Release Notes for Cisco Identity Services Engine, Release 3.5

Contents

Cisco Identity Services Engine, Release 3.5 3
New software features 3
Changes in behavior 20
Resolved issues 24
Open issues 24
Known issues 26
Compatibility 28
Related resources 32
Legal information 32

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Identity Services Engine, Release 3.5

Cisco Identity Services Engine (ISE) release 3.5 brings significant enhancements to network management, focusing on improved security and user experience. This release introduces full single-stack IPv6 support, expanding the range of configurations and supported features such as portals, RADIUS services, and APIs. A new pxGrid API enhances endpoint access, and pxGrid Cloud has expanded to support additional regions with easier integration through an Integration Catalog. Dedicated resource allocation for Active Directory join points, along with new alarms and monitoring features strengthen the monitoring capabilities of Cisco ISE. From this release, the Cognitive Threat Analytics (CTA) adapter is no longer supported for Threat Centric Network Access Control (TC-NAC) flows, indicating a strategic shift in security focus.

Security and compliance are further strengthened with OAuth2 authentication support, remote TAC support authorization, and alignment with federal certifications like DoDIN APL, FIPS 140-3, and Network Device Collaborative Protection Profile (NDcPP) v3.0e for Common Criteria certification. The release enhances profiling and authorization capabilities with SNMP-based device profiling and user/device authorization using EAP-TLS and TEAP-TLS. Security is bolstered by the addition of TACACS over TLS and expanded TLS 1.3 support for various workflows. User experience improvements include features such as a country code drop-down for guest password resets and time-restricted debug settings. Additionally, changes in the Cisco ISE licensing strategy mean that features such as pxGrid, pxGrid Direct, Profiling Services, and TrustSec will now consume licenses based on the number of active endpoints. However, enforcement for out-of-compliance licenses has not yet been implemented. Together, these enhancements provide a comprehensive, secure, and user-friendly network management solution.

This document describes the features, issues, and limitations of Cisco ISE release 3.5.

Table 1. New and changed information

Date	Description
2026-09-14	General availability of Cisco ISE release 3.5 cumulative patch 4.
2026-04-13	General availability of Cisco ISE release 3.5 cumulative patch 3.
2026-02-26	General availability of Cisco ISE release 3.5 cumulative patch 2.
2025-12-15	General availability of Cisco ISE release 3.5 cumulative patch 1.
2025-09-22	General availability of Cisco ISE release 3.5.

New software features

This section provides a brief description of the new software features introduced in this release.

Cisco ISE release 3.5 patch 4 new features

Table 2. New features in Cisco ISE release 3.5 cumulative patch 4

Product impact	Feature	Description
Ease of use	Updated profiling license requirements	Advantage license consumption for profiling has been updated to align with the behavior in Cisco ISE release 3.4. License consumption is now determined strictly by the attributes referenced in your matched authorization policy rule. Advantage license consumption is determined as follows:

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		• **Advantage license consumed**: An Advantage license is consumed if your authorization policy rule references dynamically assigned profiling attributes. These include EndpointPolicy, Endpoint IdentityGroup, LogicalProfile, or the four MFCs (Manufacturer, Model, OS, and Device Type). • **Advantage license not consumed**: An Advantage license is not consumed if your rule references only statically assigned attributes, even if the endpoint is dynamically profiled. This logic applies regardless of the authentication method, including certificate-based authentication or Authentication Bypass (MAB). The licensing behavior for specific endpoints is determined as follows: • **Statically assigned endpoints**: If an identity group is manually assigned to an endpoint, an Advantage license is not consumed if the matched rule references only that static group. However, if the rule also references a dynamic profiling attribute, an Advantage license is consumed, even if a static assignment is present. • **Guest endpoints**: Once a guest completes the portal process and is assigned a static identity group, an Advantage license is not consumed if the matched rule references that static guest group. Before the portal process is complete, while the static group remains unassigned, an Advantage license is consumed if the rule matches a dynamic profiling attribute.
	Cisco Support Assistant	Cisco Support Assistant is integrated directly into the Cisco ISE GUI to streamline your troubleshooting workflow. This feature enables you to open Technical Assistance Center (TAC) support cases, manage documentation, and perform diagnostics without leaving the Cisco ISE GUI. By centralizing these tasks, you can reduce context switching and resolve issues more efficiently through a unified self-service experience. You can now create support cases, upload debug logs, and view your existing case history directly within the interface. The assistant also includes tools for screen recording and file uploads, allowing you to provide comprehensive diagnostic information to TAC.
	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.
Software reliability	Posture policy export and import	You can now export and import posture policies to streamline the management and replication of endpoint compliance configurations across deployments. This feature enables the seamless transfer of policy definitions between Cisco ISE instances, simplifying migrations and ensuring configuration consistency. The import workflow includes guided conflict resolution for rules and conditions, while exported files are secured with AES-GCM-256 encryption to maintain data integrity during transit.
	Anomaly handling and	Cisco ISE now enforces strict reprofiling for endpoints that authenticate using the RADIUS attribute Service-Type (6) with a value of Call-Check (10).

