



Release Notes for Cisco Identity Services Engine, Release 3.4



Contents

- Cisco Identity Services Engine, Release 3.4..... 3
- New software features 3
- Changes in behavior 11
- Resolved issues 11
- Open issues..... 42
- Known issues..... 44
- Compatibility..... 45
- Related resources..... 49
- Legal information 49

Cisco Identity Services Engine, Release 3.4

Cisco ISE release 3.4 brings a host of significant improvements that enhance performance, scalability, and security. This release introduces features like identity sync configurations for Duo connections, allowing administrators to flexibly manage user data synchronization after initial setup. Performance enhancements include automatic log bundle generation during upgrades and improvements to backup log capabilities, which ensure smoother and more efficient troubleshooting processes. Security efficacy is bolstered through the introduction of configurations for Virtual Tunnel Interfaces with Native IPsec, aligning with FIPS 140-3 compliance, and enhanced password security measures that prevent plaintext exposure of sensitive information.

Ease of use and deployment are prioritized through various enhancements such as a new Certificate Authority diagnostic tool, the ability to open TAC support cases directly from the Cisco ISE GUI and improved dynamic access control list behavior for more reliable authorization responses. The release also supports PAC-less RADIUS communication for TrustSec integrations, reducing configuration burdens while maintaining secure communications. GUI enhancements and API improvements, including the addition of hot patch details to the show version command and new session directory topics available using pxGrid, further streamline the user experience and increase operational efficiency. Additionally, the support for multiple Cisco Application Centric Infrastructure connectors broadens the scope for managing access policies across diverse network environments, reinforcing Cisco ISE's role as a pivotal security and management solution.

This document describes the features, issues, and limitations for Cisco Identity Services Engine release 3.4.

Table 1. New and changed information

Date	Description
August 5, 2025	General availability of Cisco ISE release 3.4 cumulative patch 3.
June 20, 2025	General availability of Cisco ISE release 3.4 cumulative patch 2.
December 18, 2024	General availability of Cisco ISE release 3.4 cumulative patch 1.
August 5, 2024	General availability of Cisco ISE release 3.4.

New software features

This section provides a brief description of the new software features introduced in these releases.

Cisco ISE release 3.4 patch 2 new features

Table 2. New features for Cisco ISE release 3.4 cumulative patch 2

Product impact	Feature	Description
Software reliability	Remote support authorization	The remote support authorization allows a Cisco ISE administrator to authorize a specific Cisco TAC specialist to remotely and securely access the Cisco ISE deployment through CLI, UI, or both to troubleshoot and gather information. This access must be explicitly authorized by the Cisco ISE administrator and can be provided for one or more nodes within the Cisco ISE deployment.
	Time restricted	From Cisco ISE release 3.4 patch 2, the time-restricted debug enabling feature

Product impact	Feature	Description
	debug enabling	allows you select a log level from a drop-down list and set a reset timer to revert to default settings. The selected node reverts to the default state once the timer expires.
	Blast RADIUS vulnerability fix	<p>To address the Blast RADIUS vulnerability reported in CSCwk67747, the Message Authenticator Required On Response check box has been introduced in External RADIUS Server, RADIUS Token ID Store, and Device Profile.</p> <p>After an upgrade, the check box is not enabled by default, but it is automatically enabled when new resources are added. Once the checkbox is enabled, Cisco ISE will invalidate any packet that lacks a Message-Authenticator attribute in the response, causing the flow to fail.</p>
	Support for TACACS over TLS	<p>You can enable TACACS over TLS authentication for the network devices to enforce additional security. Cisco ISE supports validating the IP address (iPAddress), DNS name (dNSName), and directory name (directoryname) attributes of the certificate.</p> <p>If any of these attributes match, validation is successful, otherwise, validation fails. For each SAN attribute, multiple values are supported.</p> <p>You can view whether TACACS or TACACS over TLS authentication is enabled for a network device in the Network Devices page.</p>
	API keys and certificate authentication support for Tenable Security Center	<p>From Cisco ISE release 3.4 patch 2 onwards, the following authentication methods are additionally supported for Tenable Security Center:</p> <ul style="list-style-type: none"> • API Keys: Enter the Access key and Secret key of the user account that has access privileges in Tenable Security Center. API keys authentication is supported for Tenable Security Center 5.13.x and later releases. Before choosing this option in Cisco ISE, you must log in as an Admin user and enable API key authentication in Tenable Security Center. • Certificate Authentication: From the Authentication Certificate drop-down list, choose the required certificate. After successful authentication, Cisco ISE will retrieve the customer configured template from Tenable Security Center. Before enabling this option in Cisco ISE, you must configure Tenable Security Center to allow SSL client certificate authentication.
Ease of use	Use enhanced Endpoint Topics Settings to share Cisco ISE data	You can enhance network visibility and security by sharing endpoint attribute data with Cisco AI Endpoint Analytics and Cisco pxGrid Cloud using the enhanced Endpoint Topics Settings feature. You can use the Enable Endpoint Attributes to Topics option to forward endpoint attributes from Cisco ISE to analytic platforms through integration. You can also publish AI Endpoint Analytics profile data to Cisco ISE for network access authorization and endpoint control by using the Consume Endpoint Profiles from AI Endpoint Analytics option.
	Support for osquery condition	<p>From Cisco ISE release 3.4 patch 2, you can create an osquery condition to check the posture compliance status of an endpoint or fetch the required attributes from an endpoint.</p> <p>Note: For osquery condition support, you must use compliance module 4.3.3394 or later and Cisco Secure Client 5.1.7 or later versions.</p>

Cisco ISE release 3.4 patch 1 new features

Table 3. New features for Cisco ISE release 3.4 cumulative patch 1

Product impact	Feature	Description
Ease of use	Preview portal customization	After making the changes in the Portal Page Customization page, you must click Render Preview to preview your content. You must click Refresh Preview every time to view the updated content. Rendering portal customizations with active content or scripts might pose a security risk. We strongly recommend that you review the scripts carefully before rendering.
	Cisco pxGrid Cloud new region support	Cisco pxGrid Cloud is now supported in Europe, Asia Pacific, and Japan in addition to the U.S.
	Integrate Cisco pxGrid Cloud applications using Integration Catalog	From Cisco ISE release 3.4 patch 1, you can use a native integration catalog interface in Cisco ISE to integrate with Cisco pxGrid Cloud applications for a simplified integration experience. Cisco pxGrid Cloud apps can be integrated with Cisco ISE using the Integration Catalog (Administration > System > Deployment > Integration Catalog) . You can integrate both single-instance and multi-instance Cisco pxGrid Cloud apps.
Software reliability	Dynamic reauthorization scheduler	Starting with Cisco ISE release 3.4 patch 1 release, you can enhance access control by setting a predetermined expiration date and time for each session, ensuring sessions remain active only until the specified expiration, thereby preventing unauthorized access.
	Assign dedicated resources for join points	From Cisco ISE release 3.4 patch 1, you can reserve resources for the join points in each PSN. This resource segmentation will help reduce the performance impact caused by resource sharing among the join points.
	Change of Authorization for dictionary attributes using pxGrid Direct	From Cisco ISE release 3.4 patch 1, you can enable Change of Authorization (CoA) for dictionary attributes using pxGrid Direct. When the value of a CoA-enabled dictionary attribute changes, a CoA Port Bounce or Reauthentication is performed on the impacted endpoint.
	Inbound and outbound SGT domain rules	<p>You can create inbound SGT domain rules to map incoming SGT bindings with specific SGT domains. If no rules are defined, bindings received from workload connectors are sent to the default SGT domain.</p> <p>You can create outbound SGT domain rules to designate target destinations for specific SGT bindings.</p>
	SSHD service cryptographic algorithms enhancement	<p>From Cisco ISE release 3.4 patch 1, you can use the new algorithms under service sshd to manage a service using the Cisco ISE CLI. These algorithms are newly added:</p> <ul style="list-style-type: none"> • MAC-algorithm • Hostkey • Hostkey-algorithm • Key-exchange-algorithm • SSH-client-hostkey-algorithm
	Workload classification rules	<p>Workload classification rules can be used to classify the workloads and to assign primary and secondary SGTs to the workloads. The primary SGT is marked as “Security Group” in the pxGrid session topic and is used to publish IP-to-SGT mappings via SXP. Secondary SGTs are included in the pxGrid session topic as an ordered array named “Secondary Security Groups”.</p> <p>You can specify the order of classification rule execution. You can drag and drop the rules to change the order of priority.</p>

Product impact	Feature	Description
	Workload connectors	Common Policy is a framework for building and enforcing consistent access and segmentation policies, regardless of the domain. Workload Connectors are used in this framework to build secure connections with on-premises and cloud data centers, import application workload context, normalize that context into SGTs, and share the context with other domains for building policies.
	Workloads Live Session	The Workloads Live Session page displays the details about the live workload sessions. To view this page, in the Cisco ISE GUI, click the Menu icon and choose Operations > Workloads > Workloads Live Session.
	Security Identifiers in certificates will not be used for authentication	From Cisco ISE release 3.4 patch 1, Cisco ISE supports a new format of certificates with Security Identifiers (SID). The SIDs present in the Subject Alternative Name (SAN) fields will not be used for authentication in Cisco ISE. This enhancement prevents authentication failures caused due to incorrect SID parsing in the authentication process.
	Enable PAP/ASCII in FIPS mode	From Cisco ISE release 3.4 patch 1, Cisco ISE allows configuration of the PAP/ASCII protocol in FIPS mode. You can enable RADIUS DTLS settings when configuring network devices to support the PAP/ASCII protocol in FIPS mode.
	Support ACI for global security group	<p>The naming convention for External EPGs (EEPGs) has changed from Cisco ISE release 3.4 to Cisco ISE release 3.4 patch 1. In Cisco ISE release 3.4, EEPGs are named "ISE_SGT_<SGT_TAG>", with "ISE_SGT_" as a constant prefix followed by the Security Group Tag (SGT). In Cisco ISE Release 3.4 Patch 1, the format changes to "ISE_<SG_NAME>", using "ISE_" as the constant prefix followed by the Security Group (SG) name.</p> <p>This update lacks migration support, so EFT customers must disable outbound rules before installing Cisco ISE release 3.4 patch 1 and re-enable them after completing the patch installation.</p>
API experience	New pxGrid API: Endpoint topic	The Endpoint topic provides access to endpoints connected to a Cisco ISE-managed network device.
Upgrade	Full and split upgrade support for patches	<p>You can upgrade to a new Cisco ISE release with or without a patch for that release. If you have already installed a patch for your Cisco ISE release, you can use the Patch option to upgrade only the patch in your current release.</p> <p>You can choose the full upgrade or split upgrade option for a patch upgrade.</p> <ul style="list-style-type: none"> Full Upgrade: Full upgrade is a multistep process that enables a complete patch upgrade of all the nodes in your Cisco ISE deployment at the same time. Split Upgrade: Split upgrade is a multistep process that enables the patch upgrade of your Cisco ISE deployment while allowing services to remain available during the upgrade process.


Cisco ISE release 3.4 new features

Table 4. New features for Cisco ISE release 3.4

Product impact	Feature	Description
Software reliability	Cisco ISE resiliency use cases	From Cisco ISE release 3.4, the Excessive RADIUS Network Device Communication and Excessive Endpoint Communication alarms have been added to maintain the resiliency of Cisco ISE.

Product impact	Feature	Description
	Configure Virtual Tunnel Interfaces with Native IPsec	From Cisco ISE release 3.4, you can configure Virtual Tunnel Interfaces (VTIs) using the Native IPsec configuration page. You can use this to establish security associations between Cisco ISE PSNs and NADs across an IPsec tunnel using IKEv1 and IKEv2 protocols. Native IPsec configuration ensures that Cisco ISE is FIPS 140-3 compliant.
	Debug log settings	You can configure the maximum file size, and the maximum number of files allowed for each debug log component. You can view the current disk space usage, and the estimated space usage based on the values set for Max File Size and File Count in the Debug Level Configuration page. You can also specify the date and time after which these values must be reset to default.
	Add identity sync after creating a Duo connection	<p>If you do not want to configure user data synchronization between Active Directory and Duo while creating a Duo connection, click Skip in the Identity Sync page. You will be taken to the Summary page directly.</p> <p>After you create a Duo connection, you can add identity sync configurations at any time.</p>
	Support for multiple Cisco Application Centric Infrastructure connectors	<p>Cisco ISE enables you to create and enforce consistent access policies across multiple domains. Cisco ISE can share the SGTs and SGT bindings with Cisco Application Centric Infrastructure (Cisco ACI). Cisco ISE can also learn the endpoint groups (EPGs), endpoint security groups (ESGs), and endpoint information from Cisco ACI. You can add multiple Cisco ACI connections to Cisco ISE.</p> <p>You can configure rules to manage the learned context in Cisco ISE and to optimize the context flows between Cisco ISE and Cisco ACI connectors.</p> <p>Cisco ISE supports Cisco ACI Multi-Tenant, and Multi-Virtual Routing and Forwarding deployments. You can define multi-fabrics through multiple connections. This integration supports multi-pod and individual Cisco ACI fabrics.</p> <p>Support for multiple Cisco Application Infrastructure (Cisco ACI) connectors is a controlled introduction (Beta) feature. We recommend that you thoroughly test this feature in a test environment before using it in a production environment. For best use of this Beta feature, install this hot patch.</p>
	Enforcing domain controller selection with priority	<p>You can now choose to override Cisco ISE's selection of domain controllers in case of a preferred domain controller failover. To do this, choose Administration > Identity Management > External Identity Sources > Active Directory > Advanced Tools > Advanced Tuning. Enter the name of the registry key in the Name field and 1 in the Value field.</p> <p>When the registry key is enabled, you can also choose to set the failback interval (in seconds).</p> <p>This ensures that in the case of a domain controller failover, Cisco ISE overrides the existing priority values and selects the next domain controller in the preferred list in the order of input from left to right. The value of this registry key is set to 0 by default.</p> <p>When registry key is enabled, you can also choose to set the failback interval (in seconds). The failback interval value can be between 60 and 86400. The default failback interval is 180 seconds. This feature works only for direct domains that the domain controllers were configured on, and not for trust relationship domains.</p>

