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 15
Resolved issues 17
Open issues 18
Known issues 21
Compatibility 23
Related resources 27
Legal information 27

© 2025 Cisco and/or its affiliates. All rights reserved.

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
2026-09-12	General availability of Cisco ISE release 3.4 cumulative patch 7.
2026-04-23	General availability of Cisco ISE release 3.4 cumulative patch 6.
2026-02-23	General availability of Cisco ISE release 3.4 cumulative patch 5.
2025-11-04	General availability of Cisco ISE release 3.4 cumulative patch 4.
2025-08-05	General availability of Cisco ISE release 3.4 cumulative patch 3.
2025-06-20	General availability of Cisco ISE release 3.4 cumulative patch 2.
2024-12-18	General availability of Cisco ISE release 3.4 cumulative patch 1.
2024-08-04	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 7 new features

Table 2. New features for Cisco ISE release 3.4 cumulative patch 7

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
Ease of setup	Support for Windows Server 2025	You can use Windows Server 2025 Active Directory domains as an external identity source in Cisco ISE for your identity management needs. This support allows you to integrate with the latest Windows Server infrastructure to manage user and machine authentications. Due to enhanced security settings in Windows Server 2025, password changes done through EAP-MS-CHAPv2 and EAP-GTC are disabled by default.
Ease of use	Lua scripts for attribute customization	Cisco ISE supports the use of Lua scripts to customize RADIUS attributes within authorization policies according to your requirements. You can use this capability to manipulate RADIUS attributes with precision, tailor network access control, and adapt to diverse network needs without modifying the core Cisco ISE code. Your scripts run in a secure, sandboxed Lua environment that restricts privileges, limits execution time, and uses safeguards to prevent malicious code and resource abuse. For more information, refer to "Lua scripts for attribute customization" in the Chapter "Segmentation" in the Cisco Identity Services Engine Administrator Guide, Release 3.4.
Software reliability	Export Prometheus data to external server	Prometheus Remote Write enables Primary PAN or standalone nodes to push real-time operational metrics to an external Prometheus server for centralized monitoring. To configure this feature, run the `application configure ise` command which provides a native mechanism to transmit data securely using various proxy and authentication settings.

Cisco ISE release 3.4 patch 6 new features

Table 3. New features for Cisco ISE release 3.4 cumulative patch 6

Product impact	Feature	Description
Software reliability	Allow server EKU certificates for Cisco pxGrid and IMS	Cisco ISE will support using server certificates with only the Server Authentication EKU for Cisco pxGrid and IMS. This update ensures your services remain compatible with new public CA standards. For internal services, use the Cisco ISE internal CA to avoid external certificate dependencies.
Ease of use	SGACL syntax validation	You can use the syntax validation feature in Cisco ISE to check your Security Group ACL (SGACL) commands for accurate policy configuration. You can validate the SGACL syntax while creating or editing ACLs by using the **Validate Syntax** option. You can verify commands against standard IPv4 and IPv6 formats.

Cisco ISE release 3.4 patch 5 new features

There are no new features in Cisco ISE release 3.4 patch 5.

