service, SXP Service for TrustSec, TACACS+ Device Admin Service, and Passive Identity Service.

Verified virtual environments

Cisco ISE supports these virtual environment platforms:

Table 3: Verified virtual environments

Virtual environment	Support details
VMware	• VMware 7.0.3 or later. • ISO files support ESXi 7.0 and ESXi 8.0. • OVA templates support VMware version 14 or later on ESXi 7.0 and ESXi 8.0. • In the case of vTPM devices, you must upgrade to VMware ESXi 7.0.3 or later releases. • You can use the VMware migration feature to migrate 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.
VMware Cloud Solutions on public cloud platforms	• AWS: Host Cisco ISE on a software-defined data center provided by VMware Cloud on AWS. • Azure VMware Solution: Runs VMware workloads natively on Microsoft Azure. • Google Cloud VMware Engine: Runs software-defined data center by VMware on Google Cloud.
Microsoft Hyper-V	• Supports Microsoft Windows Server 2012 R2 and later. • Supports Azure Stack HCI 23H2 and later. The virtual machine requirements and the installation procedure for the Cisco ISE VMs in the Azure Stack HCI are the same as that of Microsoft Hyper-V.
KVM on QEMU	• Supports QEMU 2.12.0-99 and later.
Nutanix	• Supports Nutanix 20230302.100169 and later.
Public cloud platforms	• Native support for Amazon Web Services (AWS), Microsoft Azure Cloud, and Oracle Cloud Infrastructure (OCI).
Red Hat OpenShift	• Red Hat OpenShift container platform 4.19 and later. • Cisco ISE must be deployed on OpenShift platform using the standard Cisco ISE ISO image. Deploying Cisco ISE using OVA templates is not supported.

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). Cisco ISE 3.1 Patch 1 or later is required. For details about the FIPS compliance claims, refer to Global Government Certifications.

When FIPS mode is enabled on Cisco ISE, follow these considerations:

- 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.

  These protocols are not supported in FIPS mode for RADIUS:

  - EAP-MD5
  - PAP
  - CHAP
  - MS-CHAPv1
  - MS-CHAPv2
  - LEAP

Verified and supported browsers

Cisco ISE release 3.1 is supported on these browsers:

- Mozilla Firefox 123, 125, 127, and later
- Mozilla Firefox ESR 102.4 and earlier versions
- Google Chrome 122, 124, 126, and later
- Microsoft Edge 122, 125, 126, and later



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

Verified external identity sources

Table 4: Verified external identity sources

External identity source	Version
Active Directory The supported Active Directory versions are the same for both Cisco ISE and Cisco ISE-PIC.	
Microsoft Windows Active Directory 2016	Windows Server 2016
Microsoft Windows Active Directory 2019	Windows Server 2019
Microsoft Windows Active Directory 2022	Windows Server 2022 with Patch Windows10.0-KB5025230-x64-V1.006.msu
Microsoft Entra ID	—
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	

External identity source	Version
Microsoft SQL Server	Microsoft SQL Server 2012 Microsoft SQL Server 2022
Oracle	Enterprise Edition Release 12.1.0.2.0
PostgreSQL	9.0
Sybase	16.0
MySQL	6.3
Social Login (for guest user accounts)	
Facebook	Latest

Verified antivirus and antimalware products

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

Verified OpenSSL version

Cisco ISE release 3.1 is verified 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.

Bundle download prechecks fail during a full upgrade from Cisco ISE release 3.1 patch 12 to Cisco ISE release 3.2

Bundle download prechecks fail when you run a full upgrade from Cisco ISE release 3.1 patch 12 to Cisco ISE release 3.2 using the Cisco ISE release 3.2 upgrade bundle. To complete the upgrade, use a split upgrade or a CLI upgrade. Cisco recommends using a Cisco ISE release listed among the recommended releases.

For more information, refer to CSCww60992.

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.

Incorrect smart licensing consumption reports

After you upgrade to Cisco ISE Release 3.1 Patches 5 or 6, if your smart licensing configuration uses the connection methods Direct HTTPS or HTTPS Proxy, you may witness incorrect compliance statuses being reported. Incorrect license consumption counts may be reported due to a communication error between Cisco ISE and CSSM.

To troubleshoot the communication error, in the **Licensing** window of the Cisco ISE administration portal, deregister and then reregister your smart licensing.

CSCwc74531 hot patch affects Cisco ISE application server

Installing the CSCwc74531 hot patch affects the Cisco ISE application server if all the following conditions are met:

- You installed Cisco ISE Release 3.1 using the ise-3.1.0.518.SPA.x86_64.iso file
- You are running Cisco ISE Release 3.1 Patch 3 or earlier
- You have applied Log4j hot patch

In this scenario, reach out to Cisco TAC for node recovery.

We recommend that you upgrade to Patch 5 or later versions instead of applying the Log4j or CSCwc74531 hot patches while using Cisco ISE Release 3.1 Patch 3 or earlier.

If you have installed Cisco ISE Release 3.1 using the ise-3.1.0.518b.SPA.x86_64.iso file, this limitation does not affect your Cisco ISE.

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.

Authentication might fail for SNMP users after upgrade due to wrong hash value

If you are upgrading from Cisco ISE 2.7 or earlier release to Cisco ISE 3.1, you must reconfigure the settings for SNMP users after the upgrade. Otherwise, authentication might fail for SNMP users because of the wrong hash value.

Use the following commands to reconfigure the settings for SNMPv3 users:

no snmp-server user *<snmp user> <snmp version> <auth password> <priv password>*

snmp-server user *<snmp user> <snmp version> <auth password> <priv password>*

Special characters usage limitations in name and description fields

- These special characters cannot be used in the **Description** field for TACACS+ profiles and Device Administration Network conditions—[%\<>*^:"|',=/()$.@;&-!#{}.?]. Supported characters are alphanumeric, underscore, and space.
- These special characters cannot be used in the **Name** and **Description** fields for Authorization profiles—%\<>*^:\"|',=. Supported characters for the **Name** and **Description** fields are alphanumeric, hyphen, dot, underscore, and space.
- These special characters cannot be used in the **Name** and **Description** fields for Time and Date conditions—[%\#$&()~+*@{}!/?;:',=^`]"<>". Supported characters for the **Name** and **Description** fields are alphanumeric, hyphen, dot, underscore, and space.

Make a wish option not available in Japanese

If you have configured your localization settings to enable Japanese in your Cisco ISE, note that the **Make a Wish** option is not available in Japanese.

RADIUS logs for authentication

Details of an authentication event can be viewed in the **Details** field of the **Radius Authentications** window. The details of an authentication event are available only for 7 days, after which no data on the authentication event will be visible. All the authentication log data will be removed when a purge is triggered.

Server IP update under TrustSec AAA server list

When the IP address of the Cisco ISE instance is changed using the CLI, Cisco ISE services are restarted. After the services are up, you must change the IP address of the Trustsec AAA server. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Workcenters** > **TrustSec** > **Components** > **Trustsec Servers** > **Trustsec AAA Servers**.

EAP-TLS authentication might fail for certificates using TPM module

In Cisco ISE Release 3.1, EAP-TLS authentication might fail for certificates using TPM module on Windows 10. This is an issue with the TPM module and not with Cisco ISE.

From Cisco ISE Release 3.1 Patch 6, the configuration option

```
application configure ise
```

in the Cisco ISE Admin CLI to enable or disable the current status of RSA_PSS signature for EAP TLS. It is as follows:

```
[33]Enable/Disable/Current_status of RSA_PSS signature for EAP-TLS.
```

Cisco ISE release 3.1 patch 8 SLR registered node shows SL registered post patch rollback

If you install Cisco ISE release 3.1 patch 8 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 3.1 patch 8 or later, you do not have to return SLR before rolling back to an earlier release.

Upgrade information

Upgrading to release 3.1

You can directly upgrade to release 3.1 from the following Cisco ISE releases:

- 2.6
- 2.7
- 3.0

If you are on a version earlier than Cisco ISE release 2.6, you must first upgrade to one of the releases listed above, and then upgrade to release 3.1.

Cisco ISE patches are cumulative and we recommend that you upgrade to the latest patch in the existing release before starting the upgrade. We recommend that you install all the relevant patches before beginning the upgrade. For more information, see the Cisco Identity Services Engine Upgrade Guide.

Upgrade packages

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

Upgrade procedure prerequisites

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

We recommend that you install all the relevant patches before beginning the upgrade.For more information, see the Cisco Identity Services Engine Upgrade Guide.

Telemetry

After installation, when you log in to the Admin portal for the first time, the Cisco ISE Telemetry banner is displayed. Using this feature, Cisco ISE securely collects nonsensitive information about your deployment, network access devices, profiler, and other services that you are using. This data will be used to provide better services and more features in the forthcoming releases. By default, telemetry is enabled. To disable or modify the account information, choose **Administration > Settings > Network Settings Diagnostics > Telemetry**. The account is unique for each deployment. Each admin user need not provide it separately.

It may take up to 24 hours after the Telemetry feature is disabled for Cisco ISE to stop sharing telemetry data.

Types of data collected include Product Usage Telemetry and Cisco Support Diagnostics.

Cisco Support Diagnostics

The Cisco Support Diagnostics Connector enables Cisco Technical Assistance Center (TAC) and Cisco support engineers to obtain support information on the deployment through the primary administration node. By default, this feature is disabled. See the Cisco Identity Services Engine Administrator Guide for instructions on how to enable this feature.

Cisco ISE live update portals

Cisco ISE Live Update portals help you to automatically download the **Supplicant Provisioning** wizard, AV/AS support (Compliance Module), and agent installer packages that support client provisioning and posture policy services. These live update portals are configured in Cisco ISE during the initial deployment to retrieve the latest client provisioning and posture software directly from Cisco.com to the corresponding device using Cisco ISE.

If the default Update portal URL is not reachable and your network requires a proxy server, configure the proxy settings. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration > System > Settings > Proxy** before you access the Live Update portals. If proxy settings allow access to the profiler, posture, and client-provisioning feeds, access to a Mobile Device Management (MDM) server is blocked because Cisco ISE cannot bypass the proxy services for MDM communication. To resolve this, you can configure the proxy services to allow communication to the MDM servers. For more information on proxy settings, see the "Specify Proxy Settings in Cisco ISE" section in the Cisco Identity Services Engine Administrator Guide.

Client Provisioning and Posture Live Update Portals

You can download Client Provisioning resources from:

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Posture** > **Settings** > **Software Updates** > **Client Provisioning.**

The following software elements are available at this URL:

- Supplicant Provisioning wizards for Windows and Mac OS X native supplicants
- Windows versions of the latest Cisco ISE persistent and temporal agents
- Mac OS X versions of the latest Cisco ISE persistent agents
- ActiveX and Java Applet installer helpers
- AV/AS compliance module files

For more information on automatically downloading the software packages that are available at the Client Provisioning Update portal to Cisco ISE, see the "Download Client Provisioning Resources Automatically" section in the "Configure Client Provisioning" chapter in the Cisco Identity Services Engine Administrator Guide.

You can download Posture updates from:

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Posture** > **Settings** > **Software Updates** > **Posture Updates**

The following software elements are available at this URL:

- Cisco-predefined checks and rules
- Windows and Mac OS X AV/AS support charts
- Cisco ISE operating system support

For more information on automatically downloading the software packages that become available at this portal to Cisco ISE, see the "Download Posture Updates Automatically" section in the Cisco Identity Services Engine Administrator Guide.

If you do not want to enable the automatic download capabilities, you can choose to download updates offline.

Cisco ISE offline updates

This offline update option allows you to download client provisioning and posture updates, when direct internet access to Cisco.com from a device using Cisco ISE is not available or is not permitted by a security policy.

To download offline client provisioning resources:

Procedure

Step 1 Go to: https://software.cisco.com/download/home/283801620/type/283802505/release/3.1.0.

Step 2 Provide your login credentials.

Step 3 Navigate to the Cisco Identity Services Engine download window, and select the release.

The following Offline Installation Packages are available for download:

- **win_spw-**<*version*>**-isebundle.zip**—Offline SPW Installation Package for Windows
- **mac-spw-**<*version*>**.zip**—Offline SPW Installation Package for Mac OS X
- **compliancemodule-**<*version*>**-isebundle.zip**—Offline Compliance Module Installation Package
- **macagent-**<*version*>**-isebundle.zip**—Offline Mac Agent Installation Package
- **webagent-**<*version*>**-isebundle.zip**—Offline Web Agent Installation Package

Step 4 Click either **Download** or **Add to Cart**.

For more information on adding the downloaded installation packages to Cisco ISE, see the "Add Client Provisioning Resources from a Local Machine" section in the Cisco Identity Services Engine Administrator Guide.

You can update the checks, operating system information, and antivirus and antispyware support charts for Windows and Mac operating systems offline from an archive in your local system, using posture updates.

For offline updates, ensure that the versions of the archive files match the versions in the configuration file. Use offline posture updates after you configure Cisco ISE and want to enable dynamic updates for the posture policy service.

To download offline posture updates:

Procedure

Step 1 Go to https://www.cisco.com/web/secure/spa/posture-offline.html.

Step 2 Save the **posture-offline.zip** file to your local system. This file is used to update the operating system information, checks, rules, and antivirus and antispyware support charts for Windows and Mac operating systems.

Step 3 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration > System > Settings > Posture**.

Step 4 Click the arrow to view the settings for posture.

Step 5 Click **Updates**.
The **Posture Updates** window is displayed.

Step 6 Click the **Offline** option.

Step 7 Click **Browse** to locate the archive file (posture-offline.zip) from the local folder in your system.

Note
The **File to Update** field is a mandatory field. You can select only one archive file (.zip) containing the appropriate files. Archive files other than .zip, such as .tar, and .gz are not supported.

Step 8 Click **Update Now**.

Configuration prerequisites

- The relevant Cisco ISE license fees should be paid.
- The latest patches should be installed.
- Cisco ISE software capabilities should be active.

See the following resources to configure Cisco ISE:

- Getting started with Cisco ISE
- Videos on the Cisco ISE Channel on YouTube
- *Cisco ISE Design and Integration Guides*
- *Cisco Identity Services Engine Administrator Guide*

Monitoring and troubleshooting

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

Ordering information

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

Cisco ISE integration with Cisco Catalyst Center

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*.

Cisco AI Endpoint Analytics

Cisco AI Endpoint Analytics is a solution on Cisco Catalyst Center that improves endpoint profiling fidelity. It provides fine-grained endpoint identification and assigns labels to various endpoints. Information gathered through deep-packet inspection, and probes from sources such as Cisco ISE, Cisco SD-AVC, and network devices, is analyzed for endpoint profiling.

Cisco AI Endpoint Analytics also uses artificial intelligence (AI) and machine learning capabilities to intuitively group endpoints with similar attributes. IT administrators can review such groups and assign labels to them. These endpoint labels are then available in Cisco ISE if your Cisco ISE account is connected to on-premises Cisco Catalyst Center.

These endpoint labels from Cisco AI Endpoint Analytics can be used by Cisco ISE administrators to create custom authorization policies. You can provide the right set of access privileges to endpoints or endpoint groups through such authorization policies.

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*.

Warning 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.

Changes in behavior

Changes in behavior in Cisco ISE release 3.1 - Cumulative Patch 12

Table 5: Changes in behavior in Cisco ISE release 3.1 patch 12

Identifier	Description
CSCwn62873	Previously, Cisco ISE could not join Active Directory on a Windows Server 2025 domain controller and displays an error. Windows Server 2025 now blocks legacy Security Account Manager (SAM) Remote Procedure Call (RPC) password-change methods by default, so administrators must configure the SAM policy to allow all password-change RPC methods.