Product impact	Feature	Description
	Enhanced password security	<p>Cisco ISE now improves password security through the following enhancements:</p> <ul style="list-style-type: none"> You can choose to hide the Show button for the following field values, to prevent them from being viewed in plaintext during editing: <p>Under Network Devices,</p> <ul style="list-style-type: none"> RADIUS Shared Secret Radius Second Shared Secret <p>Under Native IPsec,</p> <ul style="list-style-type: none"> Pre-shared Key <p>To do this, choose Administration > Settings > Security Settings and uncheck the Show Password in Plaintext checkbox.</p> <ul style="list-style-type: none"> To prevent the RADIUS Shared Secret and Second Shared Secret from being viewed in plaintext during network device import and export, a new column with the header PasswordEncrypted:Boolean(true false) has been added to the Network Devices Import Template Format. No field value is required for this column. <p>If you are importing network devices from Cisco ISE Release 3.3 patch 1 or earlier releases, you must add a new column with this header to the right of the Authentication:Shared Secret:String(128) column, before import. If you do not add this column, an error message is displayed, and you will not be able to import the file. Network devices with encrypted passwords will be rejected if a valid key to decrypt the password is not provided during import.</p>
	Localized ISE installation	While reinstalling Cisco ISE, you can use the Localized ISE Install option (option 25) in the <code>application configure ise</code> 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.
	pxGrid filtering	From Cisco ISE release 3.4, pxGrid supports filtering of information based on the specific requirements of the clients. The pxGrid filtering feature enables clients to receive relevant information from the publisher on a per-subscription basis. The filtering of information is achieved using the filtering API on the pxGrid server
	RADIUS suppression and reports enhancement	From Cisco ISE release 3.4, the RADIUS suppression and reports feature has been enhanced to facilitate easier RADIUS (Administration > System > Settings > Protocols > RADIUS > RADIUS Settings) configurations.
	PAC-less RADIUS communication for TrustSec integrations	From Cisco ISE release 3.4, Cisco ISE supports PAC-less RADIUS communication for TrustSec integrations. This PAC-less enforcement replaces PAC-based RADIUS authentications wherever supported and is enforced through a shared secret ensuring secure communication between Cisco ISE and the TrustSec device. This feature does not require configuration changes in Cisco ISE. The network devices in the deployment may require a change in configuration. PAC-less RADIUS communication is only supported on network devices with IOS-XE version 17.15.1 or higher.

Product impact	Feature	Description
Ease of setup	Create a URL pusher pxGrid Direct connector	<p>You can now configure Cisco ISE using an IPv6 address, enabling an IPv6-only setup. This enhancement is available in addition to existing IPv4 and dual-stack configuration options. You can easily switch between IPv4 and IPv6 configurations by using the <code>reset-config</code> command. Additionally, the newly introduced <code>ipv6 default-gateway</code> command allows you to specify a default gateway using an IPv6 address.</p> <p>You can create a pxGrid Direct connector using the Cisco ISE GUI and OpenAPI (REST API). From Cisco ISE Release 3.4, you can choose between a URL Fetcher pxGrid Direct connector type or a URL Pusher pxGrid Direct connector type. You can use the URL Pusher pxGrid Direct connector to push JSON data into the Cisco ISE database using pxGrid Direct Push APIs. You can use the URL Pusher pxGrid Direct connector type to push data without a server or a CMDB. This data remains in the Cisco ISE database and can be used in the authorization policy.</p>
	TLS 1.3 support for Cisco ISE workflows	<p>Cisco ISE release 3.4 allows TLS 1.3 to communicate with peers for the following workflows:</p> <ul style="list-style-type: none"> • Cisco ISE is configured as an EAP-TLS server • Cisco ISE is configured as a TEAP server • Cisco ISE is configured as a secure TCP syslog client <p>TLS 1.3 support for Cisco ISE configured as a TEAP server has been tested under internal test conditions because at the time of Cisco ISE release 3.4, TEAP with TLS 1.3 is not supported by any available client OS.</p>
Ease of use	Certificate authority diagnostic tool	To diagnose certificate management related issues, use the CA Diagnostic Tool option in the <code>application configure ise</code> command. This tool suggests the possible reasons and remediations for the identified issues, helps to fix the issues, and provides related logs for troubleshooting.
	Hotpatch details added to show version command	<p>The <code>show version</code> CLI command now includes hotpatch details, if any, for a specific Cisco ISE release.</p> <p>To view hotpatch details on the Cisco ISE GUI, click the  icon and choose About ISE and Server.</p>
	On-demand pxGrid Direct data synchronization using Sync Now	You can use the Sync Now feature to perform on-demand synchronization of data for pxGrid Direct URL Fetcher connectors. You can perform both full and incremental syncs on-demand. On-demand data synchronization can be performed through the Cisco ISE GUI or using OpenAPI.
	Opening TAC support cases in Cisco ISE	From Cisco ISE release 3.4, you can open TAC support cases for Cisco ISE directly from the Cisco ISE GUI.
	Per-user dynamic access control list behavior change	While evaluating authorization profiles with per-user dynamic access control lists (DACLS), if a DACL does not exist in Cisco ISE configuration, authorization will fail, and Cisco ISE will send an Access-Reject response to that user. You can view this information in the Live Log Details page and the AAA Diagnostics report. From Cisco ISE Release 3.4 onwards, an authorization failure alarm is also displayed in the Alarms dashlet in the Cisco ISE dashboard.
	pxGrid Direct support for arrays in dictionary groups for authorization policies	From Cisco ISE release 3.4, you can also use pxGrid Direct Connector data with arrays as dictionary attributes to configure an authorization policy. The operators "Contains" or "Matches" (in case of REGEX) must be used while configuring the policy. The operators "Equals" and "In" will not work when there are arrays. Multiple attributes can be nested using "AND" or "OR" conditions.

Product impact	Feature	Description
	GUI enhancements in Cisco ISE release 3.4	<p>In Cisco ISE release 3.4, the Cisco ISE GUI has the following enhancements to make the user experience more intuitive.</p> <ul style="list-style-type: none"> Single Click Access to Endpoint Information <p>Objects in the Context Visibility page, such as the attribute details of endpoints in the Cisco ISE GUI, now have detailed information available to users with a single click.</p> <p>All endpoint attributes now appear on a single tab for ease-of-use and better visibility.</p> <p>You can click:</p> <ul style="list-style-type: none"> the MAC address of an endpoint to view all endpoint attributes on a single page. the See full detail option on the top right corner of this page to view all endpoint details in a new browser tab, which you can also share. the link icon next to the MAC address of an endpoint to open a full-page view of all endpoint details. <p>The following pages have been updated to include these enhancements:</p> <ul style="list-style-type: none"> Context Visibility > Endpoints. Work Center > Guest Access > Identities > Endpoints. Work Center > BYOD > Identities > Endpoints. Work Center > Network Access > Identities > Endpoints. Work Center > Profiler > Endpoint Classification. <p>Retention of user preferences for column displays: When you change the column display of a table (adjust column width, hide or show columns, reorder columns, and so on) in the Cisco ISE GUI, your preferences are retained.</p>
API experience	New session directory topic available using pxGrid	You can subscribe to the sessionTopicAll topic using pxGrid. The sessionTopicAll is like the existing sessionTopic (which continues to be supported), with one key difference. The sessionTopicAll also publishes events for sessions without IP addresses.
Upgrade	Automatic log bundle generation on upgrade	From Cisco ISE release 3.4, a mini log bundle, which contains only debug logs specific to the upgrade, is generated automatically during the upgrade process. This log bundle is copied to the repository from where the upgrade was started and can be used to troubleshoot the upgrade in case of failure. Automatic log bundle generation is available for all three upgrade options in Cisco ISE – full upgrade, split upgrade, and upgrade using CLI.
	Backup log improvements from the Cisco ISE CLI	The backup-logs CLI command has now been updated to include all backup log options that are available on the Cisco ISE GUI such as core-files, date-from, date-to, db-logs, debug-logs, local-logs, mnt-report-logs, policy-cache-logs, policy-conf-logs, and system-logs. If no output options are included, all backup logs are generated.

New and changed APIs in Cisco ISE

For detailed information on new, changed, and deprecated APIs, see the [Cisco ISE API Reference Guide](#).

Changes in behavior

Cisco ISE release 3.4 deprecated features

Table 5. Deprecate features for Cisco ISE release 3.4

Feature	Description
End of support for Legacy IPsec (ESR)	From Cisco ISE release 3.4, Legacy IPsec (ESR) is not supported on Cisco ISE. All IPsec configurations on Cisco ISE will be Native IPsec configurations. We recommend that you migrate to native IPsec from legacy IPsec (ESR) before upgrading to Cisco ISE release to avoid any loss of tunnel and tunnel configurations.
Configuring RSA or RADIUS external databases for API authentication	From Cisco ISE release 3.4, configuring RSA or RADIUS external databases for API authentication is no longer supported.
Support for Transport Gateway removed	<p>Cisco ISE no longer supports Transport Gateway. The following Cisco ISE features used Transport Gateway as a connection method:</p> <ul style="list-style-type: none">• Cisco ISE Smart Licensing <p>If you use Transport Gateway as the connection method in your smart licensing configuration, you must edit the setting before you upgrade to Cisco ISE release 3.4. You must choose a different connection method as Cisco ISE release 3.4 does not support Transport Gateway. If you upgrade to Cisco ISE release 3.4 without updating the connection method, your smart licensing configuration is automatically updated to use the Direct HTTPS connection method during the upgrade process. You can change the connection method at any time after the upgrade.</p> <ul style="list-style-type: none">• Cisco ISE Telemetry <p>Transport Gateway is no longer available as a connection method when using Cisco ISE Telemetry. The telemetry workflow is not impacted by this change.</p>
GUI deprecations	<p>The following pages have been removed from the Cisco ISE GUI in Cisco ISE Release 3.4:</p> <ul style="list-style-type: none">• Location Services (Administration > Network Resources > Location Services).• NAC Managers (Administration > Network Resources > NAC Managers).

Resolved issues

To see additional information about the issues, click the bug ID to access the Bug Search Tool (BST).

You can use the [Cisco Bug Search Tool](#) to search for a specific bug or to search for all resolved bugs in this release.

Cisco ISE release 3.4 patch 3: Resolved issues

Table 6. Resolved issues in Cisco ISE release 3.4 cumulative patch 3

Bug ID	Description
CSCwp97554	Secure Network Analytics integration with Cisco ISE release 3.4 fails after installing Cisco ISE release patch 1 or patch 2.
CSCwq14019	Cisco ISE release 3.4 patch 2 crashes due to ASN1_get_object.
CSCwp22511	Cisco ISE converts periods to commas, causing a filename mismatch.

Cisco ISE release 3.4 patch 2: Resolved issues

Table 7. Resolved issues in Cisco ISE release 3.4 cumulative patch 2

Bug ID	Description
CSCwo99449	Cisco ISE Unauthenticated Remote Code Execution Vulnerability.
CSCwp02821	Cisco ISE Unauthenticated Remote Code Execution Vulnerability.
CSCvz00208	The wildcard domain list in proxy bypass is not working for CRL retrieval.
CSCwd93959	Alarms and Syslogs should contain detailed information related to the CRL mismatching the CA.
CSCwd96743	Cisco ISE throws a Log Collection error: "warning - Log collection error. Server=xxxx; Log Type=RadiusAuthenticationPassed".
CSCwj04839	Cisco ISE throws an Azure Rest ID Store error: "Lifetime validation failed, the token has expired".
CSCwj38688	Cisco ISE throws a License Expired Error, "Host not found in identity group due to profiler null pointer exception".
CSCwj45793	In Cisco ISE release 3.2, Catalina.out is flooded with application logs when endpoint debugging is running.
CSCwj52266	The endpoint description in Context Visibility is updated with static identity group description.
CSCwk30242	Cisco ISE does not update the NAS during client fast roaming.
CSCwk51948	In Cisco ISE release 3.2, MNT is unable to connect to its own database.
CSCwk63192	The application server is going to initialize state on the MNT node.
CSCwk63893	The UDP syslog DNS name resolution must be performed in a single function call instead of two (IPv6 and IPv4).
CSCwk67747	RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS) - July 2024.
CSCwk80049	Accounting messages do not include StepLatency and StepData attributes.
CSCwk89230	Unable to see IP addresses from access restriction on Cisco ISE.
CSCwm00854	Deferred retries cause the PSN to freeze if PAN updates fail on the PSN.
CSCwm04552	Uploaded CSS files do not reflect changes on portal.
CSCwm05739	A blank screen is observed through CIMC KVM on the SNS-3755 PID after the POST (Power On Self-Test) in the customer unit.