Cisco ISE release 3.4 patch 4 new features

Table 4. New features for Cisco ISE release 3.4 cumulative patch 4

Product impact	Feature	Description
Ease of use	TACACS+ support to prevent Active Directory user lockout	The **Prevent Active Directory User Lockout** option helps reduce user lockouts caused by repeated failed login attempts with incorrect passwords. This feature is supported for both RADIUS and TACACS+ protocols. Cisco ISE uses these protocols to manage authentication requests and limit excessive failed logins, thereby minimizing account lockouts in Active Directory.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	Workload Connector Endpoints dashboard	The **Workload Connector Endpoints** dashboard in the **Context Visibility** page enables you to efficiently gather, analyze, and report data related to workload connectors. This dashboard displays endpoint attribute information collected from the **Workload Connectors** page. Click an endpoint's IP address to access or download detailed attribute information for endpoint analysis.
	New alarms for slow external resources and excessive TACACS+ activity	New alarms are introduced to enhance system monitoring and troubleshooting in Cisco ISE. These new alarms detect issues such as delays in accessing external systems or excessive traffic communication from TACACS+ devices, helping you identify and address them. These alarms detect: • high ping or communication latency between Cisco ISE nodes. • slow Active Directory (AD) connections. • slow Lightweight Directory Access Protocol (LDAP) connections. • slow Open Database Connectivity (ODBC) connections. • excessive TACACS communications.
	User and device authorization using Entra ID EAP-TLS and TEAP-TLS	Cisco ISE allows you to authorize devices and users through EAP or TEAP chaining. This enables secure network access control by combining certificate-based authentication with real-time information from Microsoft Entra ID. During authentication, Cisco ISE evaluates the certificate presented by the user or device without directly accessing Microsoft Entra ID. For authorization, you can configure a REST ID Store Attribute condition or REST ID Store Group in the policy. During authorization, Cisco ISE queries Microsoft Entra ID to retrieve relevant user, group, and device attributes. This information is then used by Cisco ISE to make informed authorization decisions.
	OAuth support for SMTP	You can enable or disable authentication settings for your Simple Mail Transfer Protocol (SMTP) servers in the Cisco ISE GUI. This release adds support for Microsoft OAuth authentication, in addition to basic password authentication.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
Hardware reliability	Support for Cisco Secure Network Server 3800 series appliance	The Cisco Secure Network Server (Cisco SNS) 3800 series appliances are based on the Cisco Unified Computing System (Cisco UCS) C225 M8 Rack Server and are configured specifically to support Cisco ISE. Cisco SNS 3800 series appliances are designed to deliver high performance and efficiency for a wide range of workloads. The Cisco SNS 3800 series appliances are available in these models: • Cisco SNS 3815 (SNS-3815-K9) • Cisco SNS 3855 (SNS-3855-K9) • Cisco SNS 3895 (SNS-3895-K9) The Cisco SNS 3815 appliance is ideal for small deployments. Cisco SNS 3855 and Cisco SNS 3895 appliances have several redundant components such as hard disks and power supplies and are suitable for larger deployments that require highly reliable system configurations. Cisco SNS 3895 is recommended for PAN and MnT personas. You must use only these OVA, ISO, and upgrade bundle files for Cisco SNS 3800 appliances: • Cisco-vISE-300-3.4.0.608b.ova • Cisco-vISE-600-3.4.0.608b.ova • Cisco-vISE-1200-3.4.0.608b.ova • Cisco-vISE-2400-3.4.0.608b.ova • ise-3.4.0.608b.SPA.x86_64.iso • ise-upgradebundle-3.1.x-3.3.x-to-3.4.0.608b.SPA.x86_64.tar.gz • ise-urtbundle-3.4.0.608b-1.0.0.SPA.x86_64.tar.gz Cisco SNS 3800 appliances are supported from Cisco ISE release 3.4 patch 4 onwards. **Note**: Cisco SNS 3855 appliances can be configured with one hard disk or four hard disks. We recommend that you enable only the PSN or pxGrid persona if your Cisco SNS 3855 appliance is configured with only one hard disk.
Software reliability	Red Hat OpenShift platform support	Cisco ISE release 3.4 patch 4 supports Red Hat OpenShift platform. You can deploy Cisco ISE VMs on Red Hat OpenShift Virtualization platform. This enables you to run and manage VM and container workloads on a single platform. **Note**: You must use only this ISO file for Red Hat OpenShift platform support: ise-3.4.0.608b.SPA.x86_64.iso.
	Monitor profiler traffic probes	These enhancements improve the resiliency and stability of Cisco ISE profiler service: • Probe-related processing is paused for chatty endpoints for a predefined cool-off period, thereby reducing system load in high-traffic environments. • Profiler queue utilization is managed based on defined thresholds (moderate, high, and maximum load), thereby prioritizing critical tasks and maintaining system stability during peak loads.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	USB disk encryption condition	You can use the **All External USB Drives** option (under **Policy > Policy Elements > Conditions > Posture > Disk Encryption Condition**) to check if external disk drives are encrypted with the selected product. When a USB drive is inserted, Cisco ISE dynamically detects the drive insertion, immediately evaluates the USB drive condition, and checks the compliance status of the endpoint. This process ensures continuous monitoring and enforcement of posture policies related to USB devices while the endpoint remains within the Cisco ISE-controlled network.

Cisco ISE release 3.4 patch 3 new features

Table 5. New features for Cisco ISE release 3.4 cumulative patch 3

Product impact	Feature	Description
Software reliability	Security service insertion	Security service insertion enhances network security by steering the traffic through firewalls based on predefined policies. This supports a zero-trust security solution. Security service insertion supports wired and wireless deployments and is compatible with Cisco and third-party firewalls, including on-premises and cloud-hosted solutions. Cisco ISE APIs play a crucial role in security service insertion by facilitating policy creation and allowing network devices to retrieve and enforce policies based on the configured source security groups.

Cisco ISE release 3.4 patch 2 new features

Table 6. New features for Cisco ISE release 3.4 cumulative patch 2

Product impact	Feature	Description
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	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. 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.
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 debug enabling	From Cisco ISE release 3.4 patch 2, the time-restricted debug enabling feature 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.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	Blast RADIUS vulnerability fix	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**. 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.
	Support for TACACS over TLS	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. If any of these attributes match, validation is successful, otherwise, validation fails. For each SAN attribute, multiple values are supported. You can view whether TACACS or TACACS over TLS authentication is enabled for a network device in the **Network Devices** page.
	API keys and certificate authentication support for Tenable Security Center	From Cisco ISE release 3.4 patch 2 onwards, these authentication methods are additionally supported for Tenable Security Center: • 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.