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

Resolved Caveats

Resolved caveats in Cisco ISE release 3.1 cumulative patch 12

Identifier	Headline
CSCwn93753	In Cisco ISE release 3.1 patch10, the External RADIUS server authentication fails with "Could not find selected Access Service" message.
CSCwn38890	Optimize RMQ connections and channels.
CSCwv60504	Cisco ISE services fail to start after installing Cisco ISE release 3.1 patch 11.
CSCwt22913	Cisco Identity Services Engine Remote Code Execution Vulnerability.
CSCwn62873	Cisco ISE fails to join Microsoft Active Directory (AD) domains hosted on Windows Server 2025.
CSCwn94797	RADIUS token configuration does not work after installing Cisco ISE release 3.1 patch 10 in a deployment.
CSCwu28438	In earlier Cisco ISE releases, you can delay the removal of idle RabbitMQ connections.

Identifier	Headline
CSCww39530	Cisco Identity Services Engine Authentication Bypass Vulnerability

Resolved caveats in Cisco ISE release 3.1 cumulative patch 11

Identifier	Headline
CSCws52717	Cisco Identity Services Engine Path Traversal Vulnerability.
CSCws52738	Cisco Identity Services Engine Remote Code Execution Vulnerability.
CSCws83036	Impact assessment of client authentication EKU enforcement in Cisco ISE.

Resolved caveats in Cisco ISE release 3.1 cumulative patch 10

Identifier	Headline
CSCwn17599	SFTP server validation fails with Cisco ISE Release 3.3 Patch 3.
CSCwf23271	Deployment of SEC_TRNREP_STATUS does not get updated from IN PROGRESS.
CSCwi88583	Handle erl_crash.dump in a better way.
CSCwk71111	Backup restoration is stuck at 75 percent.
CSCwj54376	Evaluate Configuration Validator does not parse all NAD interfaces.
CSCwk47475	Cisco ISE Arbitrary File Read and Delete Vulnerability.
CSCwm48867	The swap-on or swap-off cron should be removed as it causes high load every 6 hours.
CSCwm10693	Cisco ISE internal users account disable policy feature does not work after one day of inactivity.
CSCwk13234	Old Cisco ISE nodes are shown in TCP dump and debug profile configuration after restore.
CSCwh54899	Unable to log in to Cisco ISE GUI. After entering the credentials, it hangs on checking the credentials screen.
CSCwj71638	Policy hit count shows zero when fetched by Open API GET call.
CSCwf69715	After patch install TC-NAC adapters will be not reachable and new adapters cannot be configured.
CSCwj61421	Cisco Identity Services Engine OS Command Injection Vulnerability.
CSCwk47489	Cisco Identity Services Engine Arbitrary File Read and Delete Vulnerability.
CSCwh49351	The Cisco ISE admin portal SAML SSO should not redirect to another Cisco ISE node, such as the active PSN.

Identifier	Headline
CSCwm47216	Context leaks and stuck threads happen in the EWA flow involving MAB, Dot1x, and Passive ID.
CSCwi17200	When configuring "TROUBLESHOOTING.EncryptionOffPeriod" advanced tuning with any non-zero value of minutes for decrypting the communication with Active Directory for troubleshooting, then RPC net logon fails for all Active Directory authentications on that Cisco ISE node.
CSCwj32716	MDM configuration fails when the GUID in the client certificate is used to validate the compliance of the device.
CSCwk07454	PSN does not update the database with the correct posture lease expiry time.
CSCwm58686	Passive session is not published to FMC as Cisco ISE tries to stitch the session.
CSCwk59449	Cisco ISE redirection bypass may lead to XSS.
CSCwi20027	The TrustSec deployment request fails as the CoA request gets stuck while fetching NAD information.
CSCwj94294	Cisco Identity Services Engine REST API Blind SQL Injection Vulnerabilities.
CSCwj94297	Cisco Identity Services Engine REST API Blind SQL Injection Vulnerabilities.
CSCvy30859	In Cisco ISE Release 2.6, it is not possible to create static IP-SGT mapping for EPG's imported from ACI.
CSCwh97876	Cisco Identity Services Engine Arbitrary File Upload Vulnerability.
CSCwm33110	Heap space is fully utilized by RMQ Consumer.
CSCwk67197	Cisco ISE does not connect with external RADUIS server when proxy-state attribute is missing.
CSCwk31930	Cisco ISE skips authentication against the child domain controller when the AD Forest is marked offline.
CSCwk06043	Binding with SGT assigned through MAB policy is not seen in SGT bindings table.
CSCwj39533	RMQforwarder causes high CPU or load average on PSN nodes.
CSCwm00197	Numeric overflow exception encountered during restart of replication client.
CSCwj84724	Cisco ISE authorization profile does not persist "Security Group" data.
CSCwi59230	Non super-admin users cannot edit or delete endpoints when Cisco ISE has more than 1000 identity groups.
CSCwi72309	Cisco ISE is stuck in a profiling loop, slowing down replication, and causing errors.
CSCwm07116	For SMS gateway GET requests, the URL mapping is not visible in the guest.log.
CSCwk67747	RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS).

Identifier	Headline
CSCwj67089	Cisco ISE app server crashes while importing large files to secondary node through local disk management.
CSCwf36985	AD group retrieval fails while evaluating authorization policy.
CSCwj23933	AD connector in not in joined status.
CSCwk73785	User authentication is achieved through certificate-based methods using security identifiers.
CSCwk47423	Cisco Identity Services Engine Reflected Cross-Site Scripting Vulnerability.
CSCwk25064	SXP threads storing NULL objects in the Java heap are causing high CPU load and utilization.
CSCwk13244	Cisco ise-messaging.log is not visible on Cisco ISE GUI for download.
CSCwm53340	PSN nodes crash during TACACS flow.
CSCwk36095	The Cisco pxGrid live log serviceability.
CSCwj80616	Endpoint details in Cisco ISE context visibility does not match with RADIUS live logs or sessions during MDM flow.
CSCwm40047	Getting misleading error prompt "Unable to send email".
CSCwk14636	Insufficient virtual machine resources alarm not working on AWS.
CSCwi59555	In Cisco ISE Release 3.2 Patch 4, the search for MAC address in the format is ignored.
CSCwd49321	Cisco ISE integration fails with Cisco pxGrid is not enabled on Cisco ISE error message even when Cisco pxGrid is enabled in both nodes.
CSCwm02519	Additional fix to LSD class.
CSCwk75761	High CPU on admin node post accessing "Endpoint Identity Groups" page on Cisco ISE.
CSCwh72754	Cisco ISE active directory process stuck at "Updating" which consumes 90 to 100% CPU.
CSCwj29473	Identity Services Engine Formula Injection.
CSCwk91976	The Cisco ISE GUI does not ask confirmation of old password for password change.
CSCwm47768	Cisco ISE portals show Ukrainian when browser language is Russian.
CSCwm46079	SXP mappings is not learned for VPN users private IP.
CSCwj94305	Cisco Identity Services Engine REST API Blind SQL Injection Vulnerabilities.
CSCwk35172	The "DumpClearOnExceed" files filling up the disk on Cisco ISE PSN nodes.
CSCwj35576	Cisco ISE Server-Side Validation Missing.

Identifier	Headline
CSCwj96002	Cisco Identity Services Engine Cross-Site Scripting Vulnerability.
CSCwm61668	TC-NAC_Tenable throws "Scan Failed: Error in connecting to host: 403 Forbidden" error.
CSCwj35698	Cisco ISE business logic issue in user dictionaries.
CSCwk75775	The health check fails on input or output bandwidth performance check and returns a NULL result.
CSCwj82298	Assigned logical profile is repeated in context visbility endpoint attributes and reports.
CSCwj72680	The HS_err files gets generated on MnT nodes.
CSCwj94315	Cisco Identity Services Engine REST API Blind SQL Injection Vulnerabilities.
CSCwh78725	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerability.
CSCwm13073	With less than 3000 SGTs, Cisco ISE throws "This Custom View has exceeded the maximum number of SGTs (3000)." error.
CSCwk47451	Cisco Identity Services Engine Path Traversal Vulnerability.
CSCwj89479	When joining multiple Cisco ISE nodes to the domain controller simultaneously, duplicate accounts are created.
CSCwm73142	The app-server crashes if NAD sends radius accounting without radius settings enabled.
CSCwk47454	Cisco Identity Services Engine Reflected Cross-Site Scripting Vulnerability.
CSCwk14907	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability.
CSCwm51099	Sponsors from different GROUP_ACCOUNTS groups can see all users if they are in the same OWN_ACCOUNTS.
CSCwk85833	Cisco ISE upgrade fails at "IdentityProviderAddCertToTrustedListUpgrade" stage.
CSCwi74567	Inconsistencies in the database cause corruption in the Cisco ISE portal.
CSCwk11836	TACACS livelogs and reports get impacted during rollback of Cisco ISE Release 3.1 Patch 8 to Patch 7.
CSCwk23108	Cisco Identity Services Engine Authorization Bypass Vulnerability.
CSCwj35581	Cisco ISE missing rate limiting protection.
CSCwc62131	Cisco ISE is not able to query MySQL 8.x as mysql.proc table is not implemented.
CSCwk38327	Health check fails for MDM flow.
CSCwj52266	Endpoint description in the Context Visibility page is updated with the Static Identity Group description.

Identifier	Headline
CSCwm32937	Cisco ISE does not respond to specific accounting packets, resulting in an incorrect IP update in the system.
CSCwk61938	Cisco ISE Evaluate OpenSSH CVE-2024-6387 "regreSSHion".
CSCwk47465	Cisco Identity Services Engine XML External Entity Injection Vulnerability.
CSCwk63438	Unsafe Implementation of GET requests in RBAC pages.
CSCwk52844	Insufficient page authentication across various pages such as repository and admin groups of Cisco ISE.
CSCwk52866	Unsafe implementation of GET requests in repository page.
CSCwk46431	Password update does not require current password.
CSCwk91991	Repository key pair passphrase is accepted with null values.
CSCwk63893	UDP syslog DNS name resolution must be done in a single function call instead of two (IPv6+IPv4).
CSCwm60638	Unable to start or stop existing TCP dump capture.
CSCwd96743	Log collection error observed for the Server=xxxx with the log type "Radius Authentication Passed".
CSCwm12379	Asset probe data is cleared when MAB authenticated clients reauthorize.

Resolved caveats in Cisco ISE release 3.1 cumulative patch 9

Identifier	Headline
CSCwf24553	Umbrella defect to provide information for terminologies used in the Licensing page.
CSCwf24554	Umbrella defect to display more information on Smart Lincensing registration failure.
CSCwh64195	Data corruptions cause FailureReason=11007 or FailureReason=15022.
CSCwj35698	Cisco ISE business logic issue - user dictionaries.
CSCwi63725	SNMPD process causes memory leak on Cisco ISE.
CSCwi34405	Unable to enforce Identity Access Restricted attribute during authorization.
CSCwj47769	Invalid request page in Cisco ISE Release 3.2 Patch 5.
CSCwi53104	Exporting the report beyond a one-month period yields no data.
CSCwh92185	RADIUS Authentication report exported from the operational data purging page is empty.
CSCwi42412	Interactive help throws error in console and logs.

Identifier	Headline
CSCvz86688	Aruba-MPSK-Passphrase needs encryption support.
CSCwi42628	MAR cache replication fails between peer nodes for both NIC and non-NIC bonding interfaces.
CSCwh81035	PAN is missing non-significant attribute updates of endpoints from PSNs.
CSCwi21020	Cisco ISE messaging certificate generation does not replicate a full certificate chain on secondary nodes.
CSCwi15914	Additional IPv6-SGT session binding is created for IPv6 link local address from SXP ADD operation.
CSCwi88504	Missing step and resolution text in live logs for attribute.
CSCwj12489	Unable to delete network device group.
CSCwc85211	Cisco ISE Passive ID agent error "id to load is required for loading".
CSCwh92366	Insufficient virtual machine resource alarm is observed in Cisco ISE Release 3.1 Patch 8 longevity setup.
CSCwi45131	Apache Struts vulnerability affects Cisco products: December 2023.
CSCwc58608	Cisco ISE 3.2 crashes when RADIUS request is received with EAP-FAST and EAP chaining.
CSCwf89224	Decryption of session ticket received from the client fails on Cisco ISE.
CSCwh90610	Abandoned jedis connections are not being sent back to the thread pool.
CSCwf80386	Current value of Disable_RSA_PSS environmental value is not saved after patch installation.
CSCwh41977	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.
CSCwh79938	Cannot set preferred Domain Controllers registry value in advanced tuning.
CSCwa82035	Cisco ISE Serviceability - Include garbage collector logs, thread dump, heap dump.
CSCwi43166	TrustSec update CoA and CoA-push is broken.
CSCwi73984	Installed patches menu does not list all the patches.
CSCwi66105	Custom attribute retention failure.
CSCwh45472	Operational backups from the GUI fail to SFTP repositories if the PKI key pair pass phrase contains the symbol +.
CSCwh55667	Internal system error when premier license is disabled.
CSCwi66126	Updating DACL using ERS API does not modify last updated timestamp.

Identifier	Headline
CSCwf44736	Cisco Identity Services Engine Cross-Site Request Forgery Vulnerability.
CSCwi32576	PSN node crashes while assigning the cpmSessionId.
CSCwi54325	PRA fails if the end point is within posture lease.
CSCwd67833	ERS API takes several seconds to update a single endpoint.
CSCwe92640	Cisco ISE Releases 3.1 or 3.2 are missing validation for existing routes during CLI configuration.
CSCwi61491	Application server crashes due to metaspace exhaustion.
CSCwh77574	Cisco ISE does not allow special characters in password while importing certificates.
CSCwh00060	Cisco ISE Injection Vulnerability.
CSCwh69045	Some internal users' passwords do not expire after the configured global password expiry date.
CSCvz91952	Some Cisco ISE users are able to avoid mandatory password reset on the next login.
CSCwi38493	Advance license consumption issue is seen in Cisco ISE Release 3.1 Patch 7.
CSCwh23986	Cisco pxGrid getUserGroups API request returns empty response.
CSCvm56115	Cisco ISE allows to save the policy when an identity store is deleted from another browser tab.
CSCwj36716	Cisco ISE self-persistent Cross-Site Scripting (XSS) in my reports.
CSCwj01310	8 Node longevity - intensive garbage collection observed due to SXP component.
CSCwi98793	Profiler caches MDM attribute with wrong values.
CSCwf38083	Cisco ISE services are stuck in initializing with secure syslog.
CSCwh71435	Cisco ISE ERS API creates enable password option of the internal users even though enable password field is not specified.
CSCwi57950	Nexpose Rapid 7 Strict-Transport-Security is malformed.
CSCwh25160	Swap cleanup script to drop the swap area and program the cron.
CSCwc44298	Failed to delete self registration portal: throws 500 server error.
CSCwi59567	Issues with updating the CoA retry count to "0" .
CSCwd57846	Convert TACACS persistent authorization to SQL loader approach.
CSCwf56826	Observing cores related to jstack on the PPAN nodes of regression setup.

Resolved caveats in Cisco ISE release 3.1 cumulative patch 8

Identifier	Headline
CSCwh42683	Read-only admin group users have full accesss when logging into Cisco ISE GUI through SAML authentication.
CSCwe37377	Cisco ISE CRL retrieval failed alarm does not mention server on which CRL download failed.
CSCwc33290	Unable to delete custom endpoint attributes due to malfunctioning of "trash" button.
CSCwa97036	Unable to bind Cisco ISE messaging service with SubjectAltName extension while using wildcard certificate.
CSCwe96633	Tterrors.log and times.log are missing in support bundle.
CSCwf14957	Unable to change TrustSec status when using Japanese UI.
CSCwf83193	Unable to login into the secondary admin node Cisco ISE GUI using AD credentials.
CSCwd93717	Vulnerabilities in Cisco ISE allows unwarranted arbitrary file upload.
CSCwe89459	Cisco ISE REST API documentation provides incorrect script while creating endpoint group.
CSCwf25955	A match authorization profile with SGT, VN name, VLAN fields empty causes port to crash.
CSCwh18487	Expired guest accounts don't receive SMS when they try to reactivate account.
CSCwh71273	Disabled essential license leads to limited Cisco ISE GUI page access and inability to regenerate root CA.
CSCwh52589	During first device connection attempt, Cisco ISE does not update the Acs.Username field with the guest username.
CSCwf39284	Unable to edit and save security group ACL.
CSCwf68108	The OpenAPI for endpoints are not working for the existing IOT asset attributes.
CSCwf40861	When command set includes special characters, the UI shows HTML hexadecimal instead of the character.
CSCvy02871	Download failure for "agent resources from Cisco site".
CSCwe54318	SXP service stuck in initializing due to H2 DB delay in querying bindings.
CSCwh50304	API query of ERS the network device component returns primary shared secrets for primary and secondary fields.
CSCwf60904	ANC remediation is not functioning with AnyConnect VPN.
CSCwe72097	Unable to launch sponsor portal after edits to interface on the existing portal.