Bug ID	Description
CSCwm10884	LDAP groups on Cisco ISE cannot be saved if the CN contains parentheses.
CSCwm18037	OCSP is unreachable due to HTTP 1.0 usage from Cisco ISE side.
CSCwm26245	Secondary PAN and PSN nodes are unable to upload files larger than 14 GB using local disk management.
CSCwm26817	Duplicate FQDN entry occurs after changing the IP address in reset-config.
CSCwm26992	An IllegalStateException occurs when querying external groups from Azure.
CSCwm32937	Cisco ISE does not respond to specific accounting packets, resulting in an incorrect IP address being updated in the Cisco ISE.
CSCwm33559	GET requests to the Policy API may fail on non-primary PAN.
CSCwm34032	The 'Generate a single certificate (with CSR)' option in pxGrid services with PKCS8 format throws an error.
CSCwm42629	In Cisco ISE release 3.2 patch 4, PSN does not fully handle authentication after reload or patch installation.
CSCwm43211	Cisco ISE reports incorrect latency for RequestLatency and TotalAuthenLatency in RADIUS Accounting.
CSCwm48850	Unable to retrieve endpoint identity groups using ERS starting Cisco ISE release 3.3.
CSCwm51099	Sponsors from different GROUP_ACCOUNTS groups can see all users if they belong to the same OWN_ACCOUNTS group.
CSCwm52140	In Cisco ISE release 3.3 patch 2, DACL parse is failing.
CSCwm53340	Due to regression issue (CSCwe82004) PSN node running TACACS+ crashes.
CSCwm58226	TACACS+ accounting details do not work when primary PAN and secondary MNT are on the same node.
CSCwm59423	Cisco Identity Services Engine: Authorization Bypass Vulnerability.
CSCwm59541	Relocate sensitive API gateway data to an encrypted partition.
CSCwm60638	Unable to start or stop an existing TCP dump capture.
CSCwm60820	Scheduled restart does not work as expected when Cisco ISE nodes are in different domains.
CSCwm65550	The endpoint's static identity group gets changed due to duplicate EPIDs and stale RCM EPIDs across nodes.
CSCwm66426	Cisco ISE has become inaccessible from both the GUI and CLI.
CSCwm67082	Cisco ISE release 3.2 and later should not allow hostname, IP address, or domain name updates for ISE nodes in deployments.
CSCwm68670	Import of guest users fail adding username and password columns in Sponsor Portal template.
CSCwm71222	The /opt directory in Cisco ISE is full because alarm files are not being deleted.
CSCwm72853	In ISE-PIC, ISE MFC Profiler service should be disabled.

Bug ID	Description
CSCwm75692	Deregister the SXP node from the deployment when ACI connections are suspended, and then reconnect the ACI connection.
CSCwm80276	Authentication against ROPC identity store fails due to RSA key generation error in the asynchronous flow.
CSCwm84363	Using 'Network Device Profile = ANY' and 'Advanced Attribute' breaks GET all 'authz profile' API call.
CSCwm85239	Unable to delete user identity groups and getting an error: "java.lang.NullPointerException".
CSCwm87014	Unable to delete identity group, profiling policies or conditions due to stale references.
CSCwm87358	Throws an error when a deleted endpoint purge rule is saved.
CSCwm88083	In Cisco ISE release 3.3, smart license registration fails with error "Unable to perform Smart Licensing operation".
CSCwm88516	The option 'The enable password for TACACS+ access will never expire' is not effective.
CSCwm88519	Sending a certificate with incorrect SAN values should bring down the tunnel.
CSCwm90144	Restore fails at 60% on Cisco ISE release 3.3 with error "DB restore failed and reverted back to pre-restore state".
CSCwm91602	Modifying the TACACS+ shared secret in limited admin groups alters 'VPN Servers' attribute.
CSCwm97553	CLI commands are missing after upgrading to Cisco ISE release 3.2.
CSCwm99047	The agentless posture troubleshooting tool fails with the error: "RequiredFieldNotExist".
CSCwm99057	Agentless posture remains stuck in a pending state due to an unsupported OS.
CSCwn03702	SAML Multi-Application support issue.
CSCwn07375	The '\ ' character is being interpreted as an escape sequence during admin login.
CSCwn07856	Vulnerabilities identified in RabbitMQ version 3.6.5.
CSCwn09009	Local and Global exception policies exhibit unexpected behavior when the 'Default' policy is configured.
CSCwn09816	RADIUS shared secret masking after switch reload causes authentication failures.
CSCwn11566	Admin access IP address restrictions are enforced only on the login page.
CSCwn11732	The Cisco ISE GUI login page keeps loading, and URL gets changed to '/admin/login.jsp?mid=auth_failed'.
CSCwn12582	The script condition is not displayed on the requirement page.
CSCwn12955	Importing SGTs overwrites the name instead of failing for SGTs created by ACI.
CSCwn13021	A filter the uses 'contains' takes too long to save with scaled data.
CSCwn14897	CDP and CSDAC, partial search for IPv6 addresses has issues on the SGT binding page.
CSCwn15744	Serviceability Improvement: Audit log the Jedis connection failure.

Bug ID	Description
CSCwn17160	Clarify EAP-TLS (TLS1.2) authentication failures due to elliptic curve not being in the supported groups.
CSCwn17599	SFTP server validation fails with Cisco ISE.
CSCwn19571	A 'Transaction Exception' error occurs when attempting to save the SAML configuration with the DUO xml file.
CSCwn21814	In CDP, IPv6 prefix is not removed after purging the endpoint in the outbound filter.
CSCwn22572	Cisco ISE gets stuck at saving changes when duplicating and editing a CPP portal.
CSCwn24592	Scrolling issue under the SAML group.
CSCwn27059	Exporting filtered NADs causes infinite loading on Cisco ISE release 3.2.
CSCwn27953	In the Italian sponsor portal, the calendar should not display 'Dom, Lun, Mar, Mer, MAR, Ven, DOM'.
CSCwn30743	Custom endpoint attribute format error in Cisco ISE release 3.2 patch 6.
CSCwn31859	When the SID SAN URI is present as the first SAN value in the certificate, it causes authentication to fail.
CSCwn38427	Cisco ISE admin portal request is not processed due to bad input when accessed through Cloudflare.
CSCwn43818	Mismatch between the username and CallingStationID when calling the ODBC stored procedure for attributes retrieval.
CSCwn44838	In Egress (SGACL) Policy, the command 'show cts role-based policy' is incorrect.
CSCwn45653	In CDP and CSDAC, the filter for the 'Secondary Security Group' field does not work in SGT Binding page.
CSCwn46575	A lower interface MTU than 1280 is required.
CSCwn46625	The config drift alarm message does not appear on the dashboard for the bulk deletion of EEPGs in destination ACI.
CSCwn48457	Posture feed updates fail when FIPS is enabled with a proxy.
CSCwn50156	The default classification rule does not get created in the PSN's database.
CSCwn50257	MDM server-related attributes are missing in pxGrid session published data.
CSCwn50479	In Cisco ISE release 3.2 patch 7, unable to limit sponsor view (SAML Sponsor).
CSCwn51058	Cisco ISE release 3.3 RabbitMQ logs are not rotating, causing high disk space utilization.
CSCwn52227	MDM VPN endpoint reauthentication flows are not matching the authorization policy due to null value.
CSCwn52291	The integrity check file should be included in the support bundle.
CSCwn54074	After rolling back of patch 1 in Cisco 3.4 release patch 1 upgraded setup, the legacy patch page does not load.
CSCwn54212	Unable to remove the identity-store CLI configuration due to case-sensitive mismatches.
CSCwn54381	A retired shared secret for TACACS+ is overwritten when changing the network device configuration.

Bug ID	Description
CSCwn54494	CRL information download through proxy is failing.
CSCwn54934	Faulty behavior with non-existent per-user DACL in the VPN and posture flow.
CSCwn56909	Cisco ISE needs to send FQND in the SMTP EHLO message instead of hostname.
CSCwn57286	In Cisco ISE release 3.3, 'Security Settings' incorrectly displays TLS warning when user modifies other settings.
CSCwn58095	In Cisco ISE release 3.4, error while accessing CV page All shards failed.
CSCwn60000	In Cisco ISE release 3.4, Group Retrieval fails in secure LDAP due to the offered cipher suit in the 'Client-Hello'.
CSCwn61400	ERS PATCH and PUT do not update previousSharedSecretExpiry and previousSharedSecret.
CSCwn62873	Issue with Cisco ISE integration with Active Directory on Windows Server 2025.
CSCwn63678	Radius Accounting reports 'No data found'.
CSCwn65111	UT failures in AcsSyslogContentRadiusAuthenticationTest, and SystemMonitoringConfigManagerTest.
CSCwn66616	Predefined alarms with restricted special characters cannot be edited.
CSCwn76571	Increase the timeout for scripts in posture conditions.
CSCwn77322	Context Visibility obscures device information and MFC details.
CSCwn81215	Unable to profile devices using LLDP during onboarding as ISE does not process the LLDP attributes.
CSCwn82191	The password policy with dictionary words is not functioning as expected on Cisco ISE release 3.3.
CSCwn83477	Some Cisco ISE admin web UI pages throw a 401 error when logging using AD.
CSCwn84705	Importing guest users with a CSV template fails in Firefox.
CSCwn87602	Cisco ISE ERS POST requests to create an internal user using passwordIDStore fails intermittently.
CSCwn88214	Unable to update the 'Use Customization From' field in guest type configuration in Cisco ISE.
CSCwn89029	After SNMP server user is created, any further modifications do not take effect.
CSCwn90693	Cisco ISE release 3.2 patch 7, guest type is not replicated when sponsor group is added.
CSCwn90896	The network access user's password is set to internal if the user is removed from the administrator list.
CSCwn92228	In Cisco ISE release 3.4 patch 1, custom attributes are missing in the detail view of Context Visibility.
CSCwn93673	Disable DockerMetrics monitoring and logging.
CSCwn95732	Condition Studio missing the attribute filter, and the window size is incorrect.
CSCwn95769	Services fail to start in Cisco ISE Release 3.4 with 16 vCPUs and 64 GB of RAM after installing Cisco ISE Release 3.4 Patch 1.

Bug ID	Description
CSCwn95991	Display a warning message when configuring local log settings retention period in Cisco ISE GUI.
CSCwn96558	Authentication latency is observed while searching for MDM.OSVersion.
CSCwn96913	The incremental scheduler does not run and returns a 401 unauthorized error.
CSCwn97014	The scanDirectory method causes memory leak when large amount of Cisco ISE localStore logs are present.
CSCwn97311	In Cisco ISE release 3.3, external identity source through REST ID Store is stuck in loading state.
CSCwn97429	Copying to or from Azure SFTP fails due to a timeout.
CSCwo01012	Duplicating a sponsor group causes CRUD issues with guest types.
CSCwo03350	The 'Deny Access' in any authentication rule removes all access to authentication policy.
CSCwo05334	A valid OID shows 'No Such Object Available'.
CSCwo05386	Cisco ISE is generating alarms regarding the expiration of the internal certificate 'Baltimore CyberTrust Root'.
CSCwo07289	Syslogs handle the secret shared keys of network devices in plain text when using import feature.
CSCwo08869	The username suffix on the REST ID store page does not accept special characters.
CSCwo09728	Syslogs handle the shared secret keys of network devices in plain text when using API patch or put.
CSCwo10401	The CoA evaluation flow attempts to retrieve the ContextWrapper object, which is still acquired by posture flow.
CSCwo10602	IPv6 CoA (Proxy) through Live Session UI is failing.
CSCwo11599	The pxGrid Direct connector test connection failing due to an invalid URL.
CSCwo11703	Log rotation for ctr.log file running in Podman containers.
CSCwo12471	In Serviceability, authentication and authorization policies are not visible under the policy set.
CSCwo14210	The purgeProfiler log is filling up the ISE disk space.
CSCwo19583	High load caused by live log counter queries.
CSCwo25131	The suppression mechanism generates numerous instances of message code 5435 on Cisco ISE release 3.4.
CSCwo27144	The simultaneous logins configuration is not honored in Cisco ISE release 3.3 patch 4.
CSCwo32843	Duplicate custom field values are allowed in guest settings.
CSCwo34645	System 360 monitoring shows disk latency numbers that are too high.
CSCwo47456	Remove the masked password from pxGrid-connector log.
CSCwo53162	Permit_IP_Log and/or Deny_IP_Log with empty aclcontent.
CSCwo55160	Cisco ISE posture CP resources do not show up.

Bug ID	Description
CSCwo56178	In Cisco ISE release 3.5, Reset to Default option does not reset the max file size and count levels on secondary nodes in a deployment.
CSCwo57614	Cisco ISE ERS API requires the changePassord parameter for internal users in an external ID store.
CSCwo59299	Cisco ISE RADIUS DTLS fails to accept an ECDHE client certificate with the KU KeyAgreement for ECDHE-ECDSA.
CSCwo69641	The posture lease timer is not updated in Redis and PAN Oracle database.
CSCwo73164	In dark theme mode on UI, some words in the debug log wizard are not clearly visible.
CSCwo85071	Greenfield functionality does not work if the latest OS is not present in osgroup.xml.
CSCwo85071	Greenfield functionality does not work if the latest OS is not included in the osgroup.xml file.
CSCwo90988	The Radkit service, reachable exclusively over HTTPS, is failing the proxy check.
CSCwo97750	Network Device page: Export all (filtered NADs). The password in the exported file is not encrypted.
CSCwo97767	Navigating to any other page from the security settings page displays the Dirty Page dialog box.
CSCwp01022	The Guest, Sponsor, Certificate, and Posture portals do not load after upgrading to Cisco ISE Release 3.3 patch 5.