Cisco ISE release 3.4 patch 1 new features

Table 7. 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.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	TrustSec policy matrix GUI enhancements	The TrustSec policy matrix in Cisco ISE has been significantly optimized for deployments with large numbers of SGTs. Performance enhancements include more efficient data fetching and rendering, backend query optimization for faster handling of large SGT sets, and improvements to the Cisco ISE GUI for smoother scrolling and navigation. These enhancements increase scalability and responsiveness, providing a more efficient and seamless experience when managing extensive policy matrices.
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	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. You can create outbound SGT domain rules to designate target destinations for specific SGT bindings.
	SSHD service cryptographic algorithms enhancement	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: • MAC-algorithm • Hostkey • Hostkey-algorithm • Key-exchange-algorithm • SSH-client-hostkey-algorithm
	Workload classification rules	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”. You can specify the order of classification rule execution. You can drag and drop the rules to change the order of priority.
	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.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	Security Identifiers in certificates will not be used for authentication	Cisco ISE supports a new certificate format that includes Security Identifiers (SID) in the Subject Alternative Name (SAN) fields. SIDs in the SAN field will not be used for authentication, helping to prevent authentication failures caused by incorrect SID parsing. Cisco ISE supports these SAN_URI field formats in certificates: • SID and ID or GUID separated by a comma (in either order): <tag,sid>,<ID><GUID> or <ID><GUID>,<tag,sid> • SID and ID or GUID separated by a colon (in either order): <tag,sid>:<ID><GUID> or <ID><GUID>:<tag,sid> • Only SID present: <tag,sid> • Only ID and GUID present: <ID><GUID> All newer Microsoft certificates include the SID in the SAN_URI with the format: **tag:microsoft.com,2022-09-14:sid:<SID>**.
	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	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. 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.
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	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. You can choose the full upgrade or split upgrade option for a patch upgrade. • 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 8. New features for Cisco ISE release 3.4

© 2025 Cisco and/or its affiliates. All rights reserved.

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.
	Configure Virtual Tunnel Interfaces with Native IPsec	From Cisco ISE release 3.4, you can configure Virtual Tunnel Interfaces (VTIs) using the **Native IPse** 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	If you do not want to configure user data synchronization between Active Directory and Duo while creating a Duo connection, click **Skip** in the **Identity Sync** page. You will be taken to the **Summary** page directly. After you create a Duo connection, you can add identity sync configurations at any time.
	Support for multiple Cisco Application Centric Infrastructure connectors	Cisco ISE enables you to create and enforce consistent access policies across multiple domains. Cisco ISE can share the SGTs and SGT bindings with Cisco Application Centric Infrastructure (Cisco ACI). Cisco ISE can also learn the endpoint groups (EPGs), endpoint security groups (ESGs), and endpoint information from Cisco ACI. You can add multiple Cisco ACI connections to Cisco ISE. You can configure rules to manage the learned context in Cisco ISE and to optimize the context flows between Cisco ISE and Cisco ACI connectors. Cisco ISE supports Cisco ACI Multi-Tenant, and Multi-Virtual Routing and Forwarding deployments. You can define multi-fabrics through multiple connections. This integration supports multi-pod and individual Cisco ACI fabrics. 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.
	Enforcing domain controller selection with priority	You can now choose to override Cisco ISE's selection of domain controllers in case of a preferred domain controller failover. To do this, choose Administration > Identity Management > External Identity Sources > Active Directory > Advanced Tools > Advanced Tuning. Enter the name of the registry key in the **Name** field and **1** in the Value field. When the registry key is enabled, you can also choose to set the failback interval (in seconds). This ensures that in the case of a domain controller failover, Cisco ISE overrides the existing priority values and selects the next domain controller in the preferred list in the order of input from left to right. The value of this registry key is set to **0** by default. When 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.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	Enhanced password security	Cisco ISE now improves password security through these enhancements: • You can choose to hide the Show button for these field values, to prevent them from being viewed in plaintext during editing: Under **Network Devices**, • RADIUS Shared Secret • Radius Second Shared Secret Under **Native IPsec**, • Pre-shared Key To do this, choose Administration > Settings > Security Settings and uncheck the **Show Password in Plaintext** checkbox. • To prevent the RADIUS Shared Secret and Second Shared Secret from being viewed in plaintext during network device import and export, a new column with the header **PasswordEncrypted:Boolean(true|false)** has been added to the Network Devices Import Template Format. No field value is required for this column. If you are importing network devices from Cisco ISE Release 3.3 patch 1 or earlier releases, you must add a new column with this header to the right of the **Authentication:Shared Secret:String(128)** column, before import. If you do not add this column, an error message is displayed, and you will not be able to import the file. Network devices with encrypted passwords will be rejected if a valid key to decrypt the password is not provided during import.
	Localized ISE installation	While reinstalling Cisco ISE, you can use the **Localized ISE Install** option (option 25) in the `application configure ise` command to reduce the installation time. Though this option can be used for both Cisco Secure Network Server and virtual appliances, it significantly reduces the reinstallation time for Cisco Secure Network Servers.
	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.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
Ease of setup	Create a URL pusher pxGrid Direct connector	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 `reset-config` command. Additionally, the newly introduced `ipv6 default-gateway` command allows you to specify a default gateway using an IPv6 address. 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.
	TLS 1.3 support for Cisco ISE workflows	Cisco ISE release 3.4 allows TLS 1.3 to communicate with peers for these workflows: • 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 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.
Ease of use	Certificate authority diagnostic tool	To diagnose certificate management related issues, use the **CA Diagnostic Tool** option in the `application configure ise` command. This tool suggests the possible reasons and remediations for the identified issues, helps to fix the issues, and provides related logs for troubleshooting.
	Hotpatch details added to show version command	The `show version` CLI command now includes hotpatch details, if any, for a specific Cisco ISE release. To view hotpatch details on the Cisco ISE GUI, click the icon and choose **About ISE and Server.**
	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.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	GUI enhancements in Cisco ISE release 3.4	In Cisco ISE release 3.4, the Cisco ISE GUI has these enhancements to make the user experience more intuitive. • Single Click Access to Endpoint Information Objects in the **Context Visibility** page, such as the attribute details of endpoints in the Cisco ISE GUI, now have detailed information available to users with a single click. All endpoint attributes now appear on a single tab for ease-of-use and better visibility. You can click: • the MAC address of an endpoint to view all endpoint attributes on a single page. • the **See full detail** option on the top right corner of this page to view all endpoint details in a new browser tab, which you can also share. • the link icon next to the MAC address of an endpoint to open a full-page view of all endpoint details. These pages have been updated to include these enhancements: • Context Visibility > Endpoints. • Work Center > Guest Access > Identities > Endpoints. • Work Center > BYOD > Identities > Endpoints. • Work Center > Network Access > Identities > Endpoints. • Work Center > Profiler > Endpoint Classification. Retention of user preferences for column displays: When you change the column display of a table (adjust column width, hide or show columns, reorder columns, and so on) in the Cisco ISE GUI, your preferences are retained.
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, refer to the Cisco ISE API Reference Guide.