Identifier	Headline
CSCwd12453	Cisco ISE Release 3.1 and Release 3.0: Portal tag with special character faces validation issues.
CSCwe07822	Date of last purge has a wrong timestamp.
CSCwf44942	ISE:TACACS:PSN crashes during maximum user session authentication flow.
CSCwb63834	MNT log processor is enabled on non-MNT admin Cisco ISE node.
CSCwf19811	SXP Bindings report show "no data found".
CSCvz48764	Allow launch program remediation to have a set order.
CSCwe59587	Some items are displayed as [Test] in Japanese display.
CSCwf22794	Inconsistency in VLAN ID results in erorr message: Not a valid ODBC dictionary.
CSCwf13630	MNT log processor service stops to fucntion during night-time.
CSCvq79397	UI pages are not loading properly with custom admin menu workcenter permissions.
CSCwh51156	Cisco ISE cannot load corrupted NAS profiles that causes authorization drops due to failure Reasons 11007 and 15022.
CSCwf19463	Drag and drop of a saved condition is unreadable.
CSCuz65708	Numbering issues observed for DACL entries in Firefox 45 and Chrome 72, and all later issues.
CSCwc26835	RADIUS server sequence configuration gets corrupted.
CSCwb83304	Cisco ISE upgrade fails because of custom security group.
CSCwc47799	Cisco ISE is unresponsive while importing certificate when the special character (%) is added in the private key password field or the friendly name field.
CSCwe11676	Data is lost when accessing total compromised endpoints in Cisco ISE dashboard threat for TC-NAC.
CSCwf44906	Reconfiguration of repository with credential is required after restoration of configuration backup.
CSCwf72037	Cisco ISE Release 3.1: Administrator login report displays "administrator authentication failed" in 5 min intervals.
CSCwh47299	Cisco ISE alarm and dashboard summary fails to load.
CSCwe17953	Cisco ISE path traversal vulnerability detected.
CSCwf40128	Accept client certificate without KU purpose validation as per Cisco SSL rules.
CSCwf64662	SXP creates inconsistent mapping between IP address and SGT.

Identifier	Headline
CSCwh17448	Cisco ISE Release 3.1: Agentless posture flows fails when domain user configures for endpoint login.
CSCwf07855	Cisco ISE SXP bindings API call returns 2xx response when the call fails.
CSCvj75157	Cisco ISE API doesn't recognize identity groups while creating user accounts.
CSCwf61673	From Cisco ISE CLI, read-only users can not run a show CPU usage command.
CSCwd57628	NAD RADIUS shared secret key is incorrect when it starts with an apostrophe on Cisco ISE Release 3.1 Patches 1, 2, 3, 4, and 5.
CSCwc57630	Cisco ISE Release 3.2 BETA: GUI is not accesible after enabling TLS 1.0.
CSCwe10898	An endpoint's MAC address is not added to the endpoint identity group when using grace access in the guest portal.
CSCwe38800	Vulnerabilities detected in hibernate-validator in multiple versions.
CSCwf22527	Context Visibility: Unable to filter endpoint custom attributes with special characters.
CSCwf96294	Cisco ISE Release 3.0: Disabled domains in allowed domains makes connection attempts to ad_agent.log domains.
CSCwh05599	Cisco ISE sponsor portal shows invalid input error when using special characters in the guest type name.
CSCwh18899	Cisco ISE Open API: /certs/system-certificate/import must support multi-node deployment.
CSCwc53915	Cisco ISE Release 3.1 shows "error creating 1 domain controller" already exists, although it is a new deployment.
CSCwf88944	Guest portal FQDN is mapped with IP address of the node in the database.
CSCwf17490	Post SL update, Cisco ISE licensing page shows evaluation compliance status for consumed licenses.
CSCwd38766	Hexadecimal username stays in the database even after deleting SNMPv3 username with "-" or "_" characters.
CSCwe74135	Cisco ISE Release 3.1 Patch 5: Attempting to delete Guest portal after PAN failover fails.
CSCvo60450	Enhancement for encryption should only send AES256 for MS-RPC calls.
CSCvw81130	Cisco ISE Release 2.7: Unable to disable active directory diagnostic tool scheduled tests.
CSCwd93721	Cisco ISE privilege facing escalation vulnerability.
CSCwd93720	Cisco ISE arbitrary file upload vulnerability.
CSCwe86793	Cisco ISE filter of REST ID store groups displays error processing this request.

Identifier	Headline
CSCwd34685	Cisco ISE messaging service flapping between "not running" and "initializing".
CSCwf30570	Agentless posture script does not run when the endpoint is not connected to an AC power source.
CSCwf24158	Terms and conditions checkbox disappears when portal builder is used for Cisco ISE Release 3.0 and higher.
CSCvv90394	Cisco ISE Release 2.6 Patch 7 is not able to match "identityaccessrestricted equals true" in authorization policy.
CSCwf94289	Cisco ISE Release 3.0 Patch 6: Policy export fails to export the policies.
CSCwh23367	In Cisco ISE Release 3.2 , the self-registered email subject line truncates everything after the equal (=) sign on the sponsor guest portal.
CSCwf31073	Cisco ISE: "Error 400" displaying when fetching device admin network conditions via OpenAPI.
CSCwf09393	Cisco ISE Release 3.1 services failed to start after restoring backup from Cisco ISE Release 2.7.
CSCwc70197	Cisco ISE certificate API fails to return trusted certificate with special characters in friendly name.
CSCwe15945	Sponsors unable view guest account in a specific sponsor group
CSCwf34391	Cisco ISE EasyConnect stitching does not happen when the PassiveID syslog is received by MnT before the active authentication syslog.
CSCvo61351	Live session is stuck at "authenticated" state.
CSCwe71804	Cisco ISE Release 3.1: Key attributes is missing in session cache when third-party network device profile is in use.
CSCwh33160	Cisco ISE is not sending SNMPv3 disk traps to configured SNMP server.
CSCvy88380	Unable to select Cisco ISE messaging usage for an existing certificate as it is grayed out.
CSCvq43600	Even with disabled PSN persona the TACACS port 49 is still open.
CSCwf21585	Insecure HTTP PUT method accepted.
CSCwh21038	Session info is not stored in timed session cache during third party posture flow.
CSCwe22841	ANC with Aruba switches sends incorrect AVP's when invoked.
CSCvz86688	Aruba-MPSK-Passphrase needs encryption support.
CSCwf09364	The user identity group and endpoint identity group description fields have a character limit of 1199.
CSCwe78540	IoT asset information is missing when "get all endpoints" option is in use.

Identifier	Headline
CSCwc04447	Cisco ISE Release 2.7 Patch 6 is unable to filter TACACS live logs by network device IP.
CSCwh30893	Profiling is not processing calling station ID values with the following format: XXXXXXXXXXXX.
CSCwe43468	Static IP-SGT mapping with VN reference causes DNAC group-based policy sync to fail.
CSCwh10401	Cisco ISE Release 3.1 Patch 5: Cannot generate pxGrid client certificate leveraging the CSR option.
CSCwh70275	While registering node with left over certificates from deregistration, the certificates that are currently in use get deleted.
CSCwf47038	Trash all or selected option at pxGrid policy should not touch entries for internal group.
CSCwf07444	Cisco ISE patch GUI installation is stuck on a specific Cisco ISE node in deployment.
CSCwh04251	Cisco ISE agentless posture does not support password containing a colon.
CSCwe00424	SQL exception sent to the collection failure alarm is caused by NAS-Port-id length.
CSCwe86494	Cisco ISE dispalys tomcat stacktrace when a specific URL is in use.
CSCwf80292	Cisco ISE cannot retrieve a peer certificate during EAP-TLS authentication.
CSCvu56500	"Export all network devices" option gives an empty file.
CSCwf66237	"Get all endpoints" option request takes much longer time to execute since Cisco ISE Release 2.7.
CSCwf59058	RBAC policy with custom permissions is not working when administration menu is hidden.
CSCwe41824	Cisco ISE Release 3.2 is missing S-PAN key for PKI-based SFTP.
CSCwd82119	EAP-TLS authentication with ECDSA certificate fails on Cisco ISE Release 3.1.
CSCwf66880	Endpoint .csv file import displays "no file chosen" after selecting the file.
CSCwf26482	REST AUTH services are not running after upgrade from Cisco ISE Release 3.1 to Release 3.2.
CSCwf26951	Profiler CoA sent with the wrong session ID.
CSCwd17322	Cisco ISE in AWS: Health check I/O bandwidth performance check false alarm.
CSCwe27438	Launch page level help is not working for patch management, upgrade, and health checks.
CSCwf35760	ct_engine is using 100% CPU.

Identifier	Headline
CSCwb18744	Group Based Policy Security Groups or Access Contracts with multiple backslash characters in a row in the description causes data sync failure.
CSCwf37679	Sponsor permissions are disabled on sponsor portal when accessed from the primary PAN persona.
CSCwc22988	Disabling "disclose invalid usernames" shows popup that states displaying app server will restart.
CSCwe99961	Sponsored portal in Germany calendar shows Thursday (Donnerstag) as Di not Do.
CSCwf39620	Agentless posture is not working in Windows if the username starts with the special character '$'.
CSCwf23981	Cisco ISE authorization profile displays wrong security group and VN value.
CSCwf61939	Using an apostrophe in the first name and/or last name field presents an invalid name error.
CSCwf09674	Registered endpoint report shows unregistered guest devices.
CSCwc36589	Cisco ISE Intune MDM integration may disrupt due to end of support for MAC address-based APIs from Intune.
CSCwc53824	Cisco ISE limits connection to AMP AMQP service to TLSv1.0.
CSCwf36285	The quick filter option for SXP domains is unusable if more than 25 rows are displayed.
CSCwe53550	Cisco ISE includes a version of Apache Commons FileUpload that is affected by the vulnerabilities with CVE ID CVE-2023-24998 .
CSCwf82055	Unable to disable SHA1 for ports associated with passive ID agents.
CSCwh53159	Cisco ISE Release 3.1 Patch 7: Unable to change admin password if it contains special character '$'.
CSCwf62744	Add the "disable EDR internet check" tag.
CSCwh63501	Vulnerabilities in log4net 2.0.8.0.
CSCwh65018	Cisco ISE Release 3.1 Patch 5 install hangs indefinitely, and updates timesten sys.odbc.ini for TCNAC.
CSCwe82004	TCP sockets stuck in CLOSE_WAIT state.
CSCwe69189	Lightweight session directory is causing high bandwidth utilization.
CSCwb44638	Enhancement: Include a seperate log file with MNT database metrics.
CSCwf10004	Cisco ISE IP SGT static mapping is not sent to SXP domain even after shift to another mapping group.
CSCwf21960	During upgrade, the deregister call fails to remove all the nodes from the databse.

Identifier	Headline
CSCwd21798	Cisco ISE-PIC license expiration alarm is an error.
CSCwb01568	Cisco ISE on AWS: Operational database has limited allocation.
CSCwf71870	TACACS deployment with zero day evaluation does not work after registering to smart licensing.
CSCwf42496	Attempt to delete 'Is IPSEC Device' NDG causes all subsequent RADIUS/T+ authentications to fail.
CSCwc44622	Session gets stuck indefinitely when NAD (Meraki) misbehaves unless restarted.
CSCwh60726	Automatic crash decoder is not decoding functions properly.
CSCwf79310	Cisco ISE Release 3.1 Patch 7: No virtual networks visible under security group in authorization profile.
CSCwh51136	Cisco ISE drops RADIUS request with the message "request from a non-wireless device was dropped".
CSCwe37826	Unable to change the condition operator from AND to OR in posture policy condition.
CSCwf33018	Fix to the bug CSCwd35608 is causing CoA calls from UI to be sent to the wrong IP.
CSCwf28229	VLAN detection interval should not exceed 30 seconds.
CSCwf19039	Cisco ISE Release 3.1 Patch 5: Agentless posture failures cause /tmp/ folder size increase.
CSCwf22816	Authorization based on internal user ID group fails without the RADIUS-token authorization for VPN.
CSCwf31477	Profiler is triggering a port bounce when multiple sessions exist on a switch port.
CSCwf41103	Cisco ISE Admin CLI reset-configuration fails to reset bond interfaces.
CSCwd39746	SCCM integration with Cisco ISE needs MSAL support as MS is deprecating ADAL.
CSCwf55641	German and Italian emails cannot be saved under account expiration notification in guest type.
CSCwh28528	TopN Device and admin reports doesn't work when TACACS incoming exceeds 40M records per day.
CSCwh41693	Cisco ISE on AWS doesn't work if metadata (IMDS) version value "V2 only" is selected.
CSCwf33421	Update warning message while changing timezone.
CSCwe12618	Cisco ISE Release 3.2:Unable to receive IP-to-SGT mappings from APIC.
CSCwe96739	TLS 1.0 or 1.1 is accepted at Cisco ISE Release 3.0 admin portal.
CSCwf34596	User custom attributes is stuck on rendering state.

Identifier	Headline
CSCwe03624	Smart license registration failure with "communication send error" alarms displays intermittently.
CSCwf81550	Cisco ISE changes the MAC address format to an unacceptable MAC adress format.
CSCwf54680	Unable to edit or delete authorization profiles with parentheses in the name.
CSCwh38484	Manually deletion of the static route causes Cisco ISE to send packet with wrong MAC in Release 3.0 patch 7.
CSCwf40265	Cisco ISE maximum session counter time limit is not working.
CSCwe87660	Cisco ISE Release 3.1: Previous version hotpatch is visible in the database.
CSCwh39008	Unable to schedule or edit schedule for the configuration backup.
CSCwf59005	Cisco ISE Release 3.2 Patch 3: PEAP and EAP-TLS does not work on FIPS mode.
CSCwb72948	Cisco ISE Release 3.0 Patch 4 is unable to access system certificates page for the registered node.
CSCwf80951	Unable to edit or create admin user due to "xwt.widget.repeater.DataRepeater" error.
CSCwe98676	Vulnerable JS library issue found while executing ZAP.
CSCwd20521	AD connector process does not shutdown.
CSCwf15130	Permission for collector.log file is set as root automatically.
CSCwf59310	Cisco ISE Release 3.1 Patch 7: GUI is missing custom attributes delivered via pxGrid ContextIn.
CSCvv99093	Cisco ISE nodes intermittently triggers queue link alarm: cause=timeout.
CSCwh05647	Static IPv6 routes are removed after a reload in Cisco ISE Release 3.2.
CSCwb69830	RADIUS Vendor specific integer attributes are visisble as garbage in debug logs.
CSCwe30021	The syslog audit record for the certificate authentication failure is absent due to an internal error.
CSCwf79582	The certificates API - /admin/API/PKI/TrustCertificates is not exposed but breaks Cisco DNA Center integration with AD username.
CSCwi06794	The RADIUS live log delay issue caused by a problem in indexation is fixed.
CSCwh99772	All network device groups are deleted when a child item is removed from any group.
CSCwh44407	Cisco ISE Release 3.2 API: System certificate import does not work for a Cisco ISE node in the deployment.