Cisco ISE release 3.4 patch 1: Resolved issues

Table 8. Resolved issues in Cisco ISE release 3.4 cumulative patch 1

Bug ID	Description
CSCvy74903	IP address 169.254.4.3 seen when using certificate-based authentication for Cisco ISE administration.
CSCvy74903	IP address 169.254.4.3 is seen when using certificate-based authentication for Cisco ISE administration.
CSCwd61906	Sysaux tablespace allocation should be done based on the profile of the node.
CSCwe54931	System 360 does not show Cisco ISE nodes with different DNS domain names other than primary Cisco ISE.
CSCwh39213	Unable to replace SSH key for Cisco ISE AWS EC2 instances.
CSCwi01581	SXP binding is stuck on Cisco ISE during re-authentication of endpoint between multiple VNs.
CSCwj29473	Cisco ISE Formula Injection.
CSCwj35581	Cisco ISE misses rate limiting protection.
CSCwj35698	Cisco ISE Business Logic Issue - User Dictionaries.
CSCwj44649	In Cisco ISE release 3.3, TACACS data is not retained and everything gets purged.

Bug ID	Description
CSCwj52266	Endpoint description in context visibility is updated with static identity group description.
CSCwj57668	Post upgrade MFC profiler dashboard shows no data.
CSCwj57697	There is a data mismatch when opening live logs or live session details in Cisco ISE.
CSCwj77501	ODBC advanced attributes do not work if two or more inbound attributes are selected.
CSCwj77930	pxGrid JMESPath filter bulk download client timeout.
CSCwj82240	In Cisco ISE release 3.2, Cisco ISE counters reports are empty for secondary nodes.
CSCwj97724	Cisco ISE should not allow updating the existing library conditions with conditions that are not allowed in the policy set.
CSCwk07454	In Cisco ISE release 3.2 Patch 6, PSN does not update the database with the correct posture lease expiry time.
CSCwk15719	Cisco ISE profiler is unable to read the MAC from the LLDP port ID subtype 7 received through SNMP probe response.
CSCwk21895	Cisco ISE says CLI maximum password size is 127.
CSCwk24032	Not all Cisco ISE SRV records have IP due to UDP size limit (length = 548).
CSCwk25206	Empty GPG files are exported if there is no data to purge.
CSCwk25839	Getting higher counts external active directory logs on syslog server.
CSCwk29799	The list of installed patches does not show under patch management page due to an admin certificate issue.
CSCwk31930	Cisco ISE skips authentication against the child domain controller when the AD Forest is marked offline.
CSCwk32078	Endpoint check results remain unreachable after passive ID login event.
CSCwk33023	Update pi-profiler Prometheus configuration without app server restart.
CSCwk33597	TACACS authorization details do not work when SMNT is on the same node as primary PAN.
CSCwk34825	Cisco ISE internal user lock or suspend on incorrect attempts counter does not work as expected.
CSCwk35573	The vulnerable JS Library issue was found while executing ZAP in Cisco ISE release 3.3.
CSCwk36095	The pxGrid live log serviceability.
CSCwk38205	SGTs are not deleted when an ACI connection is deleted.
CSCwk38245	In Cisco ISE release 3.2, Cisco ISE_Internal_Operations_Diagnostics triggers FATAL logging message stating system has reached low disk space limit due to local store directory size issue.
CSCwk38327	Health check fails for MDM flow.

Bug ID	Description
CSCwk40233	Posture state synchronization feature use cases and validation steps need to be documented.
CSCwk40725	ConfD generates endless localhost:9888.access.1.1.1.1... and so on.
CSCwk45006	Device admin license does not allow Cisco ISE admin user to reset first login password.
CSCwk45395	When a previous mandatory policy fails, the audit policy fails and shows skipped conditions.
CSCwk46855	Users pending account is not displayed in the Sponsor Manage Account page.
CSCwk47423	Cisco ISE Reflected Cross-Site Scripting Vulnerability.
CSCwk47454	Cisco ISE Reflected Cross-Site Scripting Vulnerability.
CSCwk47465	Cisco ISE XML External Entity Injection Vulnerability.
CSCwk47475	Cisco ISE Arbitrary File Read and Delete Vulnerability.
CSCwk47489	Cisco ISE Arbitrary File Read and Delete Vulnerability.
CSCwk53171	Cisco ISE /ers/config/endpoint/getrejectedendpoints does not have pagination and returns only 100 endpoints.
CSCwk55333	The ise.psc.log does not print the incoming API request's URI in DEBUG mode.
CSCwk56154	RBAC admin user able to add users without static assignment group.
CSCwk57231	Blanket bug to add multi-ACI report for CDP.
CSCwk59176	The graph is not shown when you click on Cisco ISE report in launchpad from prime infrastructure.
CSCwk59325	Cisco ISE services are getting initialized due to dangling LOCK_FILE.
CSCwk59449	Cisco ISE redirection bypass may lead to XSS.
CSCwk61938	Cisco ISE Evaluate OpenSSH CVE-2024-6387 "regreSSHion" .
CSCwk63923	DNS cache timeout is not honored.
CSCwk64227	The ODBC query in authorization policy does not return result with Postgres.
CSCwk66013	Change in local log settings does not trigger old files deletion.
CSCwk67197	Cisco ISE does not connect with external RADUIS server when proxy-state attribute is missing.
CSCwk69424	ODBC advanced setting sent in procedure call should be logged.
CSCwk69537	Cisco ISE release 3.2 API does not validate if a join point is being used when deleting it over the ERS API.
CSCwk70500	From Cisco ISE release 3.2 and later, bond interfaces need MTU as configured on primary interfaces.

Bug ID	Description
CSCCwk71111	Backup restoration is stuck at 75 percent.
CSCCwk73305	Blanket bug to commit Cisco ISE XDR integration changes.
CSCCwk73315	Cisco ISE 360 Monitoring dashboard displays average CPU time percentage instead of summing the rate.
CSCCwk74068	SXP bulk download missing entries after SXP node reload.
CSCCwk74103	Cisco ISE EAP-FAST PAC-less session timeout, value does not get saved.
CSCCwk75761	High CPU on admin node post accessing " Endpoint identity Groups" page on Cisco ISE.
CSCCwk75775	The health check fails on input or output bandwidth performance check and returns a NULL result.
CSCCwk76790	When you try to edit or add a description for network access users, the description field closes.
CSCCwk79595	Page-level help for inbound and outbound SGT Domain Rules page does not work.
CSCCwk80338	In CDP, multiple SGT IP bindings are missing from Cisco ACI to Cisco ISE; Cisco ACI has mdpEps.
CSCCwk80923	Cisco ISE CLI or SSH users do not follow password policy.
CSCCwk87768	Authentication using the name of the profile fails when the default device is used.
CSCCwk88239	MDM significant attributes cause database persistent events during authentication flow.
CSCCwk91347	Allow enabling of PAP when FIPS is enabled for RADIUS DTLS compatibility.
CSCCwk91976	The GUI does not ask for confirmation of the old password for password change.
CSCCwk93711	Cybervision receives DDOS getAssets calls post Cisco ISE integration.
CSCCwk97231	The backup file is not displayed in the GUI.
CSCCwk98467	Data upgrade or restore fails from Cisco ISE release 3.3 to Cisco ISE release 3.4 if REST ID store is configured without a suffix.
CSCCwm00197	Numeric overflow exception encountered during restart of replication client.
CSCCwm00336	Domain name does not update in the system file (etc/hosts) when bond is configured.
CSCCwm00497	Cisco ISE passiveid-agent.log should include information about the user when logon event is shared.
CSCCwm02519	Additional fix to LSD class.
CSCCwm03837	Cisco ISE release 3.2 Patch 6 health check input or output bandwidth fails even when it is within the supported guidelines.
CSCCwm05976	RPC calls made through Active Directory probe for ODBC authentications.
CSCCwm07116	For SMS gateway GET requests, the URL mapping is not visible in the guest.log.

Bug ID	Description
CSCwm10693	Cisco ISE internal users account disable policy feature does not work after one day of inactivity.
CSCwm12300	Unable to change the password policy on Cisco ISE under internal identity user authentication settings.
CSCwm13073	With less than 3000 SGTs, Cisco ISE throws " This Custom View has exceeded the maximum number of SGTs (3000)." error.
CSCwm13930	Agentless posture and endpoint logs are exported as HTM instead of a zip file.
CSCwm29900	Imported endpoints show incorrect endpoint IDs causing data mismatch.
CSCwm30212	The pxGrid direct triggers sync at last restart time instead of scheduled time.
CSCwm31590	FMC integration with Cisco ISE release 3.3 Patch 3 is breaking for Azure sessions.
CSCwm33110	Heap space is fully utilized by RMQ Consumer.
CSCwm34442	Cisco ISE release 3.4 Active Directory diagnostic tool tests are failing.
CSCwm35851	If PAN failover is enabled in deployment page, PAN-HA precheck fails.
CSCwm36039	Cisco ISE release 3.4 GuestAPI query fails with an admin account who has sponsor privileges.
CSCwm36268	In Cisco ISE release 3.3 Patch 2, Endpoint incorrectly shows as a " Rejected Endpoint" after it is released.
CSCwm37824	Proposed profiled rule download button throws 400 error.
CSCwm38826	Cisco ISE release 3.4 incorrectly marks RADIUS packets as duplicates.
CSCwm40047	Getting misleading error prompts " Unable to send email" .
CSCwm43231	Custom portal files previews do not load properly.
CSCwm44513	PIV/CAC authentication for Cisco ISE admin access causes System 360 permission issues.
CSCwm46079	SXP mappings is not learned for VPN users private IP.
CSCwm47768	Cisco ISE portals show Ukrainian when browser language is Russian.
CSCwm48867	The swapon or swapoff cron should be removed as it causes high load every 6 hours.
CSCwm50409	Slow ERS API endpoint call.
CSCwm53456	In Cisco ISE release 3.3 Patch 2, errors occur when certificate details are retrieved.
CSCwm53627	Optimize the indexing for 'EDF_MDM_GUID' lookups for 'EDF_MDM_GUID' to eliminate full table scans.
CSCwm58017	Cisco ISE release 3.4 port 80 is not in the listening state.

Bug ID	Description
CSCwm58686	Passive session is not published to FMC as Cisco ISE tries to stitch session always.
CSCwm59777	IP domain-name validation is too strict and does not accept valid domains.
CSCwm60583	While enabling or disabling IPv6, multiple empty lines are created in sysctl.conf file.
CSCwm61668	TC-NAC_Tenable throws " Scan Failed: Error in connecting to host: 403 Forbidden" error.
CSCwm63134	In Cisco ISE release 3.2 Patch 6, Cisco ISE does not query MDM intermittently if it receives a 404 response from the MDM server.
CSCwm63628	All rules of source and destination tree under TrustSec policy in Cisco ISE GUI are not visible.
CSCwm65529	Static identity group cannot be changed for endpoints.
CSCwm67805	Due to CoA reauth getting stuck, BYOD devices are on WebAuth pending state even when devices are registered.
CSCwm72206	In Cisco ISE release 3.3 Patch 3, the external identity sources show "no data available" after Cisco ISE release 3.3 Patch 3 installation.
CSCwn07737	In CDP or CSDAC, bindings to SXP devices are no longer sent after workload classification rule changes.
CSCwn18814	In CDP, IPv6 traffic loss to the data center occurs after a PSN reload or an SXP move.
CSCwn21297	The installation time extension impacts the CI.
CSCwn21374	In Cisco ISE release 3.3, a delay occurs when logging into the PAN while it is in not-in-sync mode, as it does not respond on TCP port 443.
CSCwn34778	Despite having MDM attributes, the authentication session does not align with the MDM policy.
CSCwo03350	The 'Deny Access' option in any authentication rule removes all access to the authentication policy.
CSCwo95257	Monitoring issues are encountered when rolling back to Cisco ISE release 3.4 patch 1 from Cisco ISE release 3.4 patch 2.

Cisco ISE release 3.4: Resolved issues

Table 9. Resolved issues in Cisco ISE release 3.4

Bug ID	Description
CSCuz65708	The numbering of DACL entries is off in Mozilla Firefox 45 and above.
CSCvg54133	There are changes to the hostname during printing on the CLI.
CSCvj75157	Cisco ISE API doesn't recognize identity groups while creating user accounts.
CSCvm56115	Cisco ISE allows a policy to be saved even when the corresponding ID store is deleted from another browser tab.