© 2025 Cisco and/or its affiliates. All rights reserved.

Changes in behavior

Cisco ISE release 3.4 patch 7: Changes in behavior

Table 9. Changes in behavior for Cisco ISE release 3.4 patch 7

Feature	Description
Change in negation operator evaluation for null attributes	You may notice a change in how your policies are evaluated when using negation operators, such as "Not Equals." If either the left-hand side (LHS) or right-hand side (RHS) attribute resolves to a null value, Cisco ISE now returns false, whereas it previously returned true. You can verify this by checking your policy-engine debug logs for the message: "Either of LHS or RHS value is null (undefined), evaluation result = false." This change could cause your existing policies to be deselected or fail to match as they did previously. To restore the original behavior for these conditions, you can update your affected policy rule by changing the operator from "Not Equals" to "Equals" and selecting the "is-not" option in the Cisco ISE GUI. By making this adjustment, your policy continues to function as you intend, maintaining consistent evaluation logic despite the updated handling of null attributes in negation operations. Refer to CSCws89421 and CSCwo12680 for more information.
Organizational-unit option for Active Directory CLI configuration	The identity-store active-directory command now supports an optional organizational-unit parameter when joining Cisco ISE to Active Directory. If provided, the ISE machine account is created in the specified organizational unit; otherwise, it is created in the default Computers organizational unit. The existing command can still be used without the optional parameter. Refer to CSCwt68081 for more information.
Support for Active Directory domains hosted on Windows Server 2025	Cisco ISE now supports joining Active Directory domains hosted on Windows Server 2025 and rotating the machine-account password by using the Kerberos Change Password protocol instead of legacy SAM RPC password-change methods. Refer to CSCws27786 for more information.
OCSP validation for pxGrid client certificates	Cisco ISE applies certificate status validation during pxGrid client authentication. Certificate status validation includes Online Certificate Status Protocol (OCSP) and certificate revocation list (CRL) validation. Cisco ISE first validates the certificate chain and then applies the existing validation policy for the issuing trusted certificate authority. Before this patch, Cisco ISE did not apply this policy during pxGrid client certificate authentication. This change does not require pxGrid-specific certificate status validation configuration. After the upgrade, a pxGrid integration might fail if its client certificate does not satisfy the configured certificate status validation policy. Before you upgrade, verify the certificate trust chain and certificate status validation settings for each certificate-based pxGrid integration. For configuration details, refer to Trusted Certificate Settings. Confirm that the OCSP or CRL responder reports each active pxGrid client certificate as GOOD. After the upgrade, reconnect each integration and use the pxGrid Live Log to verify successful certificate validation.
Stricter DNS SAN validation for node synchronization	From Cisco ISE release 3.4 patch 7, stricter DNS Subject Alternative Name (SAN) validation applies to bulk synchronization between nodes. After installing this patch in a multinode deployment, nodes might appear as **Out of Sync** if the Admin certificate does not contain the node's fully qualified domain name (FQDN) as an exact DNS SAN entry or as a matching wildcard DNS SAN entry. To restore synchronization, deregister the affected nodes, update their Admin certificates, and replace the certificate on the Primary PAN first and then on each remaining node, one at a time. Confirm that synchronization is complete before proceeding to the next node. Refer to CSCww70696 for more information.