Resolved caveats in Cisco ISE release 3.1 cumulative patch 7

Identifier	Headline
CSCwf26226	CPU spike due to memory leak with endpoints purge call
CSCwe37041	Internal CA certificate chain becomes invalid if the original primary PAN is removed
CSCwd68070	Import SAML metadata fails
CSCwc57162	Certificate-based GUI admin login stuck
CSCvz00689	GET/ers/config/activedirectory/{id}/getUserGroups doesn't return group names with returned data
CSCwe39262	Passive ID agent sends incorrect time format events
CSCwe25138	Cannot create identity user if the user custom attribute includes characters '$' or '++'
CSCwe80760	Unable to save launch program remediation when the parameter contains double quotes ("")
CSCwd92324	Cisco ISE Release 3.2 ROPC basic serviceability improvements
CSCwe55215	Cisco ISE smart licensing now uses smart transport
CSCwd84055	Cisco ISE Release 3.1 Azure AD autodiscovery for MDM API v3 is incorrect
CSCwe52461	Unable to enable the firewall condition in Cisco ISE Release 3.1
CSCwe37978	When you export a scheduled report of a large size, it is displayed as empty in the repository
CSCwe37018	Cisco ISE-DNAC integration fails if there are invalid certificates in the Cisco ISE trusted certificates store
CSCwd31414	Guest portal displays the error loading page when the reason for visit field contains special characters
CSCwe15315	TrustSec PAC information field attribute values are lost when you import a network device CSV template file
CSCwe52296	MNT authorization status API query should be optimized
CSCwc91917	Unable to add quotation character in TACACS authorization profile
CSCwd97353	Automatic backup stops working after 3 to 5 days
CSCwd97022	Cisco ISE-PIC Release 3.2 FCS: smart licensing: PIC upgrade: out of compliance
CSCwd87161	Cisco ISE Release 3.1: certificate-based login asks for license file if only the device admin license is enabled
CSCwe63873	Qualys adapter is unable to download the knowledge base. Stuck at knowledge download in progress

Identifier	Headline
CSCwd97551	Cisco ISE cannot retrieve OU attributes from client certificate in EAP-TLS session resumption
CSCwb28410	'/' in command arguments is not preserved after CSV import of the T+ command set
CSCwd71496	Cisco ISE does not delete sessions from all SXP mapping tables
CSCwd92835	Network device profile shows HTML code as name
CSCwc13859	Unable to create scheduled backup with admin user from 'system admin' admin group
CSCwe49167	Cisco ISE Release 3.2: SAML sign authentication request setting is unchecked upon save
CSCvx15522	DNS cache enabling command in FQDN syslog popup needs correction
CSCwc20314	Cisco ISE-PIC Release 3.1: PIC license: consumption 0
CSCwe14808	Cisco ISE fails to translate AD attribute of msRASSavedFramedIPAddress
CSCwe49261	Cisco ISE Release 3.1: passiveID - probes agents for status of all domains being monitored
CSCwc64480	When importing a new certificate for a portal, Cisco ISE fails to establish secure connection
CSCwe37041	Internal CA certificate chain becomes invalid if original primary PAN is removed
CSCwd41098	Getting pxGrid error logs in ise-psc.log after disabling pxGrid
CSCwe49183	Cisco ISE SAML destination attribute is missing for signed AuthnRequests
CSCwc05718	Cisco ISE debug wizard posture profile does not contain client-webapp component to DEBUG
CSCwe68336	Posture assessment by condition generates ORA-00904: <SYSTEM_NAME>: invalid identifier
CSCwe54466	Sponsor portal print issue for from-first-login guest account expire details
CSCwe30606	Not able to download support bundles greater than 1 GB from the GUI
CSCwe24932	Agentless posture fails when using multiple domain users in the endpoint login configuration
CSCwe57764	MDM: connection to Microsoft SCCM fails after Windows DCOM server hardening for CVE-2021-26414
CSCvw50556	Cisco ISE3.0.458: enable_passwdless_auth.exp needs modification for mac clients
CSCwe43002	Read-only admin is not available for Cisco ISE admin SAML authentication
CSCwd05040	Unable to import certificates on secondary node after registration

Identifier	Headline
CSCwd69072	Session directory write fails with the alarm Cisco NAD using user-defined NAD profile
CSCwb79496	WMI status shows progress after mapping from agent protocol to WMI protocol
CSCwe34566	Authentication against ROPC identity store fails with RSA key generation error
CSCwd73282	Cisco ISE Release 3.1 patch 3: sponsor portal: session cookie SameSite salue is set to none
CSCwe13780	Unable to join node to AD by REST API if we configure a specific OU
CSCwe64558	Admin account created from network access users cannot change dark mode setting
CSCwb85502	CIAM: xstream 1.4.17
CSCwe36242	TACACS command accounting report export is not working
CSCwe70975	SMS Javascript customization is not working for SMS email gateway
CSCwc99816	Cisco ISE OpenApi restore displays complete long before show command displays complete
CSCwe45245	Smart license registration is not working. Error while enabling the smart license
CSCwe13110	Cisco ISE Release 3.1 configuration backup executed on primary MNT node
CSCwe40577	Failed to handle API resource request: failed to convert condition
CSCwe92624	Cisco ISE Africa/Cairo Timezone DST
CSCwe92177	Mexico time zone incorrectly changes to daylight saving
CSCwe39781	Cisco ISE does not remove SXP mapping when SGT is changed after CoA
CSCwe30235	Vulnerabilities in jszip 3.0.0
CSCwd74898	Posture configuration detection alarms should be INFO level and reworded
CSCwd64649	Cisco DNA Center integration issue due to more internal CA certificates
CSCwe38610	Make MDM API v3 certificate string case insensitive
CSCwe84210	Authorization policy evaluation fails due to NullPointerException in LicenseConsumptionUtil.java.
CSCwe41695	Cisco ISE 3.patches 4 and 5: standalone ISE crashes if restarted after removing admin access restriction
CSCwe36063	No validation of PBIS reg key configuration on advance tuning page

Resolved caveats in Cisco ISE release 3.1 cumulative patch 6

Identifier	Headline
CSCwd27865	Configuration Changed is not working when assigning an endpoint to a group
CSCwa25342	ADE-OS Sensitive Information Disclosure Vulnerability
CSCwc33751	ISE 3.1 TFTP copy times out
CSCwd46505	ISE-PIC does not show Queue Link Errors
CSCwd63749	ISE 3.1 AD Retrieve Groups shows a blank page when loading a big number of AD groups 400+
CSCwb77915	Toggle to enable/disable RSA PSS cipher based on policy under Allowed Protocols
CSCwd35608	ISE is sending old Audit Session ID in reath CoA after previously successful port-bounce CoA
CSCvt62460	Unable to retrieve groups/attr from diff LDAP when defined per node
CSCwd70902	PRRT should be sending unfragmented messages to MnT if IMS is enabled to avoid merge
CSCwd55061	ERS API internal error seen while creating existing NDG
CSCwd47111	ISE is unable to save the Subnet/IP Address Pool Name for voice vlans.
CSCwd13201	UI crashed while loading authz policy on chrome and edge browser
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.
CSCvv54351	Device Administration using Radius does not consume base license
CSCwd27506	ISE 3.0 patch 6 : Missing Scheduled Reports
CSCwd41773	ISE 3.1: Application server crashes if CRL is downloaded frequently having size 5 MB or more.
CSCwd97606	Multiple requests for same IP+VN+VPN combinations with diff session ID creating duplicate records
CSCwe60453	ISE 3.1 patch 5 : No dictionary attribute with id [11055]
CSCwd90613	Radius Server Sequence page showing "no data available"
CSCwd12357	SXP service gets stuck in initializing due to an exception on 9644.
CSCwd94235	31p5 : app server and api gateway service not running
CSCwe22934	ISE Authentication latency from devices with no mac address

Identifier	Headline
CSCwc93253	ISE - Network device captcha only prompting when filter matches only 1 Network device
CSCwd51812	ISE 3.1 patch 4 : GUI : Certificate Authentication : Permissions
CSCwd31137	ISE scheduled radius authentication repots failed while exporting to SFTP repository
CSCwc47015	Fix for CSCvz85074 breaks AD group retrieval in ISE
CSCvg66764	[ENH] Session stitching support with ISE PIC Agent
CSCwd42311	Unable to download rest-id-store from Download Logs on GUI
CSCwe30014	vulnerable jQuery version found in Admin UI
CSCwd19529	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability
CSCwd71574	High CPU Utilization Due To Agentless Posture Configured
CSCwc39302	3.1Respin: interface status is showing UP even after shutdown
CSCwd24304	ISE 3.2 ERS POST /ers/config/networkdevicegroup fails - broken attribute othername/type/ndgtype
CSCwc87670	ISE 3.1 patch 3 unable to import endpoints from csv file if SAML is used
CSCvv47849	[CFD] Mapped SGT entry cleared from AuthZ Rules on ISE if SG name is modified in Cisco DNA Center
CSCwc44580	ISE 3.1 creates cni-podman0 interface with IP 10.88.0.1 and ip route for 10.88.0.0/16
CSCwd22790	URI not Accepted as Group attribute or as Name in Assertion of attributes for SAML IdP in 3.1/3.2
CSCvy69943	ENH: Allow Guest Portal HTTP Requests Containing Content-headers with {} Characters
CSCwa55233	Queue Link Errors "Unknown CA" when utilizing third-party signed certificate for IMS
CSCwd74197	Issues when changing ISE IP address.
CSCwa62202	ISE with 2 interfaces configured for portal access is broken
CSCwc48311	ISE vPSN with IMS performance degrades by 30-40% compared to UDP syslog
CSCwd16837	ISE openAPI HTTP repo patch install fails when dir listing is disabled
CSCwd41651	Vertical Scrollbar Bug - ISE 3.1
CSCwc75572	Primary Admin PPAN application server stuck at initializing state
CSCwe34204	ISE upgrade tab shows upgrade in progress after installing patch

Identifier	Headline
CSCwe07406	Error Loading Page error is output when creating a guest account in the Self-Registered Guest Portal
CSCwd26845	ISE 3.2 : APIC Integration : missing fvIP subscription
CSCwc98828	Cisco Identity Services Engine Interface Feature Insufficient Access Control Vulnerability
CSCwd68806	Open API Endpoint Post returns 200 instead of 201
CSCwc98824	Posture Requirements only show the default entry
CSCwc98823	Cisco Identity Services Engine Command Injection Vulnerability
CSCwa52678	GUI TCPDUMP gets stuck on Stop_In_Progress
CSCwc62716	IndexRebuild.sql script ran over MNT
CSCwd63661	ISE 3.1 p1 : Entering incorrect password on GUI shows end user agreement
CSCwc65802	Save button for SAML configuration grayed out
CSCwe13947	OpenAPI for EP create/update should work same as ERS API in addition to providing more functionality
CSCvv10712	Sec_txnlog_master table should be truncated post 2M record count
CSCwc62419	Cisco Identity Services Engine Insufficient Access Control Vulnerability
CSCwc98831	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability
CSCwd97582	ISE 3.1p5 verifies CA certificate EKU causing "unsupported certificate" error
CSCwd51409	ISE cannot retrieve repositories and scan policies of Tenable Security Center
CSCwd24286	ISE not sending hostname attribute to DNAC
CSCwd74560	PUT operation failing with payload via DNAC to ISE (ERS)
CSCwd15888	Not able to access Time Settings Configuration Export on ERS API
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"
CSCvy33393	ISE 3.1 BH Context visibility shows \\ in username where as live logs show correct single \
CSCwc80243	ISE TCPDUMP stuck at "COPY_REPO_FAILED" state when no repository is selected
CSCwc85546	ISE 3.1 ENH "Illegal hex characters in escape (%) pattern ? For input string: ^F"

Identifier	Headline
CSCwd10864	Cisco Identity Services Engine XML External Entity Injection Vulnerability
CSCwd45783	pxGrid session publishing stops when reintergrating FMC while P-PIC is down
CSCwd98296	Network Device Port Conditions -IP Addresses/Device Groups- doesn’t accept valid port strings.
CSCwd39056	ISE 3.1 P4 Passive DC configuration failing to save username correctly
CSCwc53895	ISE 3.1 P3 SAML SSO Doesn't work if active PSN goes down
CSCwc99178	Not able to add too many Authorization Profiles with active session alarm setting
CSCwd57978	All NADs are getting deleted while doing Filter on NDG Location and IP
CSCwd13555	ISE abruptly stops consuming passive-id session from a 3rd party Syslog server
CSCwd54844	ERS API Schema for Network Device Group Creation
CSCwd82134	Incorrect SLR out of compliance error reported in ISE
CSCwd93002	Getting System Error : Null while editing the groups and adding Name in Assertion under SAML
CSCwc07082	"The phone number is invalid" when trying to import users from csv file.
CSCwd89657	ISE 3.1 certain SFTP servers stopped working after upgrade to patch 4/5
CSCvv02086	Add ability to disable TLS 1.0 and 1.1 on ISE PIC node
CSCwc97775	ISE 3.1: Installation of P3 doesnt upgrade the v$timezone_file from 32 to 34
CSCwe44750	Persisting of Reprofiling result is not updating to Oracle/VCS after feed incremental update
CSCwe63320	ISE 3.2/3.1/3.0 displays mismatched information on "Get All Endpoints" report
CSCvt73953	Mismatched Information between CLI export and Context Visibility
CSCvv54798	Context Visibility CVS exported from CLI not showing IP Addresses

Resolved caveats in cisco ISE release 3.1 cumulative patch 5

The following table lists the resolved caveats in Cisco ISE release 3.1 cumulative patch 5.