Bug ID	Description
CSCvo60450	Enhancement for encryption to only send AES256 for MS-RPC calls.
CSCvq79397	Cisco ISE GUI pages aren't loading properly with custom administration menu work center permissions.
CSCvs77939	Errors encountered while editing AnyConnect configurations and Posture agent profiles.
CSCvt75833	Cisco ISE should perform a NSLookup again when FQDN is the token server.
CSCvu56500	Exports of all network devices gives an empty file in Cisco ISE.
CSCvw77007	Cisco ISE is constantly requesting internal super admin users in response to external RADIUS token servers.
CSCvw85789	Cisco ISE HSTS header vulnerability on port 8084.
CSCvw90394	Unable to match "identityaccessrestricted equals true" in the authorization policy in Cisco ISE release 2.6 Patch 7.
CSCvw81130	Unable to disable Active Directory Diagnostic Tool scheduled tests in Cisco ISE release 2.7.
CSCvy30859	In Cisco ISE release 2.6, it's impossible to create static IP-SGT mapping for EPGs imported from ACI.
CSCvy34255	Extra pop-up screen appears while viewing the RADIUS and TACACS key after enabling "Require Admin password" to view sensitive data.
CSCvz48764	Allow Launch program remediation to have a set order.
CSCvz62183	The debug profile isn't removed when the "reset to default" option is used in the debug log configuration.
CSCvz86688	Aruba-MPSK-Passphrase needs encryption support.
CSCwa08802	Cisco ISE release 3.1 on AWS gives a false negative on the DNS check under health checks.
CSCwa15336	In Cisco ISE PIC release 3.1, the live session shouldn't show the terminated sessions.
CSCwa32407	Resend the user account details for all guest users or specific guest users to the sponsor.
CSCwa82035	Garbage collector logs, thread dump, and HEAP dump are missing from the support bundle.
CSCwb18744	Security groups and contracts with multiple backslash characters in a row in the description can't sync to Cisco ISE.
CSCwb57672	The GCMP256 authorization with the SHA384withRSA4096 certificate, a requirement in Android 12 for authorization, is failing the authorization process.
CSCwb63834	The MnT log processor service occasionally runs on other Cisco ISE admin nodes.
CSCwb77915	Toggle to enable or disable RSA PSS cipher based on policies under Allowed Protocols.

Bug ID	Description
CSCwc04447	Cisco ISE release 2.7 Patch 6 is unable to filter NAD IP by IP address.
CSCwc26835	RADIUS server sequence configuration is corrupted.
CSCwc36589	Cisco ISE - Intune MDM integration may be disrupted due to the end of support for MAC address-based APIs from Intune.
CSCwc39545	The Docker Metrics Report needs to be changed.
CSCwc53824	Cisco ISE limits connection to AMP - AMQP service to TLSv1.0.
CSCwc64144	The attributes TotalAuthenLatency and ClientLatency don't work for TACACS+ in Cisco ISE.
CSCwc80574	Cisco ISE AD connector fails during a join operation.
CSCwc85211	Cisco ISE Passive ID agent displays error "id to load is required for loading" .
CSCwd14523	The 'accountEnabled' attribute is causing authentication issues for EAP-TLS with Azure AD.
CSCwd20521	Active Directory Connector Process doesn't shut down.
CSCwd21798	Cisco ISE-PIC license expiration alarms.
CSCwd28431	Removal of EPS from Cisco ISE code.
CSCwd34467	In Cisco ISE, the authorization rule evaluation appears to be broken for authorization attempts that use EAP-chaining and Azure AD groups.
CSCwd36753	The AnyConnect posture script isn't attempted when the script condition name contains a period.
CSCwd49321	When Cisco ISE has pxGrid enabled on two nodes, the integration fails with the error " pxGrid not enabled on ISE" .
CSCwd57628	In Cisco ISE release 3.1, the NAD RADIUS shared secret key is incorrect when it starts with ' (apostrophe).
CSCwd67833	This Cisco ISE ERS API is taking several seconds to update a single endpoint.
CSCwe03624	Smart license registration failure with " communication send error" alarms triggered intermittently.
CSCwe07822	Cisco ISE date of last purge has the wrong time stamp.
CSCwe10898	Unable to add an endpoint's MAC address to Endpoint identity Group when using grace access in the Guest portal.
CSCwe12961	Evaluation Period Expired alarm is observed when the SLR license is out of compliance due to overconsumption.
CSCwe12974	The text of the Out of Compliance for 30 days alarm needs to be updated.
CSCwe15945	Guest accounts can't be seen by sponsors in a specific sponsor group.

Bug ID	Description
CSCwe25050	Wild-card certificates imported on primary PAN isn't replicated to other nodes in deployment.
CSCwe53550	Cisco ISE and CVE-2023-24998.
CSCwe74135	Guest portal removal failure and integrity constraint in Cisco ISE release 3.1 Patch 5.
CSCwe82004	TCP socket exhaustion.
CSCwe89459	The script provided for creating endpoint group in the Cisco ISE REST API document is incorrect.
CSCwe95624	In Cisco ISE release 3.2, SNMP doesn't work after a node restart.
CSCwe96739	TLS 1.0 or TLS 1.1 is accepted in the admin portal of Cisco ISE release 3.0.
CSCwe99498	Cisco ISE includes a version of libcurl that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE-2023-27536,CVE-2023-27535,CVE-2023-27538.
CSCwf02093	Nodes in Cisco ISE release 3.2 running on Hyper-V are being assigned a DHCP address in addition to the static IP configured during the initial setup.
CSCwf03445	In Cisco ISE release 3.1, there's an intermittent failure in displaying Live Log details and the error "No Data available for this record" is displayed.
CSCwf05178	Running the URT shows cosmetic warnings or errors.
CSCwf07855	Cisco ISE SXP Bindings API call returns 2x response when the call fails.
CSCwf09364	User and Endpoint identity Groups description fields become not editable when using long-form text.
CSCwf09393	In Cisco ISE release 3.1, the services failed to start after restoring a backup from Cisco ISE release 2.7.
CSCwf10516	The authorization policy feature isn't working in Cisco ISE release 3.2.
CSCwf10773	Cisco ISE restarts services directly without a prompt with the error "no ip name-server" displayed.
CSCwf14365	The warning "Configuration Missing" is seen when navigating to the Log Analytics page.
CSCwf16588	Adding the second NTP authentication key removes all authentication keys from the Cisco ISE GUI.
CSCwf17714	Multiple entries of DockerMetric seen in reports in Cisco ISE release 3.3.
CSCwf22527	In the Context Visibility page, the Endpoint Custom Attributes can't be filtered using special characters.
CSCwf22794	Inconsistence on VLAN ID or name with the error "Error: Not a valid ODBC dictionary" .
CSCwf22816	Authorization based on internal user ID group is failing without the RADIUS-token authorization for VPN.

Bug ID	Description
CSCwf23271	The deployment SEC_TRNREP_STATUS isn't getting updated from the "In Progress" state.
CSCwf23981	Cisco ISE authorization profile displays the wrong security group and VN value.
CSCwf25955	Matching authorization profiles with SGT, VN name, and VLAN causes PRRT to crash.
CSCwf26951	Profiler CoA sent with the wrong session ID.
CSCwf27484	Unable to match Azure AD group if the user belongs to more than 99 groups.
CSCwf30570	Agentless posture script is not running if the computer isn't connected to an AC power source.
CSCwf31073	Cisco ISE displays 400 errors when fetching the device administration network conditions using OpenAPI.
CSCwf31477	Profiler is triggering Port Bounce when there are multiple sessions exist on a switch port
CSCwf32255	Cisco ISE release 3.2 Patch 2 provides no response from SNMP when the "snmp-server host" is configured.
CSCwf32641	Cisco ISE release 3.3: The automatically generated SNMPv3 engine ID is identical on all the nodes. The ID displayed is AKHGCM5MKGF.
CSCwf34391	When the PassiveID syslog is received by the MnT before the Active Authentication syslog, session integration isn't happening in Cisco ISE.
CSCwf34596	The user custom attributes are stuck in the rendering stage.
CSCwf35760	The ct_engine root is using 100% of the CPU.
CSCwf36285	The row of "Manage SXP Domain filters" only displays a maximum of 25 filters.
CSCwf36985	AD group retrieval fails while evaluating authorization policies.
CSCwf37679	Sponsor permissions are disabled on the sponsor portal when they are accessed from the primary PAN.
CSCwf38083	Cisco ISE services are stuck in the initializing state with secure syslogs.
CSCwf39620	Windows Agentless Posture isn't working if the username starts with \$ (dollar sign).
CSCwf40128	Accept client certificate without KU purpose validation as per CiscoSSL rules.
CSCwf40265	Cisco ISE maximum session counter time limit isn't working.
CSCwf40861	The Cisco ISE GUI is showing the HTML Hexadecimal code for the characters in the command set.
CSCwf42496	An attempt to delete an "Is IPSEC Device" NDG causes all subsequent RADIUS and TACACS+ authentications to fail.
CSCwf44736	Cisco identity Services Engine Cross-Site Request Forgery Vulnerability.

Bug ID	Description
CSCwf44906	After restoring a configuration backup, you must reconfigure the repository with new credentials.
CSCwf44942	Cisco ISE PSN crashes when maximum number of users are a part of the user session authentication flow using TACACS.
CSCwf47838	Any space characters in the command arguments are being replaced by forward slash "/" characters after the command set is exported as a CSV file.
CSCwf51766	Cisco ISE can't create an authentication policy with DenyAccess identity source using OpenAPI.
CSCwf54680	Unable to edit or delete authorization profiles which have parentheses in their names.
CSCwf55641	German and Italian emails can't be saved under Account Expiration Notification in Guest Types.
CSCwf55795	With the ADE-OS restore option, the Cisco ISE GUI and CLI aren't accessible in Cisco ISE release 3.2 Patch 1 and later releases.
CSCwf56826	Cores related to jstack can be observed on the primary PAN nodes in a regression setup.
CSCwf59005	PEAP and EAP-TLS don't work on FIPS mode in Cisco ISE release 3.2 Patch 3.
CSCwf59058	RBAC policy with custom permissions is working when the administration menu is hidden.
CSCwf59310	Context Visibility for pxGrid Context-in is missing custom attributes in Cisco ISE release 3.1 Patch 7.
CSCwf59338	Lack of cross-origin HTTP security headers in Cisco ISE.
CSCwf60904	ANC remediation isn't functioning properly with AnyConnect VPN.
CSCwf61657	Gig 0 always participates in the TCP handshake of the sponsor FQDN.
CSCwf61939	Using an apostrophe in the First Name and Last name fields displays an invalid name error.
CSCwf62744	The "Disable EDR Internet Check" tag is a feature enhancement.
CSCwf64662	SXP creates inconsistent mapping between IP address and SGT.
CSCwf66237	Cisco ISE Get All Endpoints request takes a long time to execute since Cisco ISE release 2.7.
CSCwf66781	Bulk Creating Egress Matrix Policy Via ERS Fails With an Error
CSCwf66880	Endpoint .csv file import displays the error "No file chosen" after selecting the file.
CSCwf67438	Some VNs from the Author node aren't synced to the Reader node.
CSCwf71870	Evaluation of TACACS deployment with zero days won't work following smart licensing registration.
CSCwf72037	Administrator login report displays the error "Administrator authentication failed" every five minutes in Cisco ISE release 3.1.

Bug ID	Description
CSCwf72123	In pxGrid Direct, if the user data information is stored in nested objects within the data array, Cisco ISE is unable to use them, and it won't be visible in the pxGrid Direct Connector information in the Context Visibility page.
CSCwf72918	In Cisco ISE release 3.2, the order of the IP name-servers in the running configuration isn't respected.
CSCwf78003	The endpoint details in the pxGrid Endpoints page are incorrect.
CSCwf79582	AD Credentials fail to integrate with Cisco ISE with 2.2.1.x and later releases.
CSCwf80292	Cisco ISE can't retrieve a peer certificate during EAP-TLS authentication.
CSCwf80509	The aging time of Cisco ISE Passive ID is always 1 hour regardless of the configuration.
CSCwf80951	Can't edit or create an admin user due to the error "xwt.widget.repeater.DataRepeater".
CSCwf81550	Cisco ISE is changing the MAC address format according to the selected MAC address format even when it isn't a MAC device.
CSCwf82055	Unable to disable SHA1 for ports associated with Passive ID agents.
CSCwf83193	Unable to log in to the secondary admin node's Cisco ISE GUI using AD credentials.
CSCwf85644	Cisco-av-pair throws an error when using % for PSK.
CSCwf88944	Guest portal FQDN is mapped with the IP address of the node in the database.
CSCwf89224	Decryption of session tickets received from the client fails on Cisco ISE.
CSCwf91508	Cisco ISE GUI packet captures that were taken from CLI can't be deleted.
CSCwf92635	In Cisco ISE release 3.3, the PAN failover component is missing from the debug log configuration.
CSCwf94289	Policy export fails to export the policies in Cisco ISE release 3.0 Patch 6.
CSCwf96294	Connection attempts to domains in the "not allowed domains" list are observed in Cisco ISE release 3.0.
CSCwf97087	Posture feed update error is incorrect when there's a problem with the proxy.
CSCwf98849	A critical error seen in Client Provisioning Portal customization.
CSCwh00049	Cisco identity Services Engine Stored Cross-Site Scripting Vulnerability.
CSCwh01022	IPv6 default route disappears from the routing table after modifying the IPv6 address.
CSCwh01906	The deleted MDM server is still listed in the allowed values under MDMServerName attribute.
CSCwh03227	Cisco ISE doesn't use the license during authorization.