Cisco ISE release 3.4 patch 4: Changes in behavior

Table 10. Changes in behavior for Cisco ISE release 3.4 patch 4

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
New Cisco ISE configuration options	Cisco ISE release 3.4 patch 4 adds these node-specific options to the **application configure ise** command: • [44] Reset Remote Support Authorization Service • [45] Enable/Disable Fragmentation of RADIUS Packets **Configuring Option 45 for packet handling** Option 45 allows you to manage the behavior of Don't Fragment (DF) bit. By default, Cisco ISE sets the DF bit on packets that exceed the interface MTU. Because this behavior may cause packet-handling conflicts depending on your network configuration, use Option 45 to enable or disable the setting of the DF bit.
CSCwo12680	An issue has been identified where authentication and authorization is successful even when both the left-hand side (LHS) and right-hand side (RHS) attributes within an authentication or authorization policy condition resolve to null values. When the Equal operator is applied to these null attributes, Cisco ISE incorrectly evaluates the policy condition as true, which can result in unintended policy enforcement and potential security gaps. As a workaround, avoid configuring authentication and authorization policy rules that rely on attributes prone to resolving to null values. Policy rules must be designed to prevent scenarios where both the LHS and RHS attributes evaluate to null simultaneously, thereby maintaining the intended security posture of the authentication or authorization policy. This would restore the intended security posture and prevent the unintended policy enforcement caused by CSCwo12680.

Cisco ISE release 3.4 deprecated features

Table 11. Deprecated features for Cisco ISE release 3.4

Feature	Description
End of support for Legacy IPsec (ESR)	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	Configuring RSA or RADIUS external databases for API authentication is no longer supported.

© 2025 Cisco and/or its affiliates. All rights reserved.

Feature	Description
Support for Transport Gateway removed	Cisco ISE no longer supports Transport Gateway. These Cisco ISE features used Transport Gateway as a connection method: • Cisco ISE Smart Licensing - If you use Transport Gateway as the connection method in your smart licensing configuration, you must edit the setting before you upgrade to Cisco ISE release 3.4. You must choose a different connection method as Cisco ISE release 3.4 does not support Transport Gateway. If you upgrade to Cisco ISE release 3.4 without updating the connection method, your smart licensing configuration is automatically updated to use the Direct HTTPS connection method during the upgrade process. You can change the connection method at any time after the upgrade. • Cisco ISE Telemetry - Transport Gateway is no longer available as a connection method when using Cisco ISE Telemetry. The telemetry workflow is not impacted by this change.
GUI deprecations	These pages have been removed from the Cisco ISE GUI in Cisco ISE release 3.4: • Location Services (Administration > Network Resources > Location Services). • NAC Managers (Administration > Network Resources > NAC Managers).

Cisco ISE release 3.4 operational changes

Table 12. Operational changes for Cisco ISE release 3.4

Feature	Known issue
Cisco ISE upgrade notice: RSA_PSS protocol configuration update	RSA_PSS is now managed under **Allowed Protocols** in the Cisco ISE GUI. When you upgrade to Cisco ISE release 3.4, RSA_PSS is enabled by default. If you previously disabled RSA_PSS using the Cisco ISE CLI, you must disable it again under **Allowed Protocols** in the GUI after upgrading to Cisco ISE release 3.4.

Resolved issues

Cisco ISE release 3.4 patch 7: Resolved issues

You can use the Cisco Bug Search Tool to search for a specific bug or to search for all resolved bugs in a release.

Cisco ISE release 3.4 patch 6: Resolved issues

You can use the Cisco Bug Search Tool to search for a specific bug or to search for all resolved bugs in a release.

Cisco ISE release 3.4 patch 5: Resolved issues

You can use the Cisco Bug Search Tool to search for a specific bug or to search for all resolved bugs in a release.