Identifier	Headline
CSCwc74531	ise hourly cron should cleanup the cached buffers instead of the 95% memory usage
CSCwc52685	ENH: ISE with Twilio MessagingServiceSid for SMS gateway
CSCwc64346	ISE ERS SDK network device bulk request documentation is not correct

Identifier	Headline
CSCwc31482	NetworkSetupAssistance.exe digital signature certificate expired in BYOD flow using Windows SPW
CSCwc76720	Error with SNMPv3 Privacy Password on ISE 3.1 only
CSCwc27765	ISE Config Backup Fails due to SYS_EXPORT_SCHEMA_01
CSCwc57240	GUI not validating default value while adding custom attributes
CSCwb59162	ISE 3.1 REST API typo in SNMP password parameters
CSCwc26241	ISE 3.2 displays the error: "TypeError: Cannot read properties of undefined (reading 'attr')"
CSCwc21400	HTTP 400 response in Repo OpenAPI when an SFTP/FTP repo user password contains ! (exclamation mark)
CSCwd31405	Latency observed during query of Session.PostureStatus
CSCwc85920	ISE TrustSec Logging - SGT create event is not logged to ise-psc.log file
CSCwc39614	SYS.DBMS_RCVMAN too old
CSCwb23853	Unable to add SAML ID provider on 3.1 p1 when we did config restore from older ISE
CSCwc65802	Save button for SAML configuration grayed out
CSCwc21890	Passive Easy connect does not work in ISE with Dedicated MnT nodes
CSCwc69492	ISE 3.1 | Metaspace exhaustion causes crashes on ISE node
CSCwb62192	scheduled backup failure when ISE indexing engine backup failed
CSCwc65821	ERS API doesn't allow for use of minus character in "Network Device Group" name.
CSCwc71060	Deleted network device groups still showing up in the policy sets
CSCwc62415	Cisco Identity Services Engine Unauthorized File Access Vulnerability
CSCwa37580	ISE 3.0 NFS share stuck
CSCwb84779	Changing Parent Identity Group name breaks authorization references
CSCwc98833	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCwb88851	Inconsistent IP to SGT mapping after several re-authentications when VN value is changing
CSCwc80574	ISE AD Connector fails during join
CSCwc79321	Unable to change the Identity source from internal to external RSA/RADIUS-token server

Identifier	Headline
CSCwc64275	Precheck may get timedout with optimistic locking failed in ise-psc.log on ppan
CSCwc61320	Slowness on Support Bundle page due to Download Logs page loading in the background.
CSCwc09435	Error handling/ messaging for mobile number format not clear
CSCwc51219	CSV NAD import is rejected if += characters are at the beginning of the RADIUS shared secret
CSCwc24126	Profiler Condition not displaying the Attribute Value
CSCwc57294	Duplicate Manager doesn't remove packet when there is an exception in reading config
CSCwc95878	Intermittent issues with App activation or App not receiving events
CSCwd05697	Guest locations do not load in ISE Guest Portal
CSCwb47255	Supported HTTP methods are visible
CSCwd03009	RMQForwarder thread to control based on hardware Appliance in platform.properties on 2.7 p7
CSCvv43120	ISE-2.x: Intune MDM Alarm for connectivity || 401 Unauthorized
CSCwc81729	"All devices were successfully deleted" after trying to delete one particular NAD by filtering
CSCwc23997	ISE is showing Incorrect VLAN assignment Information in Authorization profile > Attributes Details
CSCwc42712	ISE RADIUS and PassiveID session merging
CSCwc15013	Add serviceability & fix "Could not get a resource since the pool is exhausted" Error on ISE 3.0
CSCwc59570	ISE sending SXP MSG size > 4096 bytes in SXP Ver 4
CSCwd45843	Auth Step latency for policy evaluation due to GC activity
CSCwb53455	RMQ TLS syslogs related to internal docker ip 169.254.2.2 are sent to Audit logs
CSCwa55866	Tacacs responses are not sent sometimes with single connect enabled
CSCwb24002	ISE ERS SDK the authenticationSettings are not disabled via API call
CSCwc95075	"File path field must contain a valid file name" error when configuring file conditions for posture.
CSCwb36873	Getting page not accessible pop-up message on ISE-PIC
CSCvz65945	"Invalid Length" TACACS Auth Failures within Live Logs for non-TACACS traffic

Identifier	Headline
CSCwb27894	EAP-TEAP with EAP-TLS unable to match condition that has "CERTIFICATE.Issuer - Common Name"
CSCwc74206	ISE 3.0 not saving SCCM MDM server object with new password, works when new instance is use
CSCwb48388	Licensing only displays one reserved count if licenses reserved in CSSM have multiple expiry dates
CSCwc50944	The change of profiling policy name is not reflected on the policy set conditions automatically
CSCvz91479	Schema upgrade failed while modifying constraints for 3.1->3.2.0.804 upgrade
CSCwc33850	Unable to export certificate with private key using API
CSCwc60997	ISE: SAML flow with loadbalancer is failing due to incorrect token handling on ISE
CSCwc49580	ANC COA is sent to the NAS ip address instead of the Device ip address.
CSCwc23593	LSD is causing high CPU
CSCwc44614	Using "Export Selected" under Network Devices aborts to login screen w/ more than X selections
CSCwc48509	Windows Server 2022 is actually working as the target domain controller to be monitored
CSCwc93451	Profiler should ignore non-positive RADIUS syslog messages for forwarding from default RADIUS probe
CSCvv54351	Device Administration using Radius does not consume base license
CSCwd30994	ISE : Static default route with gateway of interfaces other than Gig 0 breaks network connectivity
CSCwc07283	CONTEXT VISIBILITY ENDPOINT AUTHENTICATION TAB NOT SHOWING DATA ISE 3.1
CSCwc30643	My Devices Portal doesn't open after reloading the node unless we do CRUD.
CSCwc11613	Certificate signing request shoule not be case sensitive
CSCwc57939	ISE detects large VMs as Unsupported
CSCwc88848	ISE 3.1 Patch 1 does not created the Rest ID/ROPC folder logs

Resolved caveats in Cisco ISE release 3.1 cumulative patch 4

The following table lists the resolved caveats in Cisco ISE release 3.1 cumulative patch 4.

Caveat ID Number	Description
CSCwc62413	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCwb22662	64-character limit is not enough to accommodate external user identities, such as user principal name
CSCwb32244	Unable to edit certificates imported to ISE Trusted Certificate
CSCwb75941	Path traversal vulnerability
CSCwb75954	Cross-site request forgery vulnerability
CSCwb75959	Stored cross-site scripting vulnerability
CSCwb75965	Unauthorized file access vulnerability
CSCwb79353	OS privilege escalation issue
CSCwa88954	CIAM: python-pip 9.0.3
CSCwb64656	When Essential License is disabled on the Cisco ISE GUI, the Smart Licensing Portal does not report license consumption.
CSCwb39638	Unable to import network device configured with SNMPv3 SHA2 authorization
CSCvy77475	CIAM: libcurl 7.61.1
CSCwa61347	Cisco ISE-PIC does not forward live sessions beginning with special characters
CSCwb09824	CIAM: libjpeg-turbo 1.5.3
CSCwa96229	Cisco ISE does not allow user to change the admin password without validating current password
CSCwc00162	Certificate based admin login does not work when the client or browser send more than one certificate
CSCwb09881	CIAM: sqlite 3.26.0
CSCwa80499	CIAM: ncurses 6.1
CSCwb33727	Special characters are not supported in Attributes
CSCwc30811	Underscore is vulnerable in Guest Portals
CSCvy66496	REST ID does not filter groups based on name or SID for Azure AD groups
CSCwb92006	Having a single quote (') in the middle of the password on Proxy settings causes the page to become un-editable
CSCwb56878	No Replication Stopped Alarm triggered
CSCwb55232	Create a nested endpoint group using ERS API
CSCwb82814	OpenAPI Error 400 while fetching Nested Conditions

Caveat ID Number	Description
CSCvv87286	Failure to import Internal CA and key from ISE 2.7P2 to 3.0
CSCwb92643	ADE-OS CLI TCP parameters fail to make changes and are no longer relevant
CSCwb88360	Disable temporary management persona on upgraded node fails in split upgrade
CSCwb14106	CIAM: cyrus-sasl 2.1.27
CSCwb75964	Unable to edit PAN Auto Failover alarms
CSCvz71874	CIAM: libdnf 0.39.1
CSCwb19256	Ping-node call causes application server to crash (OOM exception) during CRL validation
CSCwc12303	PGA memory used by the instance exceeds PGA_AGGREGATE_LIMIT on MNT node
CSCwa97123	NTP Sync Failure Alarms with more than 2 NTP Servers Configured.
CSCwa40040	Session Directory Write failed, SQLException: String Data right truncation on ISE3.0P4
CSCwb95433	"File path field must contain a valid file name" error when file conditions are configured for posture
CSCwa80710	CIAM: jszip 2.5.0
CSCwa06912	High latency observed for TACACS+ requests with date or time condition in authorization policies
CSCwb29498	High Operations DB Usage Alarm percentage needs to be configurable
CSCwb61614	Guest users (AD or internal) cannot delete or add their own devices on a specific node
CSCwb82141	Context Visibility Endpoints And NADs from an existing deployment are not removed after Restore
CSCvx08772	Frequent Insufficient Virtual Machine Resources alarms
CSCwb42924	Unable to get message option in Posture remediation actions
CSCwc18751	Unable to download a created support bundle from GUI if logged in using the DomainName\UserName format
CSCwb25789	Inconsistent behaviour on handling of SSH host keys
CSCwb52396	ISE PRA failover
CSCwa85010	SAML certificates should not be marked as Stale if PAN is removed from deployment
CSCwb59170	SHA-2 option is not available for NAD creation using REST API
CSCwb91645	TrustSec Dashboard Refresh Call causes High CPU on MNT

Caveat ID Number	Description
CSCwb35304	Race condition causes registration or sync failure in Cisco ISE 3.1
CSCwa95892	ui_time_left variable shows the wrong duration
CSCwa60903	Cisco ISE adds six additional hours to nextUpdate date for CRL
CSCwc06638	System summary does not get updated post Patch RollBack and Patch Install
CSCwa83517	Guest portal registration page shows "error loading page" error when the email address contains apostrophe
CSCwa89443	DNA Center - ISE Integration: ISE shows an old DNAC certificate for pxGrid endpoint
CSCvz57222	Admin access is allowed for ISE GUI with secondary interfaces GigabitEthernet 1 and Bond 1
CSCwb05059	P1 Stale nodes in TCPDump Menu
CSCwb97579	Compatibility problems with Hyper-V Gen-2
CSCwb26965	Error when network device groups are created using REST APIs
CSCwb21669	Unable to enter ipv6 address for on-premise SSM server
CSCwb79056	ERS call /ers/config/sgmapping/{id} does not return SGT value for custom SGT's
CSCwa80488	CIAM: openssh 7.6
CSCvy91805	Max Sessions are not enforced with EAP-FAST-Chaining
CSCwa80480	CIAM: bind 9.11.4
CSCwb34910	Multiline issues for guest SMS notification in Cisco ISE Portal
CSCwb55979	NTP Service Failure
CSCwa95889	Unable to host SSH/SFTP with newer HostKeyAlgorithms (e.g. RSA-SHA2-512)
CSCwb26227	CIAM: jackson-databind 2.9.8
CSCwa73860	After ppgrade, the files in the rabbitmq certificate directory show incorrect permissions
CSCwb85456	CIAM: openssl upgrade to 1.0.2ze and 1.1.1o
CSCwc12693	ISE ERS Validation Error - [validDays] mandatory field is missing
CSCwb91392	BH Healthcheck and full upgrade pre-check times out when third party CA certificate is used for admin
CSCwb70401	Patch 2 - Services do not start due to "Integrity check failed" error
CSCwc09104	Guest redirect with authentication virtual LAN no longer works on ISE 3.1
CSCwa17925	After fixing failed pre-upgrade check, Proceed button is still not available

Caveat ID Number	Description
CSCwb86283	ISE Deployment : All nodes throw OUT_OF_SYNC error as a result of incorrect certificate expiry check
CSCwb09861	CIAM: glib 2.56.4
CSCwb09860	CIAM: openssl 1.1.1g
CSCvy69483	CIAM: libgcrypt 1.5.3
CSCwa79799	PermSize attribute on sysodbcini file is missing
CSCwa97357	Cisco ISE does not send $mobilenumber$ value in the SMTP API body
CSCwb37760	Sponsor Portal shows error 500 when "Allow kerberos SSO" portal setting is enabled
CSCwb94890	Key Performance Metrics report has no entries for 8 AM and 9 AM every day
CSCwb09045	ISE PSN nodes crash due to incorrect cryptoLib initialization
CSCwa90930	Queue size needs to be capped on RMQ in 3.x
CSCvz24558	Spring Hibernate TPS upgrade (Hibernate 5.5.2, Spring 5.3.8)
CSCwa75348	ODBC Behavior Failover Issues
CSCwb04898	Unable to restore CFG backup from linux SFTP repository if the file is owned by a group name without space
CSCwb57665	ISE Evaluation for Struts2 CVE-2021-31805
CSCwb43007	Posture policy page does not load for SAML login
CSCvz94133	Configuration backup fails due to "EDF_DB_LOG"
CSCwc41697	Data dump transfer between nodes fail during upgrade due to connection error
CSCwa76896	Duplicated column "Failure Reasons" is found in RADIUS Authentications Report
CSCwa47133	ISE Evaluation log4j CVE-2021-44228
CSCwb05532	Location of "Location" and "Device Type" fields keep changing whenever Network Devices tab is clicked
CSCvz42996	CIAM: glibc 2.17
CSCwa91335	Default domain configuration in Passive-Syslog provider does not work in ISE 3.1
CSCwb81416	Cisco ISE GUI does not load after login
CSCwb01854	Upgrade External Radius Server List does not show up after upgrading to Cisco ISE 3.0 or above
CSCwb27857	Unable to login into GUI of MnT nodes using RSA 2FA in distributed deployment

Caveat ID Number	Description
CSCwc09737	CIAM: cups 1.6.3
CSCwb02129	SSH to Cisco ISE fails on maually imported SSH Public Keys
CSCwb36849	Cisco ISE must avoid sending Empty Cisco AV-Pairs in access-accept packets
CSCwb41741	Invalid character error in Admin Groups
CSCwb32466	Unable to delete endpoint identity group created via REST API if no description is set
CSCwb57675	Cannot disable "Dedicated MnT" Option from GUI after it is enabled
CSCwa82553	Default route is on the incorrect interface if bonding is configured
CSCwa04370	Default route is removed or tied to the wrong interface after upgrading
CSCvw90778	T+ ports (49) are still open if disable Device admin process under deployment page
CSCwb11147	Improvement to logs needed with Conflict handling SGT-IP mapping with Virtual Networks
CSCwb40942	From address to send email is invalid if it does not end with .com or .net
CSCwb96942	Application Server is stuck in the initializing state after configuration backup is restored
CSCwb98854	Cisco ISE does not update expiry date after SLR license is updated
CSCvz43125	CIAM: nettle 3.4.1
CSCwb40349	Invalid Characters in External RADIUS Token Shared Secret.
CSCwb38069	Services fail to start after backup from old ISE vrsion 2.6 is restored
CSCwb01843	Timezone update should happen automatically
CSCwb29357	AD User SamAccountName parameter is null for user sessions
CSCwb80572	Application Server stays in Initializing state after installing Cisco ISE 3.1 Patch 3 on Cisco ISE Patch 2
CSCwb39964	Cisco ISE can login to GUI with disabled shadow admin accounts with external identity source
CSCwb07504	Sorting internal users based on User Identity Groups does not work in Identities under Identity Mangement tab
CSCwb88129	CIAM: samba 4.13.3
CSCwc39844	Services auto restart fail with an internal error during IP address change in eth 1
CSCwa80553	CIAM: samba 4.8.3
CSCwb23028	Inaccurate dictionary word evaluation for passwords

Caveat ID Number	Description
CSCvk25808	Unable to edit or remove Scheduled Reports if the admin who created them is no longer available
CSCwa88948	CIAM: cryptography 2.3
CSCwb93156	TrustCertQuickView gives the same information for all trusted certificates
CSCwb40131	400 Bad Request error is thrown when Internal User is enabled with external password type using Rest API.
CSCwb32492	Application server restart on all nodes after changing the Primary PAN Admin certificate
CSCvv02086	Add ability to disable TLS 1.0 and 1.1 on ISE PIC node
CSCwc03220	Removing an IP Access list from ISE destroys the distributed deployment
CSCwc57630	3.2 BETA : ISE GUI is not accesible after enabling TLS 1.0.

Resolved caveats in Cisco ISE release 3.1 cumulative patch 3

The following table lists the resolved caveats in Release 3.1 cumulative patch 3.