Bug ID	Description
CSCwh03306	Threads get blocked on primary PAN if port 1521 isn't available.
CSCwh03740	CRL retrieval is failing.
CSCwh04251	Cisco ISE agentless posture doesn't support passwords containing ":" character.
CSCwh05599	Cisco ISE Sponsor Portal shows an invalid input when special characters are used in the Guest Type.
CSCwh05647	Static IPV6 routes are removed after a reload in Cisco ISE release 3.2.
CSCwh06081	Deregistering a Cisco ISE node should verify whether the process has been initiated by the primary PAN.
CSCwh06338	The Cisco ISE GUI doesn't load when trying to edit the Client Provisioning Portal configuration.
CSCwh08408	Cisco ISE release 3.3 can't register new nodes to deployment after an upgrade as the node exporter password isn't found.
CSCwh08440	Live log events 5422 and 5434 don't show any data in the Authentication and Authorization columns.
CSCwh10401	In Cisco ISE release 3.1 Patch 5, the pxGrid client certificate can't be generated by using CSR.
CSCwh14249	There's a spelling mistake in API gateway settings in Cisco ISE 3.x releases.
CSCwh16289	Add an option to delete temporary files from "/opt/backup" if the CLI backup process fails during transfer.
CSCwh17285	In Cisco ISE release 3.2 Patch 3 and Cisco ISE release 3.3, the portals don't initialize if "IPV6 is enable" is the only IPV6 command on the interface.
CSCwh17386	Dedicated MnT nodes in Cisco ISE don't replicate SMTP configuration.
CSCwh17448	In Cisco ISE release 3.1, the Agentless Posture flows fail when the domain user is configured for endpoint login.
CSCwh18487	Expired guest accounts don't receive SMS when they try to reactivate their accounts.
CSCwh18731	Upgrade to Cisco ISE release 3.2 with LSD disabled before the upgrade workflow is causing a profiler exception.
CSCwh21038	The session information isn't stored in the time session cache during third-party posture flows.
CSCwh23367	In Cisco ISE release 3.2, the subject line of the self-registration email truncates everything after the "=" sign on the Sponsor-Guest portal.
CSCwh23986	The pxGrid getUserGroups API requests return an empty response.
CSCwh24754	An excess number of AD groups being mapped to sponsor groups is causing latency in sponsor login
CSCwh24823	When nonmandatory attributes aren't included in the body of Update PUT requests, their values are reset to empty or the default value.

Bug ID	Description
CSCwh25160	Swap memory usage is high.
CSCwh26698	Addition of a mechanism to fetch user data for pxGrid connectors.
CSCwh28098	In Cisco ISE release 3.2 Patch 3, the CoA Disconnect call is sent instead of the CoA Push call during a Posture Assessment when the RSD is disabled.
CSCwh28528	The TopN device administration reports don't work when incoming TACACS records exceed 40 million records per day.
CSCwh30723	Cisco ISE context visibility doesn't validate static MAC entries if a separator like colon is omitted.
CSCwh30893	Profiling isn't processing the Calling Station ID values that are in the format "XXXXXXXXXXXX" .
CSCwh32290	After performing a reset configuration with the FQDN value, a mismatch occurs between the GUI and the CLI.
CSCwh33160	Cisco ISE isn't sending SNMPv3 disk traps to configure SNMP servers.
CSCwh36544	pxGrid doesn't show topic registration details.
CSCwh36667	Cisco ISE monitoring GUI is stuck at the "Welcome to Grafana" page.
CSCwh38464	Cisco ISE CLI admin user is unable login after not logging in over a two-month period.
CSCwh38484	Manually deleting the static routes cause Cisco ISE to send packets with wrong MAC addresses in Cisco ISE release 3.0 Patch 7.
CSCwh39008	Not able to schedule or edit schedule for a configuration backup.
CSCwh39802	Cisco ISE is sending misleading messages when it's unable to send an email to a guest after sponsor approval.
CSCwh41693	Cisco ISE on AWS doesn't work if Metadata (IMDS) version value "V2 only" selected.
CSCwh41977	Verify the existence of per-user DACL on Cisco ISE configurations in Cisco ISE release 3.2.
CSCwh42009	In Cisco ISE release 3.2 Patch 3, the adapter log information remains constant.
CSCwh42442	CRL download failure seen in Cisco ISE release 3.2 Patch 3.
CSCwh42683	Read-only permissions are provided for Cisco ISE admin access during SAML authentication.
CSCwh44407	The System Certificate Import doesn't work for Cisco ISE nodes in a deployment in Cisco ISE release 3.2.
CSCwh45472	Operational backups from the Cisco ISE GUI fail with the following status: "Backup Failed; copy to repository failed" .
CSCwh46669	After the administration certificate change, Cisco ISE doesn't restart the services if the Bond interface is configured.

Bug ID	Description
CSCwh46877	A COA port-bounce must take place when an ANC policy with PORT_BOUNCE is removed.
CSCwh47299	The Cisco ISE Alarm and Dashboard Summary doesn't load.
CSCwh47601	Unable to create a user with auth-password and priv-password equal to 40 characters in Cisco ISE release 3.2 Patches 2 and 3.
CSCwh48978	Evaluation of Open VM tools CVE-2023-20900.
CSCwh51136	Cisco ISE drops a RADIUS request with the error message "Request from a non-wireless device was dropped".
CSCwh51156	Cisco ISE can't load corrupted NAD profiles causing authorization drops due to failure reasons 11007 and 15022.
CSCwh51548	Hot patches aren't installed when both patches and hot patches are in ZTP configuration.
CSCwh52589	When a guest user connects to Cisco ISE for the first time, Cisco ISE doesn't update the ACS.Username field with the guest username.
CSCwh53159	Unable to change the admin password if it contains "\$" in Cisco ISE release 3.1 Patch 7.
CSCwh55667	Internal system error for posture is seen when premier license is disabled in Cisco ISE.
CSCwh56565	Primary PAN REST calls to MnT nodes for live logs and reports aren't loaded balanced.
CSCwh58768	Unable to delete existing devices in the My Device portal after restoring from Cisco ISE release 2.7.
CSCwh60726	Cisco ISE automatic crash decoder isn't decoding functions properly.
CSCwh61339	Cisco ISE times out when using the Export All option on the Network Devices page to export more than 90,000 network devices.
CSCwh64195	Data corruptions causing FailureReason=11007 or FailureReason=15022 in Cisco ISE.
CSCwh64394	After the Import button is clicked, the .csv file shouldn't be selected, and the Import button shouldn't work.
CSCwh65018	The Cisco ISE release 3.1 Patch 5 install stalls indefinitely.
CSCwh67500	Cisco ISE release 3.2 couldn't find selected authorization profiles.
CSCwh68651	Recreating the undo-tablespace causes URT to fail in Cisco ISE release 3.1 Patch 7.
CSCwh69045	In Cisco ISE release 3.1 Patch 5, the passwords of a few internal users aren't expiring even after the configured global password expiry date.
CSCwh69267	Post ADEOS restore, the app server is stuck at the initializing phase.
CSCwh69466	In Cisco ISE release 3.1, the detailed report doesn't show both user and machine authentication policies for EAP chaining.

Bug ID	Description
CSCwh70275	During the registration of a node that was previously registered to the deployment, it's observed that all the certificates of the deployment were deleted and that all the nodes in the deployment were restarted.
CSCwh70696	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability.
CSCwh71117	Enabling only "User Services" also enables admin GUI access.
CSCwh71157	The mobile number format field for JavaScript code doesn't support more than 100 characters.
CSCwh71273	In Cisco ISE release 3.2, there's limited GUI access and an inability to regenerate root CA when Essentials licenses are disabled.
CSCwh71435	The "Enable Password" of the internal users is created even when it's specified through ERS API.
CSCwh72754	Impact on the authentications that use Active Directory as the identity source.
CSCwh74135	Unable to integrate to prime Infrastructure due to a wrong password error.
CSCwh74236	The detailed Live Log page isn't loading for the TACACS+ authorization flow.
CSCwh77574	Cisco ISE doesn't allow special characters in passwords while importing certificates.
CSCwh79938	You can't set the value of the preferred domain controllers registry during advanced tuning.
CSCwh81035	The Cisco ISE PAN is missing updates of nonsignificant attributes for endpoints from the Cisco ISE PSN.
CSCwh81943	The portal name and results filters aren't working in the Primary Guest report.
CSCwh83323	In Cisco ISE release 3.2, the SMS is not sent during the "Reset Password" flow when using a custom "SMTP API Destination Address".
CSCwh83482	Cisco ISE database doesn't update the email field for Sponsor accounts.
CSCwh84446	If the Account Expiration notification has special characters, you can't save the Guest Type.
CSCwh88801	0.0.0.0 default static routes configured on all interfaces are deleted post Cisco ISE reload.
CSCwh88911	Cisco ISE database only allows 100 characters in the email field for a Sponsor account.
CSCwh89520	Cisco ISE CLI upgrade fails with the error "Internal error during command execution".
CSCwh90610	The abandoned Jedis connections aren't being sent back to the thread pool in Cisco ISE.
CSCwh90691	Show CLI commands throw an exception after configuring log level up to five.
CSCwh92117	The Sysaux tablespace is full due to the growth size of the AUD\$ table.
CSCwh92185	RADIUS Authentication reports exported from the Operational Data Purging page are empty.

Bug ID	Description
CSCwh92366	Observing the Insufficient Virtual Machine Resource alarm in Cisco ISE release 3.1 Patch 8.
CSCwh93498	In Cisco ISE release 3.1, the endpoint purging rule is automatically created after duplicating the My Devices portal in Cisco ISE BYOD configuration causing endpoints to be deleted from the Cisco ISE database after 30 days.
CSCwh93925	Cisco ISE incorrectly routes RADIUS Traffic when multiple static default routes are present.
CSCwh95022	Sponsor portal shows the wrong days of week information in the "Setting date" tab when using the Japanese GUI.
CSCwh95232	Cisco ISE allows duplicate interface IP addresses.
CSCwh95587	NFS repository stops working suddenly on a single node in a distributed deployment in Cisco ISE release 3.2.
CSCwh96018	Failure due to case-sensitive check when new mobile device managers are created with the same name but with a different case.
CSCwh96376	Cisco ISE release 3.3 can't switch the administration certificate role.
CSCwh97876	Cisco Identity Services Engine Arbitrary File Upload Vulnerability.
CSCwh99534	The endpoint probe doesn't clean up SXP mappings.
CSCwh99772	All network device groups are deleted after a child item is removed from any group.
CSCwi03961	Location group information is missing from policy sets.
CSCwi04514	Posture client provisioning resources display an HTTP error when the dictionary attribute contains " - " .
CSCwi05445	Unable to delete a support bundle from the Cisco ISE GUI in Cisco ISE release 3.1 Patch 7.
CSCwi10922	The message description for message code 13036 has a misspelled word.
CSCwi11762	Korean support issue on Context Visibility page.
CSCwi11965	Cisco Identity Services Engine Server-Side Request Forgery Vulnerability.
CSCwi12671	The TCP Dump diagnostic tool doesn't allow for simultaneous multiple interface captures on a node.
CSCwi15793	An error with custom attribute special characters in Cisco ISE.
CSCwi15914	Additional IPV6-SGT session binding created for IPV6 to link local address from SXP ADD operation.
CSCwi17200	When configuring "TROUBLESHOOTING.EncryptionOffPeriod" advanced tuning with any nonzero value of minutes for decrypting the communication with Active Directory for troubleshooting, then RPC net logon fails for all Active Directory authentications on that Cisco ISE node.
CSCwi17694	If the configured synflood-limit is beyond 10000, the limit isn't working.

Bug ID	Description
CSCwi18005	The external RADIUS server list doesn't show up after upgrading to Cisco ISE release 3.2.
CSCwi18917	Cisco ISE SNMP polling doesn't work with privacy protocol AES 192 or AES 256.
CSCwi19460	Unsupported message codes 91092 and 91103, and respective alarms seen in syslogs.
CSCwi20027	The TrustSec deployment request fails as the CoA request gets stuck while fetching NAD information.
CSCwi21020	Cisco ISE messaging certificate generation doesn't replicate the full certificate chain on secondary nodes.
CSCwi23166	Unable to save changes in the patch management condition.
CSCwi25755	SAML Provider can't be added in Cisco ISE release 3.2 and later releases.
CSCwi26921	The DumpClearOnExceed files can be seen by using the "dir" command in the Cisco ISE CLI.
CSCwi27497	Cisco ISE REST authorization service isn't running due to an error in the IP tables.
CSCwi28131	Custom attributes used in the Never Purge rule are still purging the endpoints.
CSCwi29253	Cisco ISE AD Diagnostic Tool stops working upon upgrade and you can't retrieve the list of available tests.
CSCwi29623	Scheduled backup configuration details aren't visible to Read-only user in Cisco ISE release 3.1 Patch 7.
CSCwi30707	In Cisco ISE release 3.1 Patch 7, the removed device types can still be selected in the policy set.
CSCwi32576	PSN node crashed during assignment of CPMSessionID.
CSCwi33361	Problems seen with Cisco ISE CLI access as it fails to connect to the server.
CSCwi34405	Unable to enforce the IdentityAccessRestricted attribute in the authorization policy.
CSCwi36040	IP access list control in Cisco ISE release 3.2 isn't visible.
CSCwi37079	Cisco ISE URT bundle upgrade fails with the error "RADIUS dictionary attribute duplicate entry exists" .
CSCwi38377	Unable to trigger COA and is stuck at the dispatcher queue.
CSCwi38644	The agent rule defaults to the default rule setting while editing an existing agent.
CSCwi38912	The debug elements repeat three or more times in the debug profile configuration in Cisco ISE release 3.3.
CSCwi42412	In Cisco ISE 3.x releases, Interactive Help throws an error in the console and logs.
CSCwi42628	MAR cache replication fails between peer nodes for both NIC and Non-NIC bonding interfaces.