Cisco ISE release 3.4 patch 4: Resolved issues

You can use the Cisco Bug Search Tool to search for a specific bug or to search for all resolved bugs in a release.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco ISE release 3.4 patch 3: Resolved issues

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

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

Table 13. 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

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 1: Resolved issues

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: Resolved issues

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

Open issues

Cisco ISE release 3.4 patch 7: Open issues

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

Bug ID	Description
CSCwu53699	After a Cisco ISE node restarts, the Vulnerability Assessment (VA) services might not start automatically if the internal watchdog times out while waiting for the VA Database to become ready. This is more likely to occur after unclean shutdowns or periods of high system load. When the watchdog reaches its retry limit, it stops attempting to restart the VA services, causing them to remain down until manually recovered.
CSCwt34939	Extracting the GUID from the SAN URI causes an incorrect epid assignment.
CSCwv09701	Creating an endpoint statically or through import is not allowed because of the RCM flow.
CSCwu54421	An unvalidated endpoint owner lookup causes a NullPointerException when endpoint ownership is transferred to the RCM state machine.
CSCww18723	An epid is not generated when RCM merge is disabled.
CSCww19459	Endpoint purge VCS evaluation skips all endpoints when RCM is disabled.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco ISE release 3.4 patch 6: Open issues

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

Table 14. Open issues in Cisco ISE release 3.4 cumulative patch 6

Bug ID	Description
CSCwc30161	After node registration or a restore operation, the application service may fail to initialize due to a LifecycleException related to an empty trustAnchors parameter. This error appears in the catalina.out file as a failure to start the component. To resolve this issue, refer to the following workaround: de-register the node, regenerate the ISE Root CA on the Policy Administration Node (PAN), and re-register the node.
CSCwu13703	When Entra ID is utilized in Authorization Policies, users may observe authentication latency or missing device and user group memberships. These symptoms often occur when the Entra ID configuration includes assigned roles or Administrative Units, or when the Directory.Read.All application permission is not granted. To address this, refer to the workaround of granting the Directory.Read.All application-type API permission and performing a test connection on the REST ID Store to refresh the token.
CSCwk80440	Exporting Network Access Devices (NAD) configured with TrustSec settings fails after a Change of Authorization (CoA) push, resulting in an empty CSV file. This issue occurs because generating a PAC and pushing a CoA causes an incorrect value to be set in a network device database field.
CSCwu56865	You may encounter two issues when using a REST Identity Store with Microsoft Entra ID. First, authorization attributes are silently dropped if a user belongs to an Entra ID group with a display name containing the substring "error" regardless of case. To resolve this, refer to the workaround of renaming or removing the affected group display names. Second, authentication fails for users with an apostrophe in their userPrincipalName. To address this, refer to the workaround of renaming the user UPN in Microsoft Entra ID or using an alternate UPN alias that does not contain an apostrophe.

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

Cisco ISE release 3.4 patch 5: Open issues

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

Table 15. Open issues in Cisco ISE release 3.4 cumulative patch 5

Bug ID	Description
CSCwt16625	When creating or modifying a Facebook Social Login provider in Cisco ISE, you may encounter an error stating the root CA chain is missing or untrusted. This is because Facebook (Meta) is updating their SSL certificate chain in November 2025 to DigiCert Global Root G2, which Cisco ISE trusts only for CISCO_SERVICES by default. To resolve this, edit the "DigiCert Global Root G2 CA" certificate in Cisco ISE Trusted Certificates and enable **Trust for authentication within ISE**.

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

Cisco ISE release 3.4 patch 4: Open issues

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

Table 16. Open issues in Cisco ISE release 3.4 cumulative patch 4

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCws52326	Cisco ISE does not correctly evaluate custom attributes for endpoints shown on the Context Visibility page. As a result, authorization rules that use custom attributes may be matched inaccurately, causing incorrect authorization profiles to be assigned.
CSCws30603	You may encounter an issue where user group membership cannot be fetched if an Entra AD user belongs to more than 20 groups. This results in authorization failures, as the Microsoft Graph API used by Cisco ISE returns only the first 20 groups for each user. If the required group for your policy is not included in these first 20, group membership evaluation will fail.
CSCws18653	When you upgrade to Cisco ISE release 3.4 patch 4 from Cisco ISE release 3.4 patch 3 in a standalone deployment, the **RADIUS Authentication Detail Reports** may be missing sections such as attributes, results, and steps. This issue occurs because the expected database patch script (mntpatchinstall_v4.sql) was not run, resulting in an error in the debug log file (collector.log) indicating that a table or view does not exist. We recommend that you roll back both patch 4 and patch 3, then reapply patch 4 to restore the missing report details.

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

Cisco ISE release 3.4 patch 3: Open issues

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

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

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

Table 17. 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.

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

Cisco ISE release 3.4 patch 1: Open issues

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

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

Cisco ISE release 3.4: Open issues

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

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

© 2025 Cisco and/or its affiliates. All rights reserved.

Known issues

Cisco ISE release 3.4 patch 7: Known issues

There are no known issues in Cisco ISE release 3.4 patch 7.

Cisco ISE release 3.4 patch 6: Known issues

There are no known issues in Cisco ISE release 3.4 patch 6.