Caveat ID Number	Description
CSCwb70401	After installing patch 2 services are stuck due to "Integrity check failed" error
CSCwa55996	New objects do not exist in the condition studio
CSCwa51150	WLC failed to validate EAPOL Key M2 with ISE 3.1
CSCvz91603	Unable to fetch the attributes from ODBC after upgrading to ISE 3.0 patch 3
CSCwa07580	Could not create Identity User if username includes $
CSCwa09113	Single Byod Flow with Internal CA failing with "12557 User Auth failed because OCSP status is unknown" error
CSCvy99582	Upgrade from ISE 2.4 patch 13 to ISE 2.7 fails if external RADIUS server is configured
CSCwa37040	backup-logs using public key encryption on the ISE CLI does not allow for caputure of core files
CSCvz67479	Local Log Settings tooltip on all fields shows irrelevant and unuseful Trust Certificates
CSCwa17470	ISE 3.1 SAML admin authentication fails when user assertion contains multiple values in the "Groups" claim
CSCwa35293	ISE 2.7 Authentication success settings shows success/success url
CSCvz88188	TACACS authorization policy querying for username fails because username from session cache is null

Caveat ID Number	Description
CSCwa26210	nextPage field is missing from the json response of API 'GET /ers/config/radiusserversequence'
CSCwa88845	Device Port Network Conditions does not validate interface ID
CSCwa11658	CIAM: gnutls 3.6.14
CSCwa11659	CIAM: libx11 1.6.8
CSCwa11657	CIAM: python 3.6.8
CSCwa11654	CIAM: file 5.33
CSCwa11655	CIAM: sysstat 11.7.3
CSCwa78479	Cisco Identity Services Engine Assessment of CVE-2021-4034 Polkit
CSCwa20354	Node database utilization information is not properly displayed in Operational Data Purging > Database Utilization window
CSCvz79665	Microsoft Intune Graph Url change from graph.windows.net/tenant to graph.microsoft.com
CSCwa16401	Get-By-Id server sequence returns empty server list after first change made on the sequence via GUI
CSCwa48465	Reports are unusable due to misshandling fields with multiple values
CSCvx54894	Sponsor Portal admin unable to create random guest accounts with 1 hour duration or less
CSCvz71872	CIAM: nss - multiple versions
CSCvz37241	Queue Link Error:WARN:{socket_closed_unexpectedly;'connection.start'}
CSCvv04957	GRUB2 Arbitrary Code Execution Vulnerability
CSCvz78841	CIAM: openssh 7.6
CSCvz90468	Internal users using External Password Store are getting disabled if we create users using API flow
CSCvy84989	Enabling cookies for POST /ers/config/internaluser/ causes Identity Group(s) does not exist error
CSCvz56358	ISE 3.0 checks only the first SAN entry
CSCwa57705	IP-SGT mapping does not link with new network access device group
CSCvx23375	ISE authorization profiles option get truncated during editing/saving (Chrome only)
CSCwa32312	RCM and MDM flows fail because of session cache not being populated
CSCvz65576	Full upgrade not working with patch when CLI or disk repository is used

Caveat ID Number	Description
CSCwa33462	CSV NAD import is rejected due to special symbol @ at the beginning of RADIUS shared secret
CSCvz85074	Fix for CSCvu35802 breaks AD group retrieval with certificate attribute as identity in EAP-Chaining
CSCwa13696	ISE 3.1 Guest Username/Password Policy is not modifiable
CSCwa23207	Multiple runtime crashes seen due to memory allocation inconsistency
CSCwa47190	AD security groups cannot have their OU end with dot character in Posture Policy
CSCwa11678	CIAM: binutils 2.30
CSCwa11679	CIAM: json-c 0.13.1
CSCwa57955	Posture firewall remediation action unchangeable
CSCwa41166	RegEx expressions in TACACS Command Sets malformed
CSCwa17718	Session service unavailable for pxGrid Session Directory with dedicated MnT
CSCvz18627	PEAP session timeout value restricted to max 604800
CSCwa78042	ISE 3.1 is requesting ISE-PIC licenses from Smart account
CSCwa53231	CIAM: nss - multiple versions
CSCwa08802	ISE 3.1 on AWS gives a false negative on the DNS check for Health Checks
CSCwa49859	Attribute value dc-opaque causing issues with Live Logs
CSCwa03126	ISE CPP not loading correctly for some languages
CSCvz83204	ISE unable to fetch the url attribute value from improper index during posture flow
CSCvz74457	ERS API does't allow for use of dot character in "Network Device Group" name or create / update
CSCvy45345	Eap-chaining authorization failure due to machine authentication flag set to true incorrectly
CSCvz36192	GET for dacls using /ers/config/downloadableacl does not return a value for nextPage or previousPage
CSCwa04454	ISE 3.0 & 3.1: Device Admin License alone should allow access to all TACACS menus
CSCwa11662	CIAM: lz4 1.8.3
CSCwa11661	CIAM: glibc 2.28
CSCvy76328	IPv6 changes the Subnet to /128 when using the duplicate option from Network device tab

Caveat ID Number	Description
CSCwa20309	Unknown NAD and Misconfigured Network Device Detected alarms
CSCwa56934	Inconsistent sorting on ERS APIs for endpoint group
CSCwa45316	MDM intune integration broken for vpn user on ISE 3.1
CSCvz63405	ISE client pxGrid certificate is not delivered to DNAC
CSCvn27270	Unable to create network device group with name Location or Device Type
CSCwa15191	Endpoint stuck in posture unknown state
CSCwa13877	ISE displays an alarm stating an invalid response from licensing cloud
CSCwa46758	Deleted Root Network Device groups are still referenced in the Network Devices exported CSV report
CSCvz71284	SNMPv3 COA request is not issued by ISE 2.7
CSCwa94984	ISE API add user operation with long custom attribute string takes around 4 minutes using Curl
CSCvw09460	Updated fields list for PUT on /erc/config/authorizationprofile/{id} usually empty
CSCvw90586	Unable to change network Device group Name and Description at the same time
CSCvs55875	Existing routes are not installed in routing table after MTU change
CSCwa47566	ISE Conditions Studio - Identity Groups Drop-down limited to 1000
CSCvz34849	DELETE /ers/config/networkdevicegroup/{id} not working; CRUD exception
CSCvy71309	CIAM: tcp-dump 4.9.3
CSCvy16894	Authorization profile throws an error when special characters are used
CSCwa47133	ISE Evaluation log4j CVE-2021-44228
CSCwa20152	CoA was not initiated for switches for which matrix was not changed, hence Policy sync failed
CSCvz83753	Empty User Custom attribute included in Authorization Advanced Attributes Settings results in incorrect AVP
CSCvz75902	ISE replacing pxGrid certificate when generating ISE internal CA
CSCwa43187	"Queue Link Error: Message=From Node1 To Node2; Cause=Timeout" error seen when NAT is used
CSCwa59924	ISE 3.1 Patch 1: Unable to connect to ISE via SSH when FIPS is enabled
CSCwa19573	Catalina.out file is huge because of SSL audit events
CSCwa52114	CIAM: sqlite 3.18.2

Caveat ID Number	Description
CSCwa52110	When SNMP config is set on the network device, a delay of 20 seconds is introduced while processing SNMP record
CSCwa59237	Deployment-RegistrationPoller causing performance issues on PAN node with 200+ internal certificates
CSCwa38023	ISE 3.1: Unable to generate pxGrid certificates with Active Directory superadmin
CSCwa32814	ISE configured with 15 Collection filters hides the 15th filter
CSCwa60873	Optimize bouncy-castle class to improve performance on PAN
CSCvz79518	Serviceability: "DNS Resolution Failure" alarm should show ISE server
CSCvy96761	Session cache must be updated during EAP chaining flow to handle relevant identities
CSCwa16291	Guest Portal fields causing words to be repeated for Apple VoiceOver
CSCvz90852	Success page is blank and Done button not enabled in Hotspot Guest Portals
CSCwa05404	Sessions are not removed when the Tacacs+ requests resulted in "Could not find selected service" error
CSCvz95326	Unable to add more than one ACI IP address/hostname when trying to enable ACI integration in ISE
CSCwa08018	ISE 3.1 - GUI is not working when IPv6 disabled globally
CSCwa11682	CIAM: pcre 8.41
CSCvz93230	Guest portal does not load if hosted on a different interface from Gig0
CSCwa53499	REST ID is fetching the groups from Cloud when the connector settings page is opened
CSCwa56771	ISE 3.0p2 - Monitor All setting displays incorrectly with multiple matrices and different views
CSCwa47221	AD security groups cannot have their OU end with dot character in Client Provisioning Policy
CSCwa52133	CIAM: libsolv 0.7.16
CSCvz60870	High Active Directory latency during high TPS causes HOL Blocking on ADRT
CSCvs95495	Reauthentication issue seen in third party devices
CSCwa11633	ISE 3.0 APIC Integration: Failed to create security groups
CSCwa18443	Need to handle Posture expiry when 8 octet MAC is present in endpoint on the deployment node
CSCwa67433	Cannot export SAML provider info xml file from ISE GUI
CSCwa59621	Inconsistent sorting on ERS API for identity groups

Resolved caveats in Cisco ISE release 3.1 cumulative patch 1

The following table lists the resolved caveats in Cisco ISE release 3.1 cumulative patch 1.

Caveat ID Number	Description
CSCvo39514	MnT log processor is not running because collector log permission.
CSCvq53373	/ers/config/<obj>/bulk/submit returning invalid Location URI /ers/config/<obj>/bulk/submit/<bulkID>
CSCvs04091	Blanket bug for code enhancements for MnT component
CSCvt25277	2.4p12 patch install stuck forever
CSCvu47280	A race condition was found in the mkhomedir tool shipped with the oddjo
CSCvu94544	ISE 3.0 BH : TACACS live logs do not give an option select Network Device IP
CSCvv96532	DOC: unknown maximum time difference for thisUpdate of OCSP response
CSCvw65181	CIAM found poi vulnerable
CSCvw78289	Auth Passed live logs are not seen when using a profile name with more than 50 characters
CSCvx14400	Multiple Vulnerabilities in glibc
CSCvx43866	3.0P2:Accounting Report Export is taking more time to complete.
CSCvx55668	CIAM found netty vulnerable
CSCvy14905	CTS-SXP-CONN : ph_tcp_close from device to ISE SXP connection - Hawkeye
CSCvy43246	[CFD] User unable to create a guest SSID during Portal Creation step - ISE is busy error
CSCvy53842	Certificate Validation Syslog Message Sent During Specific Certificate Audits--ISE
CSCvy69539	CIAM: openjdk - multiple versions
CSCvy71229	CIAM: libx11 1.6.8
CSCvy71232	CIAM: glibc 2.28
CSCvy71238	CIAM: gnupg 2.2.9
CSCvy71239	CIAM: systemd 219
CSCvy71240	CIAM: vim 8.0.1763
CSCvy71261	CIAM: nettle 3.4.1
CSCvy71292	CIAM: unbound 1.7.3
CSCvy71296	CIAM: pcre2 10.32

Caveat ID Number	Description
CSCvy71313	CIAM: cpio 2.12
CSCvy71322	CIAM: libarchive 3.3.2
CSCvy71345	CIAM: network-manager 1.22.8
CSCvy71690	Customer fields in guest portal contains & - $ #
CSCvy75191	Cisco Identity Services Engine XML External Entity Injection Vulnerability
CSCvy77472	CIAM: librepo 1.11.0
CSCvy81435	ISE Guest SAML authentication fails with "Access rights validated" HTML page
CSCvy82023	Incorrect Posture Compound Condition Hotfixes
CSCvy88092	CTS PAC not activating on Switch: via ISE 3.1 build 3.1.0.477
CSCvy88764	CIAM: go 1.15.7 CVE-2021-33194
CSCvy92040	ISE restore popup menu displays wrong text
CSCvy92536	ISE 3.0 Device Admin License alone should allow access to Administration > System > Logging menu
CSCvy93847	Possible to choose SPAN without Policy persona in NAD Send configuration changes to device CoA
CSCvy94427	posture lease breaks for eap chaining from 2.7
CSCvy94511	TACACs report showing duplicate entries due to EPOCH time being null
CSCvy94553	TACACS Authentication report shows duplicate entries
CSCvy94818	EP's incorreclty profiled as "cisco-router" due to nmap performing aggressive guesses
CSCvz00258	SessionCache not cleared for Tacacs AuthZ failures results in high heap usage and auth latency
CSCvz00659	Special characters in Banner blocking SFTP repo
CSCvz01485	ISE 2.7 patch 4 unable to upload .json file for Umbrella security profile.
CSCvz05383	P1PNSBaseline: SuperMnT: on last 30days Radius Auth report takes ~5mins with filter
CSCvz05966	ISE 2.6 p 9, Default permissions can't go back to default group Internal after adding a new group
CSCvz07191	ISE GUI stuck at loading if AD group does not exist when using cert based auth for GUI access
CSCvz07823	ise 2.7 Failed to add endpoint to group

Caveat ID Number	Description
CSCvz08813	Not able to scroll to different pages in Issued certficates page
CSCvz17020	ISE GUI shows all the licenses as Out of Compliance - Smart Licensing
CSCvz18848	Agentless posture breaks for locale
CSCvz20020	Okta redirection fails for first ID store and works when second ID store is assigned
CSCvz20770	Unable to see the UI pxgrid pages, if we enabled&disabled pxgrid at deployment tab on secondary node
CSCvz27791	ISE: Application server stuck initializing after backup restore due to mdm configuration
CSCvz28133	User unable to generate support bundle
CSCvz33839	menu access customization is not working
CSCvz35550	ISE Health Check MDM Validation false alarm
CSCvz37623	NTP (' - ') source state description missing in ISE CLI
CSCvz43038	CIAM: libxml 2.9.1
CSCvz43123	CIAM: jspdf 2.3.0
CSCvz43126	CIAM: systemd - multiple versions
CSCvz43154	CIAM: podman 1.6.4
CSCvz43183	Sponsor Permissions are not passed to Guest REST API for "By Name" calls.
CSCvz44655	ISE manage account selection issue
CSCvz45150	ISE PIC 3.1 Request traditional license
CSCvz46933	CIAM: jsoup 1.10.3
CSCvz49086	ISE 3.0 TimesTen connection closed when an SQLException is encountered
CSCvz49871	ISE GUI : net::ERR_ABORTED 404 : /admin/ng/nls/fr-fr/
CSCvz50255	CIAM: bind 9.11.20
CSCvz55258	Cisco:cisco-av-pair AuthZ conditions stopped working
CSCvz57267	Inability to import ISE certificates issued for PAN to other nodes in spite of the SAN field fqdn.
CSCvz61191	ISE3.1 No response when click "choose file" on import Endpoints from CSV file page.
CSCvz63643	ISE 2.7: EndpointPersister thread getting stopped
CSCvz64833	CIAM: libgcrypt 1.5.3

Caveat ID Number	Description
CSCvz65182	If we set mtu greater than 1500 then the mtu value is not setting persistently across reboot.
CSCvz66289	Local disk management UI for uploading file is broken
CSCvz67479	Local Log Settings tooltip on all fields shows irrelevant and unuseful 'Trust Certificates'
CSCvz68091	Configuration changes to Guest types is not updated in audit reports
CSCvz72034	ISE 3.1:While updating Network Device from DNAC, Shared Secret/password is empty or masked
CSCvz72069	Pxgrid shown disabled on Summary page for ISE-PIC
CSCvz72208	ISE 3.1 : Authentication tab shows blank result in Context Visivility
CSCvz72225	adding FQDN in discovery host, Discovery host: invalid ip address or host name
CSCvz73445	Agentless Posture for Windows 10 devices not passing AntiMalware check -
CSCvz77482	ISE 3.0 Can't deselect the 'location' settings as part of the guest self registration portal
CSCvz80829	Version pre-check fails for 3.2 full upgrade.
CSCvz85117	ISE Health Check I/O bandwidth performance check false Alarm
CSCvz87476	Unsupported message code 91104 and 91105 Alarms
CSCwa00729	All NADs got deleted due to one particular NAD deletion
CSCvz86020	live log/session not showing latest data due to "too many files open" error
CSCwa12273	AD users in Super Admin group can't create/edit admin user with error "Operation is not permitted"
CSCvz66279	Radius reports older than 7 days are empty (regression of CSCvw78289)
CSCvz91116	Oracle process are increasing and gettingTNS:connection closed

Resolved caveats in Cisco ISE release 3.1

The resolved caveats in Cisco ISE Release 3.1, have parity with these Cisco ISE patch releases: 2.6 Patch 9, 2.7 Patch 4, and 3.0 Patch 2.