Bug ID	Description
CSCwi43166	TrustSec update with CoA or CoA-push is broken.
CSCwi45090	The filter field 'name' isn't supported for downloadable ACLs through Cisco ISE ERS APIs.
CSCwi45131	Apache Struts Vulnerability affecting Cisco products: December 2023
CSCwi45879	Unable to select hotspot portal if an existent or duplicated authorization profile is selected.
CSCwi46648	The PRA fails if the endpoint is within posture lease.
CSCwi48806	Unable to load the authorization policy due to duplicate portal entries.
CSCwi52041	Changes in rank cause the authorization rule to be committed to the database table which triggers the save call from the G UI
CSCwi52264	Cisco ISE SAML ID provider configuration attributes are deleted even when they are referenced elsewhere.
CSCwi53104	Exporting a report for a period of over one month provides a report with no data.
CSCwi53884	Vulnerabilities in OpenSSL 1.0.2o.
CSCwi53915	The " Save" option under Advanced filters isn't working for filtering Client Provisioning resources.
CSCwi54325	The PRA fails if the endpoint is in a posture lease.
CSCwi54722	Redirect URLs using FQDN that end with the IP address have the IP address replaced by the Cisco ISE hostname.
CSCwi57069	NA PRRT needs to be decoupled from logging using the main thread pool.
CSCwi57761	CVE-2023-48795 seen in OpenSSH in Cisco ISE.
CSCwi57812	Listening noted on port TCP and 67 in Cisco ISE release 3.2.
CSCwi57903	No alarm is generated for a failed scheduled backup.
CSCwi57950	Strict transport security is incorrectly formed in Cisco ISE release 3.2.
CSCwi58421	When the posture lease is enabled, Cisco ISE PSN doesn't update the database with the correct posture expiry time.
CSCwi58699	COA is triggered using a Guest Flow when Cisco Catalyst Center or Endpoint Analytics dictionary attributes are updated on Cisco ISE.
CSCwi59216	The Sponsor Portal displays the error " 400 Bad Request" when you click the Contact Support option on the Cisco ISE GUI.
CSCwi59230	Only superadmin users can edit or delete endpoints when Cisco ISE has more than 1000 identity groups.

Bug ID	Description
CSCwi59312	Cisco ISE authorization profiles don't persist data with "Security Group" and "Reauthentication" common tasks.
CSCwi59555	In Cisco ISE release 3.2 Patch 4, the search for MAC address in the format is ignored.
CSCwi59567	Issues seen when the COA retry count is updated to "0" .
CSCwi59868	Account extension is not properly defined in the Sponsor-based Guest Portal.
CSCwi60778	The endpoint is losing the static identity group assignment after reauthentication.
CSCwi61491	The application server is crashing because of Meta space exhaustion.
CSCwi61700	The "iselocalstore" logs aren't getting collected in the support bundle logs obtained from the Cisco ISE CLI.
CSCwi61950	Cisco ISE is reaching the context limit in proxy flows when querying LDAP groups for authorization policies.
CSCwi63725	The SNMPD process causes memory leaks on Cisco ISE.
CSCwi66105	Custom attribute failure seen in Cisco ISE release 3.1 Patch 7.
CSCwi66126	Updating the DACL doesn't modify the last update timestamp in the Cisco ISE ERS API.
CSCwi66608	In Cisco ISE release 3.2, the RMQ is sending outgoing RST packets with APIPA IP 169.254.2.2.
CSCwi67503	Cisco ISE couldn't find the selected authorization profile if the profile has been created using API.
CSCwi67639	The command "show cpu usage" doesn't display information in Cisco ISE 3.x releases.
CSCwi69659	During the TrustSec deployment verification, the policy difference alarm is triggered while policy the is identical on Cisco ISE and the NAD.
CSCwi72309	Cisco ISE is stuck in a profiling loop, slowing down replication, and causing errors.
CSCwi73981	An identity store that's added using uppercase FQDN can't be removed from the CLI.
CSCwi73984	In Cisco ISE release 3.1Patch 8, the Installed Patches menu doesn't list all the patches.
CSCwi74567	Corruption in the Cisco ISE portal due to inconsistencies in the database.
CSCwi75143	Unable to update the profiling settings as the PriorityType is mandated.
CSCwi78164	Cisco ISE DNS Resolvability Health Check fails due to a duplicated entry (IP, name, and FQDN).
CSCwi79159	Cisco ISE release 3.2 Patch 4 displays a "deleteCertFromStore: Failed to parse certificate" error.
CSCwi86762	Right COA to be triggered in VPM flow when posture and MDM flows are configured together.

Bug ID	Description
CSCwi88583	The <code>erl_crash.dump</code> must be handled in a better way.
CSCwi89082	The Cisco ISE default portal is deleted from the database and is needed for SAML configuration.
CSCwi89466	Cisco ISE AD User <code>SamAccountName</code> parameter is null for user sessions in Cisco ISE release 3.2 Patch 3.
CSCwi89689	Cisco ISE displaying "Invalid IP or hostname" error.
CSCwi89720	Microsoft Azure AD has been officially renamed as Microsoft Entra ID.
CSCwi92655	The Context Visibility pages open drawer action displays an error while loading subtitles in Cisco ISE release 3.3 Patch 1.
CSCwi93050	Endpoint import fails for RBAC when Azure SAML is used for administration access.
CSCwi94938	In Cisco ISE release 3.2, the guest user API gives incorrect results when the filter is used.
CSCwi98793	Profiler is caching the MDM attributes with wrong values.
CSCwj01310	Intensive GC observed due to the SXP component causing node longevity issues in Cisco ISE release 3.4.
CSCwj03747	Profiling isn't suppressing CoA even if the option to suppress CoA for specific logical groups is enabled.
CSCwi04049	When using an LDAP connection to connect to AD, Cisco ISE can't translate the value of AD attribute " <code>msRASSavedFramedIPAddress</code> " or " <code>msRADIUSFramedIPAddress</code> ".
CSCwj05508	The error "Name or service not known" is displayed when you try to reach the configured IP host under certain procedures.
CSCwj05881	Authentication fails and the advanced options are ignored in Cisco ISE.
CSCwj06269	No report or alarm is triggered for changes in the Device Administration settings.
CSCwj06401	Endpoints having a null key value pair in the attributes section are interrupting the purge flow.
CSCwj07319	The API <code>ers/config/session servicenode</code> is returning the incorrect total.
CSCwj07675	Cisco ISE release 3.2 sends outgoing RST packets with APIPA IP 169.254.4.x.
CSCwj07717	Cisco ISE audit reports log APIPA addresses as the source of the API requests.
CSCwj09890	When upgrading to Cisco ISE release 3.4, the Duo seeder is missing in the MnT table post the upgrade.
CSCwj12359	Interrupting execution of " <code>show tech-support</code> " causes services to stop on Cisco ISE.
CSCwj12489	Unable to delete Network Device Group.

Bug ID	Description
CSCwj14217	The Device Network Conditions GUI page doesn't load.
CSCwj14231	Cisco ISE release 3.2 custom filters for TACACS reports don't work as expected.
CSCwj21203	1000 database connections are exhausted due to the "Dashboard System Status" query.
CSCwj21403	REST authorization services won't be enabled when hosts have multiple entries.
CSCwj23933	The AD connector in not joined status update.
CSCwj25817	Initial setup fails if the default gateway and configured IP address are on different subnets.
CSCwj27469	Cisco ISE release 3.3 on Cloud (Azure, AWS, OCI) isn't reading disk size properly and always defaults to 300 GB.
CSCwj31619	In Cisco ISE release 3.2 and later releases, conditions from Condition Studio have a default disabled icon in the information pop-up.
CSCwj32716	MDM configuration fails when the GUID in the client certificate is used to validate the compliance of the device.
CSCwj33906	IP or SXP mappings aren't created for VPN clients.
CSCwj35576	Validation is missing on the Cisco ISE server.
CSCwj35581	Cisco ISE Missing Rate Limiting Protection.
CSCwj35602	The requirement to enter the current password during a password update can be bypassed in Cisco ISE.
CSCwj36716	Cisco ISE Self-Persistent Cross-Site Scripting (XSS) is seen in My Reports.
CSCwj39533	High CPU usage caused by RMQforwarder.
CSCwj40026	Backups triggered rom the Cisco ISE GUI have errors saying that backups were triggered from the CLI.
CSCwj42214	Syslogs for Cisco ISE MnT purge events are incorrectly formatted.
CSCwj43362	An upgrade to Cisco ISE release 3.2 fails with the error - integrity constraint (CEPM.REF_HOSTCONFIG_HA_PEER1) violated.
CSCwj43480	Cisco ISE release 3.3 doesn't invoke MFA for the user with UPN (User Principle Name).
CSCwj43912	The application remediation disappears after editing.
CSCwj44649	In Cisco ISE release 3.3, TACACS data isn't retained and is purged.
CSCwj47769	Cisco ISE can't download Passive ID agent.
CSCwj48359	The pxGrid Databases Synchronization Test on Cisco ISE displays the error " Out of Sync" .

Bug ID	Description
CSCwj48625	Agentless posture fails for EAP-TLS flows with multiple domains configured for endpoints to log in.
CSCwj48827	Unable to add multiple tasks within quotes “ in the launch program remediation.
CSCwj51329	MDM compliance check fails when there are multiple MAC addresses with VMware Workspace One as the mobile device management server.
CSCwj52266	Endpoint description in the Context Visibility page is updated with the Static Identity Group description.
CSCwj58727	Cisco ISE shouldn't allow a user to save the Allowed Protocols when no protocols have been checked.
CSCwj59848	The Log Analytics page isn't launching in Cisco ISE.
CSCwj60125	The User Account search and Manage Accounts functionality has been enhanced.
CSCwj60692	TLS is restricted to using only a few ciphers in Cisco ISE release 3.3, but the ports 8905, 9094, and 9095 use all TLS ciphers.
CSCwj66951	The first name and last name fields in Network Access User don't allow for " 'OR" in the names.
CSCwj67980	Primary Guest Report shows duplicate entries of title when exported to an external repository.
CSCwj68795	Replication error " Error synchronizing object: EDF2EndPoint: Operation: Update" is displayed during replication in Cisco ISE.
CSCwj72117	Operational data purging only shows the name of the primary monitoring node.
CSCwj72680	HS_err files are being generated on the MnT nodes.
CSCwj74175	Compress restprobe-OOMHeap dumps.
CSCwj76445	Cisco ISE ERS Guest documentation should be updated to exclude the Portal ID from GET calls.
CSCwj77067	Provide a comprehensible description for the error displays while editing internal users.
CSCwj80589	An error is displayed while launching the Log Analytics page.
CSCwj80616	Endpoint details in the Cisco ISE Context Visibility page don't match with the RADIUS live logs or sessions during the MDM flow.
CSCwj80950	Cisco ISE isn't sharing posture-compliant sessions properly over pxGrid.
CSCwj81776	Unable to use the advanced filter in Cisco ISE release 3.2 for " Empty" and " Not Empty" filters.
CSCwj82278	Stale lock files are blocking the API gateway and the Context Visibility page.
CSCwj82298	Assigned logical profile is repeated in the endpoint attributes and reports on the Context Visibility page.

Bug ID	Description
CSCWj83459	Unable to create a new internal user and the error " couldn't execute statement; SQL [n/a]; constraint [CEPM.BKUPSLASTAUTHTIMEENTRY]" is displayed on the Cisco ISE GUI.
CSCWj83460	Discrepancy in the count of identity groups between the CV and Oracle databases.
CSCWj84815	The error " No session available" is displayed in Cisco ISE release 3.3 Patch 2.
CSCWj85626	Unable to retrieve the endpoint IP address using API calls.
CSCWj89479	When joining multiple Cisco ISE nodes to the domain controller simultaneously duplicate accounts are created.
CSCWj91517	You need to disable the unbound anchor while starting Cisco ISE.
CSCWj95818	Maximum concurrent CLI sessions don't work in Cisco ISE release 3.4.
CSCWj97449	The Cisco ISE admin isn't alerted about incorrect engineID format in snmp-server host during SNMPv3 configuration.
CSCwk00439	pxGrid Direct service is stuck in the initializing state because the lock file isn't removed.
CSCwk04493	Methods used for retrieving policy details use the internal method and aren't cached in Cisco ISE release 3.1 Patch 6.
CSCwk04644	In Cisco ISE release 3.2 and later releases, System 360 Monitoring debug log rotation isn't working.
CSCwk07230	Duplicating network devices recreate the devices without RADIUS settings in Cisco ISE release 3.3 Patch 2.
CSCwk07324	The main thread pool in Cisco ISE is stuck due to the ACE third-party library ContextIn leak.
CSCwk07483	The Profiler NetworkDeviceEventHandler failed to add a device as a result of the input containing "0-255" in the string.
CSCwk07593	Get-All Guest User API isn't retrieving all the guest accounts.
CSCwk07789	An invalid IP or hostname error is displayed when using "_" as the first character in the NSLookup request.
CSCwk09094	A misleading pop-up seen while setting the password lifetime as more than 365 days.
CSCwk13212	In Cisco ISE release 3.2 and later releases, the System 360 monitoring debug log level needs to be reduced.
CSCwk13234	Old Cisco ISE nodes are shown in the TCP dump and debug profile configuration after a restore operation.
CSCwk13244	The ise-messaging.log not visible for downloading on the Cisco ISE GUI.
CSCwk14636	An issue with the Insufficient Virtual Machine Resources Alarm on AWS is seen in Cisco ISE release 3.2 Patch 6.