Cisco ISE release 3.4 patch 5: Known issues

Table 18. Known issues for Cisco ISE release 3.4 cumulative patch 5

Bug ID	Known issue
CSCws61409	If Cisco ISE release 3.4 patch 5 is installed on top of Cisco ISE release 3.4 patch 1 through Cisco ISE release 3.4 patch 3, then the **Secure System Diagnostics report** and **SXP Binding report** appear empty. If Cisco ISE release 3.4 patch 5 is installed on top of Cisco ISE release 3.4 patch 4, then the reports **Change Configuration Audit**, **Posture-related reports**, and **SXP Binding reports** appear empty. If Cisco ISE release 3.4 patch 5 is upgraded from Cisco ISE release 3.3 patch 8 or Cisco ISE release 3.3 patch 9, then the **Change Configuration Audit**, **Posture-related report**, and **Active Directory Operations report** appear empty.

Cisco ISE release 3.4 patch 4: Known issues

Table 19. Known issues for Cisco ISE release 3.4 cumulative patch 4

© 2025 Cisco and/or its affiliates. All rights reserved.

Feature	Known issue
Cisco ISE on cloud vulnerability fix	When upgrading to Cisco ISE release 3.4 patch 4 from patch 1, patch 2, or any other Cisco ISE release, Cisco ISE will perform a mandatory restart of internal services upon login. This restart is required to address the vulnerability identified in CSCwn63400. This fix is applicable only to cloud deployments. To fully apply the fix, you must synchronize all the nodes in your deployments with the PAN using one of these options: • **Proceed with Auto Sync**: All nodes will be restarted to ensure immediate synchronization and application of the fix. You can verify the synchronization status of nodes in your deployment in the **Deployment Nodes** page (**Administration > System > Deployment**). We recommend this option to ensure automatic synchronization across all nodes. • **Proceed with Manual Sync**: After the restart, you must manually synchronize all nodes as soon as possible to prevent desynchronization. If nodes are desynchronized, you must deregister, reset the configuration, and then register the nodes again to resolve the issue. Manual synchronization is critical to maintain deployment integrity after the mandatory restart. Without timely manual sync, key features such as endpoint database updates and certificate-based authentications will fail due to configuration mismatches. • **Decide Later**: Options for fixing the vulnerability will be available to you at your next login. **Note**: This requirement does not apply if you have installed the latest Cisco ISE release 3.4 patch 3 AMI before upgrading to Cisco ISE release 3.4 patch 4 and later releases.

Cisco ISE release 3.4 patch 3: Known issues

Table 20. Known issues for Cisco ISE release 3.4 cumulative patch 3

Feature	Known issue
Initialization issue in Log Analytics after upgrade to Cisco ISE release 3.4 patch 3	After upgrading from Cisco ISE release 3.3 patch 7 to Cisco ISE release 3.4 patch 3, you may find the application server stuck in an "initializing" state. This occurs because the Kibana migration fails when it encounters unrecognized telemetry objects from previous releases. You can resolve this by manually deleting the problematic document and temporarily modifying the Kibana configuration to allow the migration to complete. Refer to the instructions in the workaround section of CSCwt07284.

Cisco ISE release 3.4 patch 2: Known issues

There are no known issues in Cisco ISE release 3.4 patch 2.

Cisco ISE release 3.4 patch 1: Known issues

Table 21. 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.

© 2025 Cisco and/or its affiliates. All rights reserved.

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.

Cisco ISE release 3.4: Known issues

There are no known issues in Cisco ISE release 3.4.

Compatibility

Upgrade packages replaced

Cisco ISE release 3.4 upgrade bundle files have been replaced on the Cisco ISE Software Download site.

This entails:

- resolution of bug CSCwt99926.
- that the filenames of the new files will have "c" appended to the build number (for example, ise upgradebundle-3.1.x-3.3.x-to-3.4.0.608c.SPA.x86_64.tar.gz).
- that existing Cisco ISE release 3.4 cumulative patches will continue to work with this new upgrade bundle.

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

Cisco ISE release 3.4 OVA, ISO, and upgrade bundle files have been replaced on the Cisco ISE Software Download site. You must use only these files for Cisco SNS 3800 appliance support:

- Cisco-vISE-300-3.4.0.608b.ova
- Cisco-vISE-600-3.4.0.608b.ova
- Cisco-vISE-1200-3.4.0.608b.ova
- Cisco-vISE-2400-3.4.0.608b.ova
- ise-3.4.0.608b.SPA.x86_64.iso
- ise-upgradebundle-3.1.x-3.3.x-to-3.4.0.608c.SPA.x86_64.tar.gz
- ise-urtbundle-3.4.0.608b-1.0.0.SPA.x86_64.tar.gz

Cisco SNS 3800 appliances are supported from Cisco ISE release 3.4 patch 4. Support for the Cisco SNS 3800 OVA and ISO with the Cisco SNS 3800 profile is only available from Cisco ISE release 3.4 patch 4.