Caveat ID Number	Description
CSCwa04370	ISE 3.1 shows incorrect outgoing interface for the default interface if two interfaces are configured with IP addresses and the default gateway references the subnet on eth1
CSCwa82553	ISE 3.1 default route is on the incorrect interface if bonding is configured
CSCuo73496	RADIUS maximum session-timeout value restricted to 65535
CSCvf61114	ERS Create/Update for "Authorization Profile" failing XML schema validation

Caveat ID Number	Description
CSCvf88737	Blank guest portal window seen in portal created in portal builder
CSCvg75448	Customization for support information in Client Provisioning portal is missing
CSCvg77872	No logo in guest approval email when portal is set to Sponsored-Guest Portal
CSCvh04231	Guest Remember Me RADIUS accounting and access accept not sending guest username
CSCvi53134	Account used for AD join may become locked after passive-id service is enabled
CSCvi59005	Unable to see complete list of AD groups when using scrollbar
CSCvk11224	Problem with renaming the reports
CSCvm47584	Unable to configure grace period for more than 1 day because of posture lease
CSCvn25548	MnT API call with admin credentials disables the account
CSCvn38371	Ability to suppress session information pop up when logging in to GUI
CSCvo02275	Profiling and conditions studio not loading or taking up to 30 minutes
CSCvo56767	Error when attempting to change ISE-PIC GUI admin user settings
CSCvo75723	When running a report for endpoint purge, no reports are shown if the purged endpoint count is 0
CSCvp88242	Bad Request error when refreshing My Devices portal
CSCvq44063	Incorrect DNS configuration can lead to TACACS or RADIUS authentication failure
CSCvq58506	Show running-config fails to complete
CSCvr22065	Import NAD is failing with an error when shared secret key has special character
CSCvr76539	Changes to Network Device Groups not reflected in Change Audit logs
CSCvs24459	Unable to manage ISE internal network access users without an Identity Group
CSCvs27232	RADIUS Authentication Troubleshooting window not filtering properly
CSCvs29611	Cisco ISE 2.4 patch 5 crashing frequently and generating core files
CSCvs81248	PassiveID alarms should be triggered for inactivity for each DC separately
CSCvs81264	PSN should be capable of identifying delays in mappings from PassiveID agent
CSCvt64739	Application server takes more time to initialize
CSCvt65332	While updating the Profile Description field in Client Provisioning Resources window, if Enter is used to create a new line, "Fail to receive server response due to the network error" message is displayed

Caveat ID Number	Description
CSCvt85370	Posture Condition failed with "Check vc_visInst_v4_CiscoAnyConnectSecureMobility Client_4_x is not found" error
CSCvt94587	"Plus License is out of compliance" message seen while regenerating the ISE Root CA
CSCvu04874	Suspected memory leak in io.netty.buffer.PoolChunk
CSCvu05121	Guest email not sent after changing SMTP server
CSCvu14215	Sponsor group membership removed when adding or removing AD group
CSCvu22058	ISE with DUO as External RADIUS Proxy drops access-reject
CSCvu33861	ISE 2.4 patch 6: REST API MnT query to get device by MAC address taking more than 2 minutes
CSCvu47779	Change Configuration Audit report missing IP Address and modified properties in CSV export
CSCvu62938	Posture fails when primary PSN or PAN is unreachable
CSCvu84184	Certificate chain is not sent on the guest portal
CSCvu84773	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvu87758	Guest password policy settings cannot be saved when set to ranges for alphabets or numbers
CSCvu89715	Time Vs Throughput chart in ISE Health Summary report using wrong units
CSCvu90761	ISE Radius Live Sessions window showing No Data Found
CSCvu91039	ISE not doing lookup for all MAC addresses causing redirectless Posture to fail
CSCvu94025	ISE should either allow IP only for syslog targets or provide DNS caching
CSCvu97657	ISE 2.4 Application server going to Initializing state on enabling endpoint debugs
CSCvv00951	Application server crashes while transitioning into stopping state
CSCvv02998	MAC 11 Big sur BYOD flow failed
CSCvv04416	Endpoint data not visible on secondary Admin node
CSCvv04957	GRUB2 Arbitrary Code Execution Vulnerability
CSCvv08466	Log Collection Error alarms appear
CSCvv09127	Guest API allows restricted sponsor to create guest accounts even for the unallowed guest type
CSCvv10683	Session cache for dropped session not getting cleared and causing High CPU on the PSNs

Caveat ID Number	Description
CSCvv14001	Authorization profile not saved with proper attributes when Security Group selected under common tasks
CSCvv14390	Max Sessions Limit is not working for Users and Groups
CSCvv15060	Going back to network list removes the applied filter
CSCvv16401	pxGrid internal client ping failed
CSCvv19065	Not able to see the guest identity in the DNAC Assurance window
CSCvv25102	Modify TCP settings to enhance TACACS+ and TCP on ISE
CSCvv27690	While renewing ISE certificate for HTTPS, EAP, DTLS, PORTAL, only Portal and Admin roles gets applied
CSCvv29190	BYOD Flow is broken in iOS 14 beta
CSCvv29737	DNA ACA Security Groups sync fails with JDBCException error
CSCvv30133	Discovery host description text is misleading
CSCvv30161	Live session details report show incorrect authorization profile and policy for VPN Posture scenario
CSCvv30226	Livelog sessions show incomplete authorization policy for VPN Posture scenario
CSCvv30274	Context Visibility shows incorrect authorization profile and policy for VPN Posture scenario
CSCvv31500	ISE Guest portal registration and expiration email need to maintain format entered in the portal
CSCvv35921	Cannot start CSV exporting for Selected User in internal ID Store
CSCvv36189	RADIUS passed-auth live logs not sent due to invalid IPv6 Address
CSCvv38249	Manual NMAP not working when only custom ports are enabled
CSCvv39000	Unable to create posture condition for LANDESK
CSCvv41935	PSK cisco-av-pair throws an error if the key contains < or > symbols
CSCvv43383	NFS repository is not working from GUI
CSCvv44401	Generate self-signed certificates and CSR default parameters doesn't match with pre-installed self-signed certificate
CSCvv45063	Internal CA Certificate not getting deleted when node is removed from deployment
CSCvv45340	Error storing the running-config lead to loss of startup config
CSCvv46034	Device admin service is getting disabled when updating TACACS configuration

Caveat ID Number	Description
CSCvv46958	TrustSec enabled NADs not showing in TrustSec Matrices when NDG column exceeds 255 characters
CSCvv47849	Mapped SGT entry cleared from Authorization Rules if Security Group name is modified in Cisco DNA Center
CSCvv50028	Heap Dump generation fails post reset-config of ISE node
CSCvv50168	ISE must allow Posture Grace Period more than 30 days
CSCvv50721	Can't get the download link of NetworkSetupAssistant.exe using Aruba dynamic URL redirect
CSCvv52637	ISE Hotspot guest portal flow broken
CSCvv53221	Application server marked as Initializing when ISE_EST_Local_Host RADIUS shared secret is empty
CSCvv54761	Export of current active session reports only shows sessions that has been updated since midnight
CSCvv54798	Context Visibility CSV exported from CLI not showing IP addresses
CSCvv55663	ISE 2.6/2.7 Repositories get deleted post ISE node reload
CSCvv57628	Suspended Guest User is not automatically removed from Endpoint Group
CSCvv57639	Saving command with parenthesis in TACACS command set gives an error
CSCvv57830	Group lookup failed as empty value was appended to the context
CSCvv58629	Certificate Authority Service initializing EST Service not running after upgrade to ISE 2.7 patch 2
CSCvv59233	ISE RADIUS Live Log details missing AD-Group-Names under Other Attributes section
CSCvv60014	Operational backup throws error if available free space in /opt folder is 1 TB or greater
CSCvv60353	Authentication summary report gets stuck if the total records are more than 5M
CSCvv60686	ISE SXP should have a mechanism to clear stale mappings learned from session
CSCvv60923	Need to add the ability to use a forward slash in the IP data type of internal user custom attribute
CSCvv61732	Unable to create unique community string for different SNMP servers
CSCvv62382	Proxy bypass settings does not allow upper characters
CSCvv62549	Custom Attribute from Culinda not showing in endpoint GUI page
CSCvv62729	Network Device API call throws error 500 if you query an non-existent network device

Caveat ID Number	Description
CSCvv63548	PSN rmi GC collection not working properly causing memory leak in PassiveID flow
CSCvv64190	Case sensitivity on User Identity Groups causes "Select Sponsor Group Members" window to not load
CSCvv65036	Memory Leak on PSN nodes
CSCvv67051	Radius Server Sequence window showing "no data available"
CSCvv67091	Cisco Identity Services Engine Untrusted File Upload Vulnerability
CSCvv67743	Posture Assessment by Condition report displays No Data with Condition Status filter
CSCvv67935	Security Group values in Authorization Profile disappear shortly after fetching
CSCvv68028	Can't modify AUP Text
CSCvv68293	ISE not consuming plus license when using local or global exceptions
CSCvv72418	ISE 3.0 REST ID log file not included in support bundle
CSCvv74361	ISE 3.0 Health Check License validation false Alarm
CSCvv77007	ISE constantly sending internal Super Admin user requests to external RADIUS token server
CSCvv77530	Unable to retrieve LDAP Groups/Subject Attributes when % character is used twice or more in bind password
CSCvv77914	Client Provisioning window does not show current settings properly
CSCvv77928	Bulk certificate generation failed with "An unexpected error occurred" message after primary PAN failure
CSCvv78097	Missing local disk utilization information
CSCvv79940	ISE generating CSR with hostname-x in SAN gives an error
CSCvv80113	Posture auto-update not running
CSCvv80297	Need DigitCert Global Root G2 in CTL for ROPC
CSCvv82806	Network Device IP filter does not match IPs that are inside subnets
CSCvv83510	Upgrade failing at RuleResultsSGTUpgradeService step
CSCvv85588	High memory usage on the PSN nodes with PassiveID flow
CSCvv91007	Smart Licensing Entitlement tab gets stuck at "Refreshing" if there is connection failure
CSCvv91234	ISE 2.6 scheduled reports are not working when primary MnT is down
CSCvv91684	ISE collection filters not displayed in GUI

Caveat ID Number	Description
CSCvv92203	"NetworkAuthZProfile with entered name already exists" message seen while trying to create an SGT with name "Employees"
CSCvv92613	Users that do not belong to the sponsor group are able to login in the sponsor portal
CSCvv92638	Cannot configure scheduled config and operational backup with start date same as current day
CSCvv93442	Double Slash "//" added in File Path for SFTP servers
CSCvv94791	GBAC configuration not synced between DNAC and ISE
CSCvv95150	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability
CSCvv95516	ISE PIC Licensing window is not loading
CSCvv96532	Maximum time difference not specified for "thisUpdate of OCSP response"
CSCvv99093	ISE nodes intermittently trigger Queue Link alarms
CSCvw00375	Unable to load Context Visibility window for custom view in ISE 2.7 patch 2
CSCvw01225	ISE configuration restore fails at 40% with "DB Restore using IMPDP failed" error
CSCvw01829	ISE GUI login page shows error while using Chrome version 85/86
CSCvw02887	Memory leak after adding AD Groups for PassiveID flow
CSCvw03693	NTP does not work because internal user 'chrony' not created
CSCvw06722	Sponsor is unable to view the list of created guest users
CSCvw08292	ACI mappings are not being deleted after a delete message
CSCvw08330	Posture does not work with dynamic redirection on third party NADs
CSCvw08602	Not throwing error for IP overlap case
CSCvw09827	High CPU on PSN node
CSCvw16237	Scheduled operational data backups not being triggered after Primary MnT reload
CSCvw17908	Pushing IP to SGT mapping from ISE to switch doesn't work if default route is tagged
CSCvw19785	Editing external data source posture condition is showing always the wrong AD
CSCvw20021	NAD Location is not updated in Context Visibility ElasticSearch
CSCvw20060	Agent marks DC as down if agent service comes up before windows network interface
CSCvw20636	Authorization Profiles showing "No data available" after NAD profile is deleted
CSCvw24227	Endpoints not purged due to an exception
CSCvw24268	Cisco Identity Services Engine Untrusted File Upload Vulnerability

Caveat ID Number	Description
CSCvw25285	PassiveID is not working stable with multi-connect syslog clients
CSCvw26415	ISE 3.0 not importing certificates missing CN and SAN into Trusted Certificate Store
CSCvw26570	International Phone Number dropdown box not working in ISE 2.7
CSCvw28441	NADs shared secrets are visible in the logs while using APIs
CSCvw29490	Internal User custom attributes are not sent in CoA-Push
CSCvw31269	SAML groups do not work if they are applied in the Sponsor Portal Groups
CSCvw33115	ISE MnT Live Session status is not changing to Postured in VPN use case
CSCvw34491	Enabling Essentials licenses only block access to Network Devices tab
CSCvw36486	GUI not accessible after applying IP Access restrictions
CSCvw36743	ISE Service Account Locked and WMI not established due to special characters in password
CSCvw37844	ANC CoA not working as ISE uses hostname for internal calls
CSCvw38530	Exception shown in ise-psc.log for repository while loading Backup and Restore window
CSCvw38853	Sophos 10.x definition missing from Anti-malware condition for MAC OSX
CSCvw44120	Guest portal creation failure with ISE 3.0
CSCvw46096	ISE 3.0 Syslog provider cannot apply configuration
CSCvw48396	Cisco ADE-OS Local File Inclusion Vulnerability
CSCvw48403	ISE is not processing gathered SNMP information for endpoint
CSCvw48697	API IP SGT mapping not returning result for [No Devices]
CSCvw49938	No TACACS Command Accounting report for third party device with a space before TACACS command
CSCvw50381	CoA-disconnect is not issued by ISE for Aruba WLC when grace access is expired
CSCvw50829	AD security groups cannot have their OU end with dot character on RBAC policies
CSCvw51787	ISE is not allowing to import CA signed certificate on top of self-signed certificate
CSCvw51801	Session which was previously having Postured Live Session state is moving to Started upon receiving Accounting Interim Update from NAD
CSCvw53412	SB should collect Hibernate.log
CSCvw54878	ISE does not display Full Authorization rules if it has 50 rules or more in Japanese GUI

Caveat ID Number	Description
CSCvw55793	ISE fails to send CoA from PSNs with "Identifier Allocation Failed" error
CSCvw61589	RADIUS requests dropped after deleting policy sets
CSCvw61786	All Processes need to be stopped before dropping schema objects
CSCvw63264	ISE 3.0 policy condition studio GUI bug
CSCvw66483	RADIUS server sequence gets corrupted when selected external server list is modified
CSCvw68480	Total mappings not displayed properly when using multiple SXP nodes in ISE deployment
CSCvw68512	Guest user is created with incorrect lifetime
CSCvw68944	Sponsor portal shows wrong week information on setting date while using Chinese language
CSCvw69977	"All SXP Mapping" table contains terminated sessions on ISE
CSCvw73928	NTP sync failure alarms that are not relevant need to be changed
CSCvw75397	MnT node name set to NULL when IP access enabled
CSCvw75563	HotSpot Guest portal displays Error Loading Page when passcode field contains special characters
CSCvw76847	ISE Conditions Library corruption during Pen test
CSCvw77219	Dot1x authentication failed due to duplicate manager
CSCvw78019	NTP out of sync after upgrade to ISE 2.7
CSCvw78269	CWE-20: Improper input validation for Create Node Group
CSCvw78289	Authentication Passed live logs are not seen when using a profile name with more than 50 characters
CSCvw80520	"Radius Authentication Details" report takes time when ISE Messaging Service is disabled
CSCvw81454	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerabilities
CSCvw82774	Sorting based on username doesn't work in User Identity Groups
CSCvw82784	TACACS+ Endstation Network Conditions scrollbar not working
CSCvw82815	Authorization profile CWA option does not work correctly with some network device profiles
CSCvw82927	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerabilities
CSCvw83296	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerabilities

Caveat ID Number	Description
CSCvw83334	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerabilities
CSCvw84127	Configuration Audit detail does not show which Policy Set was modified
CSCvw85599	TACACS+ Device Network Conditions and Device Port Network Conditions tabs scrollbar not working
CSCvw85860	ISE pxGrid exceptions should have ERROR log level instead of DEBUG
CSCvw87147	Live session is not showing correct active session
CSCvw87173	MAB authorization is failing if AD object representing the MAC address is in disabled state
CSCvw87175	MAB authentication via Active Directory passes with AD object disabled
CSCvw88881	DB Clean up hourly cron acquiring DB lock causing deployment registration failure
CSCvw89326	For PKI based SFTP, exporting GUI key for MnT node is only possible when it is promoted as PAN
CSCvw89818	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerabilities
CSCvw90961	RBAC rules not enforced in ISE 2.7
CSCvw93570	Unable to edit, duplicate, or delete guest portals.
CSCvw94603	Change in Polling interval not taking effect for external MDM server (Microsoft_intune)
CSCvw96371	Static policy and group assignment are lost from EP when updating custom attributes from API
CSCvw97905	Internal user export feature shows no error for invalid characters in password
CSCvx00245	Itune integration throws error while Test Connection works fine in MDM window
CSCvx00345	Unable to fetch Azure AD groups
CSCvx01272	Generate bulk certificates do not include ISE self-signed certificate
CSCvx01798	Adding a network device gives "Unable to load NetworkDevices" error
CSCvx04512	Admin access with certificate based authentication can be bypassed by going directly to login.jsp
CSCvx04692	Creating a node group named "None" breaks replication
CSCvx09383	Error seen when trying to sort endpoint's Applications by "Running process" in Context Visibility
CSCvx10186	ISE remains in eval expire state even after registering with Smart Licensing
CSCvx11857	Latency in loading certain pages due to stale certificate entries in ISE TrustCert Store

Caveat ID Number	Description
CSCvx15427	DNS Resolvability in Health Checks: False failures with ISE FQDN as CNAME
CSCvx18730	Sudo Privilege Escalation Vulnerability Affecting Cisco Products: January 2021
CSCvx22229	"ipv6 address autoconfig" gets removed when changing IP address of bond interface
CSCvx27632	Authorization should look up MAC address in format configured in ODBC Stored-Procedures window
CSCvx28402	Support bundle does not capture ise-jedis.log files on ISE 2.7 and later
CSCvx30276	On recreating Root CA, Jedis DB connection pool is not recreated
CSCvx32666	Authentication Method conditions not matching in Policy Set entry evaluation
CSCvx37149	SGA value under-provisioned for SNS 3515 running all personas on same node
CSCvx37297	Error 400 while authenticating to Sponsor portal with Single Sign-on/Kerberos user account
CSCvx37467	Sponsor portal gives "Invalid Input" if the "mobile number" field is unchecked in portal settings
CSCvx41826	Unable to get all tenable adapter repositories with Tenable SC 5.17
CSCvx43566	No login fail log when using external username and wrong password
CSCvx43825	Receiving acct stop without NAS-IP address keeps session in started state
CSCvx44815	ISE AD runtime should support rewrite a1-a2-a3-a4-a5-a6 to a1a2a3a4a5a6
CSCvx45481	CoA failure upon endpoint change to a new switch-port and Endpoint Identity Group change
CSCvx46638	In EAP chaining scenario, posture policy failed to retrieve machine AD group membership
CSCvx47691	Session Directory topic does not update user SGT attribute after a dynamic authorization
CSCvx47891	AMP events for new endpoints are not correctly mapped
CSCvx48922	Memory leak on TACACS flow
CSCvx53205	NIC bonding prevents MAR cache replication
CSCvx53905	Authorization policy conditions are not correctly formatted
CSCvx54213	Default Network Devices window requires Plus license to allow configuration
CSCvx57433	TrustSec policy matrix allows limited scrolling in ISE 3.0
CSCvx57545	isedailycron temp1 tracking is causing delay in AWR reports

Caveat ID Number	Description
CSCvx58516	Clicking a network device in Top N Authentication by Network Device report is redirecting to TACACS Authentication instead of RADIUS Authentication
CSCvx60818	ERS self-registration portal update is not deleting fields as expected in PSN
CSCvx61462	ISE Log Collection error "Session directory write failed"
CSCvx61664	ISE not updating the Json file information in the AnyConnect output config file
CSCvx64247	"Invalid phone number format" error seen on mobile devices using the Country-code drop-down option
CSCvx69701	Deployment went out of sync due to unavailabiltiy of database connections
CSCvx70633	ISE does not accept % in EXEC or Enable Mode password in network device trustsec configuration
CSCvx72642	REST authentication service is disabled when backup interface is configured
CSCvx78643	Emails sent for all system alarms using legacy data even when there is no email address configured in current deployment
CSCvx79693	Qualys integration is failing with ISE
CSCvx82808	MacOS Big Sur 11.x BYOD failing EAP-TLS when using a CA signed certificate
CSCvx85355	Increase the maximum allowable value of the posture grace period from 30 to 90 days
CSCvx85391	Internal user inactivity timer is not updated due to login letter case
CSCvx85675	ISE can't handle deletion/addition of SXP-IP mappings propagation due to race condition
CSCvx85807	Smart license of de-registration flow is not working in ISE and ISE-PIC
CSCvx86571	The instruction box should be removed when the login-page message is empty
CSCvx86915	UI issues on TrustSec window
CSCvx86921	RADIUS Token Identity Source Prompt vs Internal User prompt for TACACS authentication
CSCvx94452	EST service not running on ISE 2.7 patch 2 and above
CSCvx96190	Top Authorization report does not show filter in scheduled reports
CSCvx97249	PAN should not be listening on port 8905
CSCvx97501	ROPC authentication is failing with non Base64 characters in the password
CSCvx99151	Internal ERS user attempting to authenticate via external ID store causing REST delays
CSCvx99176	NAD IP definitions using - or * do not perform full IP comparison

Caveat ID Number	Description
CSCvy04443	MNT REST API for ReAuth fails when used in distributed deployment (with separate MnT)
CSCvy04665	TACACS Reports Advance filters not working when matching full numeric ID entries
CSCvy05954	All SXP Mappings window not displaying IPv6 mappings learned via Session
CSCvy06719	Manual Active Session report is empty
CSCvy07088	Agentless Posture doesn't install CA certificate chain in endpoint Trusted Store
CSCvy10026	Agentless Posture fails if ISE admin certificate CN is not equal to FQDN
CSCvy11617	Agentless posture breaks if Windows username includes a space
CSCvy14342	High CPU seen on PSN nodes from ISE 2.6 patch 3 onwards due to PIP query evaluation
CSCvy15058	Unable to update domains to be blocked/allowed via API
CSCvy15172	Cisco Identity Services Engine Self Cross-Site Scripting Issue
CSCvy17893	ISE REST API returns duplicate values for IP-SGT mappings
CSCvy18560	RADIUS Accounting Details report does not display Accounting details
CSCvy20277	Special characters allowed previously in Descriptions field for few objects no longer can be used
CSCvy23354	Maximum height of Description field in ISE authorization profile UI too small in FF 88
CSCvy24370	ISE not accepting more than 6 attributes to be modified in RADIUS server sequence configuration
CSCvy25533	"/opt/CSCOcpm/config/cpmenv.sh:line 396:<ipv6>:command not found" error seen during CLI backup
CSCvy25550	ISE does not accept name of custom attribute for Framed-IPv6-Address in the authorization profile
CSCvy30119	LDAP groups disappear from Sponsor group when making other changes to options
CSCvy32461	Sponsor user cannot edit data when phone/email fields are filled
CSCvy34977	Application Server stuck on initializing state due to certificate template curve type P-192
CSCvy36868	ISE 2.3 and later version do not support "cariage return" <cr> character in command-set
CSCvy38459	ISE 2.7 patch 3 GUI doesn't show all device admin authorization policies
CSCvy38896	AAA requests without Framed-IP value will cause exception in SXP process

Caveat ID Number	Description
CSCvy40845	Updating a custom attribute through ERS request updates another attribute as well
CSCvy41066	TACACS custom AV pair as condition in policies is not working
CSCvy42885	ISE Application server crash/restart due to cancellation of configuration backup
CSCvy45015	ISE Guest Self-Registration error for duplicate user when "Use Phone number as username" option is enabled
CSCvy46504	Intermittent error on Cisco DNA Center while trying to deploy policy
CSCvy48766	ISE installation fails with Database Priming Failed error when All Numbers subdomain is used
CSCvy51073	ISE authorization profile ERS update ignores accessType attribute changes
CSCvy58771	While editing a NAD, wrong device profile is being mapped
CSCvy60752	Setup wizard password does not supports hyphen after reset of config via CLI
CSCvy61564	ISE 2.7 Patch 3 ERS call is not accepting RADIUS shared secret with 3 characters
CSCvy61894	Generate key pair accepts space but cannot export key
CSCvy62875	[400] Bad Request error with SAML SSO OKTA on Apple devices
CSCvy63778	REST API for CoA works with any server IP
CSCvy65786	Configuring WMI with an AD account password containing % results in an error
CSCvy71690	Customer fields in guest portal contains & - $ #
CSCvy74456	Authentication via ISE fails with "Invalid login credentials" error
CSCvy74919	ISE internal users are not getting disabled after hitting inactivity timer
CSCvy76262	ISE DACL Syntax validator does not comply with ASA's code requirements
CSCvy76601	Delete 'All' function showing incorrect number of endpoints on confirmation popup
CSCvy76617	Need the Select ALL device option with or without filter in NAD page
CSCvy82023	Incorrect Posture Compound Condition Hotfixes
CSCvy82114	First/Last name wrongly displayed as Unicode of Chinese in Network Access Users window after upgrade
CSCvy90691	Duplicated RADIUS vendor ID can cause PSN to crash
CSCvz00034	The log level for OcspClient must be changed to ERROR instead of WARN
CSCvx59893	Inconsistency between ISE syslog level and message level

Cisco ISE release 3.1 files replaced on software download site

Cisco ISE 3.1 OVA, ISO, and upgrade bundle files have been replaced on the Cisco ISE Software Download site.

What changes are made?

- The following bugs are resolved in this build:
  - CSCwa04370: ISE 3.1 shows incorrect outgoing interface for the default interface if two interfaces are configured with IP addresses and the default gateway references the subnet on eth1
  - CSCwa82553: ISE 3.1 default route is on the incorrect interface if bonding is configured
- Option to skip ICMP, DNS, and NTP checks in the ZTP tool. For more information, see "Zero Touch Provisioning" in the Chapter "Additional Installation Information" in *Cisco ISE Installation Guide, Release 3.1*.

Note

- The filenames of the new files will have "b" appended to the build number (for example, ise-3.1.0.518b.SPA.x86_64.iso).
- If you want to import the SNS 3695 OVA template to the VMware vCenter content library, you can use the ISE-3.x.x.xxx-virtual-SNS3695-1800.ova template. This OVA template is similar to the ISE-3.x.x.xxx-virtual-SNS3695-2400.ova template, except for the reserved disk size, which has been reduced from 2400 GB to 1800 GB to workaround a limitation in the Vmware vCenter content library that prevents import of OVAs with disk size larger than 2 TB.
- You will see the following ISE version in the output of **show tech-support** command:

  `ZTPBUNDLE`

- Existing Cisco ISE 3.1 patches will work fine with this build.

Open Caveats

Open caveats in Cisco ISE release 3.1 cumulative patch 10

Caveat ID Number	Description
CSCwn93753	External RADIUS Server authentication fails with could not find selected access service message.
CSCwn94797	RADIUS token configuration does not work after installing Cisco ISE Release 3.1 Patch 10 in deployment.

Open caveats in Cisco ISE release 3.1 cumulative patch 9

Any unresolved issue from a previous release remains applicable to subsequent releases until it is resolved.

Open caveats in Cisco ISE release 3.1 cumulative patch 8

Caveat ID Number	Description
CSCwf69715	After a patch install on Cisco ISE, TC-NAC adapters will be not reachable and new adapters cannot be configured.
CSCwh92366	In 3.1 Patch 8: Observing Insufficient Virtual Machine Resource Alarm in 3.1Patch 8 Longevity setup.

Open caveats in Cisco ISE release 3.1 cumulative patch 7

Caveat ID Number	Description
CSCwf80292	Cisco ISE cannot retrieve a peer certificate during EAP-TLS authentication.
CSCwf79310	ISE 3.1 patch 7: no VN's under security group in authorization profile.
CSCwh92366	In 3.1 Patch 8: Observing Insufficient Virtual Machine Resource Alarm in 3.1Patch 8 Longevity setup.

Open caveats in Cisco ISE release 3.1 cumulative patch 6

Identifier	Headline
CSCwe72097	31P6:Unable to launch sponor portal with eth1 FQDN(diff dns)- when existing portal is edited.
CSCwe25050	Wild card Certificate imported on PPAN not replicated to other nodes in deployment.
CSCwh92366	In 3.1 Patch 8: Observing Insufficient Virtual Machine Resource Alarm in 3.1Patch 8 Longevity setup.

Open caveats in Cisco ISE release 3.1 cumulative patch 5

The following table lists the open caveats in Cisco ISE release 3.1 cumulative patch 5

Bug ID	Description
CSCwd70346	After a full upgrade to Cisco ISE Release 3.1 patch 5, the precheck page loads with old selected data, and the start button is disabled.
CSCwd97582	Cisco ISE Release 3.1 Patch 5 verifies CA certificate EKU causing Unsupported Certificate error.
CSCwh92366	In 3.1 Patch 8: Observing Insufficient Virtual Machine Resource Alarm in 3.1Patch 8 Longevity setup.

Open caveats in Cisco ISE release 3.1 cumulative patch 4

The following table lists the open caveats in Cisco ISE release 3.1 cumulative patch 4

Bug ID	Description
CSCwc62413	Cisco Identity Services Engine Cross-Site Scripting Vulnerability.
CSCwh92366	In 3.1 Patch 8: Observing Insufficient Virtual Machine Resource Alarm in 3.1Patch 8 Longevity setup.

Open caveats in Cisco ISE release 3.1 cumulative patch 3

Caveat ID Number	Description
CSCwb30989	SXP service is not starting after restart from ISE UI
CSCwb36873	Getting "Page not accessible" pop-up message in ISE-PIC node.
CSCwb09045	ISE PSN nodes crashing due to incorrect cryptoLib initialization.
CSCwh92366	In 3.1 Patch 8: Observing Insufficient Virtual Machine Resource Alarm in 3.1Patch 8 Longevity setup.

Open caveats in Cisco ISE release 3.1 cumulative patch 1

Caveat ID Number	Description
CSCwa09113	Single Byod Flow with Internal CA failing "12557 User Auth failed because OCSP status is unknown".
CSCwh92366	In 3.1 Patch 8: Observing Insufficient Virtual Machine Resource Alarm in 3.1Patch 8 Longevity setup.

Open caveats in Cisco ISE release 3.1

Caveat ID Number	Description
CSCvx43866	Accounting report export is taking more time to complete.
CSCwc83059	Post full upgrade VCS information is missing.
CSCvy14905	Version negotiation fails as new SXP version is unrecognizable in ISE.
CSCvy76622	Android BYOD flow with EST and StaticIP/Hostname/FQDN fails.
CSCvy88861	Policy change doesn’t get pushed to the network device after ISE HA.
CSCvz20020	Okta redirection happens only after the initially added SAML configuration is deleted and reconfigured.
CSCvz20770	Unable to see the pxGrid pages in GUI, after pxGrid is enabled and disabled in Deployment tab on secondary node.
CSCwe99609	Timestamps need adjustment whenever timezone is changed.
CSCwe99666	Live logs and live sessions pages are displayed in incorrect sorting order when timezone is changed on PSN and MnT nodes.

Caveat ID Number	Description
CSCwe99706	Session data is shown at the bottom when PSNs are in different timezones.
CSCwh92366	In 3.1 Patch 8: Observing Insufficient Virtual Machine Resource Alarm in 3.1Patch 8 Longevity setup.
CSCwn62873	Known issue with Cisco ISE integration with Active Directory on Windows server 2025.

Communications, services, and additional information

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

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)

© 2021–2026 Cisco Systems, Inc. All rights reserved.