Bug ID	Description
CSCwk20019	While using the SMS HTTP method as the SMS gateway the attribute name in the SMS HTTP URL causes problems.
CSCwk25064	Enabling the SXP role on the Cisco ISE PSN causes high CPU load and utilization.
CSCwk30610	In Cisco ISE release 3.2, the TACACS+ end-station network condition has high step latency while accessing the NAD using the console.
CSCwk32104	Both agentprobeoom.sh & restprobeoom.sh need to clean up their own OOM Heap files to optimize Cisco ISE database usage.
CSCwk32677	The ise-duo.log isn't collected at the time of support bundle creation.
CSCwk35172	The DumpClearOnExceed files are using excessive disk space on the Cisco ISE PSN nodes.
CSCwk38279	The ea.log file must be included in the support bundle.
CSCwk61938	Cisco ISE to evaluate OpenSSH CVE-2024-6387.

Open issues

To see additional information about the issues, click the bug ID to access the Bug Search Tool (BST). This section lists the open issues that apply to the current release and might apply to releases earlier than Cisco ISE 3.4. An issue that is open for an earlier release and is still unresolved applies to all future releases until it is resolved.

You can use the [Cisco Bug Search Tool](#) to search for a specific bug or to search for all open bugs in this release.

To search for a documented Cisco product issue, type in the browser: <bug_number> site:cisco.com

Cisco ISE release 3.4 patch 2: Open issues

Table 10. Open issues in Cisco ISE release 3.4 cumulative patch 2

Bug ID	Description
CSCwh77618	Cisco ISE RMQ Full: High latency exists between ISE nodes when EPO is enabled.
CSCwn97980	The cell in the TrustSec policy matrix is intermittently unresponsive.
CSCwo05386	Cisco ISE is receiving alarms about the expiration of the internal certificate 'Baltimore CyberTrust Root'.
CSCwo99311	In Cisco ISE Release 3.4 Patch 2, no endpoints are onboarded in the EPO PSN1 unreachable scenario.
CSCwp22511	New Patch Upload UI converts periods to commas, causing filename mismatches.
CSCwp60343	During certificate-based authentication, ERS post-operation for internal users fails due to client validation failure.

Cisco ISE release 3.4 patch 1: Open issues

Table 11. Open issues in Cisco ISE release 3.4 cumulative patch 1

Bug ID	Description
CSCwk39635	In Cisco ISE release 3.3 Patch 2, multi-factor authentication is not working with MSCHAPv2.
CSCwm40972	When configuring an AWS workload connector, only public and private IPv4 addresses are detected, while IPv6 addresses are not recognized.
CSCwm61368	If you use a workload connector in a workload classification rule as the source attribute with "Contains" operator, you cannot delete the connector.
CSCwm75692	SXP nodes need to be deregistered from deployment and ACI connection should be reconnected when ACI connections are suspended.
CSCwn08908	After rolling back to version Cisco ISE release 3.4 Patch 1, only session data is being published, while SXP data is not.
CSCwn12955	When importing SGTs, the process overwrites existing names instead of failing for those created by ACI.
CSCwn13021	The "Contains" filter takes too long to save when applied to large-scale data.
CSCwn14897	In CDP or CSDAC, partial search for IPv6 address has issues on SGT Bindings page.
CSCwn21814	In CDP, the IPv6 prefix is not getting removed after performing "Purge Endpoint" operation in outbound filter.
CSCwn33420	When the default classification rule is enabled, all other policy rules will add the SGTs from the default policy to their resultant workloads.
CSCwn33420	SGTs from default classification page gets appended to the bindings from other rules.
CSCwn45653	In CDP or CSDAC, Secondary Security Group filter does not work in SGT Bindings page.
CSCwn46625	The configuration drift alarm message is not appearing on the dashboard following the bulk deletion of Endpoint Groups (EPGs) in the destination ACI.
CSCwn47826	In Log Analytics, error comes in Radius Step latency dashboard.
CSCwn50156	Default classification rule is not created on PSN's Database.
CSCwn50666	pxGrid Direct sync now is taking more time than baseline and is also causing memory issues.
CSCwn54074	After rolling back to Cisco ISE release 3.4 Patch 1 in an upgraded setup, the legacy patch page fails to load.
CSCwn54494	CRL information download through proxy fails.

Cisco ISE release 3.4: Open issues

Table 12. Open issues in Cisco ISE release 3.4

Bug ID	Description
CSCwj57668	After upgrade, the MFC Profiler dashboard displays no data.
CSCwk38205	SGTs are not deleted when an ACI connection is deleted.
CSCwk39635	Duo MFA with VPN login does not work with MS-CHAP-v2.
CSCwk67747	RADIUS Protocol Spoofing Vulnerability (Blast RADIUS).
CSCwk74068	SXP bulk download missing entries after SXP node reload.
CSCwk78054	Endpoints are not listed in the Context Visibility page, but they are listed in the Live Logs and Live Sessions pages, when a standalone node is assigned both PPA and PSN personas.
CSCwk79595	Page-level help for Inbound and Outbound SGT Domain Rules page is not working.
CSCwk85207	Authorization fails if DACL is not found in the ISE configuration.
CSCwk98200	<p>The following error is received under Administration > Identity Management > External Identity Sources > SAML ID Providers:</p> <p>Signing certificate validation failed, error:</p> <p>The IdP signing certificate is self-signed and cannot be found in Trusted Certificates.</p> <p>Check Trusted Certificates contain the IdP signing certificate.</p>
CSCwk98467	Data Upgrade and Restore from Cisco ISE 3.3 to 3.4 fails if the username suffix is not configured in the REST ID store.
CSCwm05210	Getting a '500 internal error' when sending ISE 9060/ers/config/endpoint/{MAC address}/releaserejectedendpoint.
CSCwm35551	After exporting network devices from the Cisco ISE GUI, the values under Network Device Groups in the CSV file are different from the values in the Cisco ISE GUI.
CSCwm38203	<p>With the Bring Your Own Device (BYOD) workflow on MacOS 15.1 Beta 2, when you download the Cisco Network Setup Assistant application and try to open it, the following error is generated:</p> <p>Unable to check for updates</p>
CSCwm40972	In Cisco ISE release 3.4 Patch 1, when you configure a workload connection to AWS, only public and private IPv4 addresses are learned. IPv6 addresses aren't learned.
CSCwn62873	Known issue with Cisco ISE integration with Active Directory on Windows server 2025.

Known issues

Cisco ISE release 3.4 patch 1: Known issues

Table 13. Known issues for Cisco ISE release 3.4 cumulative patch 1

Feature	Known issue
Usage of IPv6 addresses in ACI connections	You must suspend the ACI connections before installing Cisco ISE release 3.4 patch 1 to ensure that the IPv6 addresses are maintained in the same format across the integrations.

Feature	Known issue
Patch rollback flow with newly supported operators	From Cisco ISE release 3.4 patch 1, IP Equals , IP Not Equals , In , Not In , Contains , and Not Contains operators are supported for workload classification rules and inbound SGT domain rules. When you use the Patch Rollback option for Cisco ISE release 3.4 Patch 1, the workload classification rules and inbound SGT domain rules that contain these operators will be deleted during the patch rollback flow, because these operators are not supported in Cisco ISE release 3.4.

Compatibility

Cisco ISE release 3.4 ISO, upgrade bundle, and Cisco ISE-PIC 3.4 ISO files replaced on software download site

Cisco ISE Release 3.4 ISO, Cisco ISE Release 3.4 Upgrade Bundle, and Cisco ISE-PIC 3.4 ISO files have been replaced on the [Cisco ISE Software Download](#) site. The filenames of the new files are:

- ise-3.4.0.608a.SPA.x86_64.iso
- ise-upgradebundle-3.1.x-3.3.x-to-3.4.0.608a.SPA.x86_64.tar.gz
- Cisco-ISE-PIC-3.4.0.608a.SPA.x86_64.iso

You can use Fedora Media Writer and BalenaEtcher USB tools in addition to Rufus to create a bootable USB device from the new ISO file.

The following steps are not required while creating a bootable USB device using the new ISO file:

- Replacing the term "cdrom" with "hd:sdb1" in the following files:
 - isolinux/isolinux.cfg or syslinux/syslinux.cfg
 - EFI/BOOT/grub.cfg
- Replacing the term "cdrom" with "harddrive --partition=/dev/disk/by-label/ADEOS --dir=/" in the ks.cfg file

For more information, see "[SNS Appliance Reference](#)" in the chapter "Additional Installation Information" in the Cisco Identity Services Engine Installation Guide, Release 3.4.

If you have used the previous files (for example, ise-3.4.0.608.SPA.x86_64.iso) for Cisco ISE Release 3.4 or Cisco ISE-PIC 3.4, there is no need to reinstall Cisco ISE or Cisco ISE-PIC. The new files include only changes to improve the installation process.

Upgrading to Cisco ISE release 3.4

You can directly upgrade to Release 3.4 from the following Cisco ISE releases 3.3, 3.2, and 3.1.

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

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](#).

For information about upgrade packages and supported platforms, see [Cisco ISE Software Download](#).

Cisco ISE on cloud

Native cloud environments must use the Cisco ISE backup and restore method for upgrades. Upgrades cannot be performed on Cisco ISE nodes deployed in native cloud environments. You must deploy a new node with a newer version of Cisco ISE and restore the configuration of your older Cisco ISE deployment onto it. For more information, see [Deploy Cisco Identity Services Engine Natively on Cloud Platforms](#).

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](#).

Supported hardware

Cisco ISE 3.4 can be installed on these Secure Network Server (SNS) hardware platforms. 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)

For more details on hardware platforms and installation of this Cisco ISE release, see the [Cisco Identity Services Engine Hardware Installation Guide](#).

Supported virtual environments

This table summarizes supported platforms and provides key details about Cisco ISE deployment options.

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

Table 14. Supported virtual environments

Virtual environment	Support details
VMware	<ul style="list-style-type: none"> • VMware 7.0.3 or later • In the case of vTPM devices, you must upgrade to VMware ESXi 7.0.3 or later releases. • OVA templates support VMware version 14 or later on ESXi 7.0, and ESXi 8.0. • ISO files support ESXi 7.0, and ESXi 8.0. • From Cisco ISE release 3.1, 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Supports Microsoft Windows Server 2012 R2 and later. • Supports Azure Stack HCI 23H2 and later versions. 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 QEM	<ul style="list-style-type: none"> • Supports QEMU 2.12.0-99 and later. • Cisco ISE cannot be installed on OpenStack.
Nutanix	<ul style="list-style-type: none"> • Supports Nutanix 20230302.100169.
Public cloud platforms	<ul style="list-style-type: none"> • Native support for Amazon Web Services (AWS), Microsoft Azure Cloud, and Oracle Cloud Infrastructure (OCI).

Browser compatibility

The Cisco ISE GUI is intended to be compatible with the most recent desktop version of most common browsers, including Chrome, Firefox, and Edge. In most cases, compatibility will extend one version behind their most recent release. Currently, you cannot access the Cisco ISE GUI on mobile devices.

Cisco ISE release 3.4 is validated on:

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

Validated external identity sources

Table 15. Validated external identity sources

External identity source	Details	Version
Active Directory	Microsoft Windows Active Directory 2012	Windows Server 2012
	Microsoft Windows Active Directory 2012 R2	Windows Server 2012 R2 Note: Cisco ISE supports all the legacy features in Microsoft Windows Active Directory 2012 R2. However, the new features in Microsoft Windows Active Directory 2012 R2, such as Protected User Groups, are not supported.
	Microsoft Windows Active Directory 2016	Windows Server 2016
	Microsoft Windows Active Directory 2019	Windows Server 2019
	Microsoft Windows Active Directory 2022	Windows Server 2022 with patch Windows10.0-KB5025230-x64-V1.006.msu
LDAP servers	SunONE LDAP Directory server	Version 5.2
	OpenLDAP Directory server	Version 2.4.23
	Any LDAP v3-compliant server	Any version that is LDAP v3 compliant
	AD as LDAP	Windows Server 2022 with patch Windows10.0-KB5025230-x64-V1.006.msu
Token servers	RSA ACE/server	6.x series
	RSA authentication manager	7.x and 8.x series
	Any RADIUS RFC 2865-compliant token server	Any version that is RFC 2865 compliant
Security Assertion Markup Language (SAML) Single Sign-On (SSO)	Microsoft Azure MFA	Latest
	Oracle Access Manager (OAM)	Version 11.1.2.2.0
	Oracle Identity Federation (OIF)	Version 11.1.1.2.0
	PingFederate server	Version 6.10.0.4
	PingOne Cloud	Latest
	Secure Auth	8.1.1
	Any SAMLv2-compliant identity provider	Any SAMLv2-compliant identity provider version
Open Database Connectivity (ODBC) identity source	Microsoft SQL server	Microsoft SQL servers 2012 and 2022
	Oracle	Enterprise Edition Release 12.1.0.2.0
	PostgreSQL	9.0
	Sybase	16.0
	MySQL	6.3

External identity source	Details	Version
Social Login (for Guest User Accounts)	Facebook	Latest

Supported antivirus and antimalware products

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

Validated OpenSSL version

Cisco ISE 3.4 is validated with CiscoSSL 7.3.410 based on OpenSSL 1.1.1za.

Related resources

See our [collection pages](#) for additional resources that you can use when working with Cisco ISE.

Legal information

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: www.cisco.com/go/trademarks. 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)

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.

© 2025 Cisco Systems, Inc. All rights reserved.