Upgrading to Cisco ISE release 3.4

You can directly upgrade to release 3.4 from these 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, refer to the Cisco Identity Services Engine Upgrade Guide.

© 2025 Cisco and/or its affiliates. All rights reserved.

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

Cisco SNS 37x5 appliance firmware upgrade

Before upgrading your Cisco SNS 37x5 appliance firmware from 4.x to 6.x, you must install the ise-apply-CSCwu00192_3.4_patchall-SPA.tar.gz hot patch if you are using Cisco ISE release 3.4 patch 6 or earlier versions. This step is mandatory and must be completed before starting the firmware upgrade process.

After the BIOS and HUU upgrades complete successfully, verify the TPM firmware as follows:

1. In the CIMC web UI, navigate to **Chassis > Inventory > TPM**.
2. If the TPM firmware version is 7.86 or later, no further action is required.

   If the version is 7.85 or earlier:

   In the CIMC web UI, navigate to **Host Power > Power Cycle**.

   Stop Cisco ISE services if the OS has booted.

   After the CIMC reboots, verify that the TPM firmware version is now 7.86 or later.

This issue is resolved in Cisco ISE release 3.4 patch 7. If you are running this patch or a later version, you do not need to install the hot patch. However, you must verify the TPM firmware and perform a reboot if the TPM firmware version is 7.85 or earlier.

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. To successfully deploy Cisco ISE natively in cloud environments, refer to Deploy Cisco ISE Natively on Cloud Platforms. For information on supported Cisco ISE instances, refer to Cisco ISE instances and intended usage.

Install a new patch

For instructions on how to apply the patch to your system, refer to 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, refer to the " Patch Install" section in the Cisco Identity Services Engine CLI Reference Guide.

Verified hardware

Cisco ISE release 3.4 can be installed on these Secure Network Server (SNS) hardware platforms. For appliance hardware specifications, refer to 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)
- Cisco SNS-3815-K9 (small)

© 2025 Cisco and/or its affiliates. All rights reserved.

- Cisco SNS-3855-K9 (medium)
- Cisco SNS-3895-K9 (large)

Note: Cisco SNS 3800 appliances are supported from Cisco ISE release 3.4 patch 4 onwards.

For more details on hardware platforms and installation of this Cisco ISE release, refer to the Cisco Identity Services Engine Hardware Installation Guide.

Verified virtual environments

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

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

Table 22. Verified virtual environments

Virtual environment	Support details
VMware	• ISO files support ESXi 7.0, ESXi 8.0, and ESXi 9.0. • OVA templates support VMware version 14 or later on ESXi 7.0, ESXi 8.0, and ESXi 9.0. • In the case of vTPM devices, you must upgrade to VMware ESXi 7.0.3 or later releases. • You can use the VMware migration feature to migrate VM instances (running any persona) between hosts. Cisco ISE supports both hot and cold migration. Hot migration is also called live migration or **vMotion**. Cisco ISE need not be shut down or powered off during the hot migration. You can migrate the Cisco ISE VM without any interruption in its availability.
VMware Cloud Solutions on public cloud platforms	• AWS: Host Cisco ISE on a software-defined data center provided by VMware Cloud on AWS. • Azure VMware Solution: Runs VMware workloads natively on Microsoft Azure. • Google Cloud VMware Engine: Runs software-defined data center by VMware on Google Cloud.
Microsoft Hyper-V	• Supports Microsoft Windows Server 2012 R2 and later. • Supports Azure Stack HCI 23H2 and later 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	• Supports QEMU 2.12.0-99 and later. • Cisco ISE release 3.4 patch 4 and later releases support OpenStack. Note: You must use this ISO file for OpenStack support: ise-3.4.0.608b.SPA.x86_64.iso

© 2025 Cisco and/or its affiliates. All rights reserved.

Virtual environment	Support details
Nutanix	• Supported and verified Nutanix versions: AOS 7.3.1.7 AVH 10.3.1.7, AOS 7.5.1.2 AVH 11.0.1.1, AOS 7.5.0.6 AVH 11.0.0.2, AOS 7.0 AHV 10.0, AOS 6.8 AHV 20230302.100169. • Supports Nutanix Cloud Clusters (NC2).
Public cloud platforms	• Native support for Amazon Web Services (AWS), Microsoft Azure Cloud, and Oracle Cloud Infrastructure (OCI).
Red Hat OpenShift	• Red Hat OpenShift container platform 4.19 and later. • Cisco ISE must be deployed on OpenShift platform using the standard Cisco ISE ISO image. Deploying Cisco ISE using OVA templates is not supported.

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 supported and verified 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.

Verified external identity sources

Table 23. Verified 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

© 2025 Cisco and/or its affiliates. All rights reserved.

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

Verified antivirus and antimalware products

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

Verified OpenSSL version

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

Related resources

Refer to 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.

© 2025 Cisco and/or its affiliates. All rights reserved.

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.

© 2026 Cisco Systems, Inc. All rights reserved.