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	probe obsolescence detection	When an endpoint reconnects and fewer probe attributes are available, Cisco ISE removes selected initial profiling data collected through DHCP, DHCP-SPAN, CDP, LLDP, mDNS, and Wi-Fi analytics. It retains data from active probes, custom attributes, and on-demand probes such as NMAP and SNMP to preserve the endpoint's relevant security and profiling context. To minimize false detections, maintain consistent probe parity throughout your network infrastructure. For example, ensure the Cisco AV pair stays uniform on all network devices. Cisco ISE relies on classification results from anomaly detection and on consistent profiling across probes, such as LLDP and CDP, provided by various vendors. Maintaining this consistency reduces incorrect classifications and improves endpoint identification and profiling accuracy. Cisco ISE provides OpenAPI-based configuration capabilities for creating optional filters that control detection within predefined identity groups and suppress false detections for specific endpoints. For more information, refer to the Cisco ISE API Reference Guide.
	Support for SMB version 3.x	SMB version 3.x is now used by default. If Active Directory does not permit SMB version 3.x, Cisco ISE automatically falls back to SMB version 2.x.

Cisco ISE release 3.5 patch 3 new features

Table 3. New features in Cisco ISE release 3.5 cumulative patch 3

Product impact	Feature	Description
Ease of use	High availability and failover support for TC-NAC nodes in Cisco ISE	High availability and failover support for TC-NAC nodes is now available, ensuring continuous Cisco ISE service in the event of a primary TC-NAC node failure. You can configure up to two TC-NAC nodes per deployment: one primary and one secondary, with the primary node assuming the active TC-NAC role. If only one TC-NAC node is present, it automatically becomes primary and assumes the active role. All role changes are tracked in the Change Configuration Audit for compliance.
	Continuous reassessment	Continuous reassessment helps you monitor endpoint health and posture in real time using Cisco Secure Client. When you enable this option, Cisco Secure Client performs continuous reassessment and detects posture changes as they occur for certain events and at regular intervals of 10 minutes for others. This capability helps you quickly identify dynamic posture changes and enhances visibility into endpoint behavior through continuous monitoring and reporting. Cisco Secure Client 5.1.17.3382 and later versions support continuous reassessment.
	OAuth support for MDM vendors	You can enhance security by using OAuth 2.0 to integrate with MDM vendors. When adding a server, you can choose from two new authentication types: **OAuth - Client Credentials - Intune** (specifically for Microsoft Intune) or **OAuth - Client Credentials - Generic** (for vendors like Jamf Pro and Omnissa). This support allows you to automatically reauthorize sessions for non-compliant endpoints, providing a secure alternative to basic authentication.
	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. SGACL syntax can be validated while creating or editing ACLs by clicking on the **Validate Syntax** button. You can verify commands against standard IPv4 and IPv6 formats.
	Enhanced user interface for TrustSec policy management	The TrustSec Policy page in Cisco ISE has a redesigned layout and modern visual elements that improve user experience. The streamlined interface provides visual clarity, so you can navigate and understand policy configurations easily

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		Intuitive controls and well-organized policy components reduce complexity, making policy management tasks simpler. The optimizations allow you to create, modify, and review policies efficiently. You gain more effective experience when managing TrustSec Security Group Access Control Lists (SGACL) and policy matrices.
	The Workload Connector Endpoints dashboard	The **Workload Connector Endpoints** tab in **Context Visibility** enables you to efficiently gather, analyze, and report data related to Workload connectors. This tab displays endpoint attribute information collected from the **Workload Connectors** page. By clicking on an endpoint's IP address, you can access or download detailed attribute information for endpoint analysis.
	FQDN to SGT mapping with multiple IP addresses in global deployment	You can use IP and hostname SGT static mappings in Cisco ISE to deploy SGT information across your TrustSec environment. These mappings can be configured in Cisco ISE to ensure that all resolved IP addresses for a specific hostname are captured and mapped to the correct SGT. This feature is particularly useful for global deployments where a single hostname may resolve to different IP addresses depending on the location.
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.
Software reliability	Include **Message-Authenticator in all Cisco ISE RADIUS response packets**	Cisco ISE now allows including the **Message-Authenticator RADIUS attribute in all response packets** (Access-Accept, Access-Reject, and Access-Challenge). This setting can be enabled per-NAD or through Default Device settings.
	Support for HTTP 2.0	The API gateway supports HTTP 2.0-based requests starting with Cisco ISE release 3.5 patch 3.
	Allow server EKU certificates for Cisco pxGrid and IMS	Cisco ISE now supports 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.
	IPv6 Support for SXP	You can now enable the SXP service for IPv6 nodes by selecting the **Enable SXP Service** check box under Deployment Settings. The **IPv6 Address** field is automatically populated when you select the network interface, and a new field called **Node ID** has been added. The Node ID is an IPv4 address that uniquely identifies the SXP node within the network. If the interface has an IPv4 address or is configured as dual-stack, the Node ID is auto-populated. However, if the interface uses only an IPv6 address, you must manually enter an IPv4 address for the Node ID.
	IPv6 support for TrustSec Policy download and servers list via RADIUS	Cisco ISE now supports IPv6 for TrustSec AAA Servers in addition to IPv4. This enhancement enables TrustSec devices to authenticate against Cisco ISE servers using IPv6 addresses, thereby improving network flexibility and deployment options.

Cisco ISE release 3.5 patch 2 new features

There are no new features in Cisco ISE release 3.5 patch 2.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco ISE release 3.5 patch 1 new features

Table 4. New features in Cisco ISE release 3.5 cumulative patch 1

Product impact	Feature	Description
Ease of use	Enhancements to user attribute monitoring for CoA	You can now use these enhancements for user attribute monitoring with Change of Authorization (CoA) based on Microsoft Entra ID attribute updates: • New date and time attributes are added to the list of existing user attributes. • You can now select custom directory extension attributes in the format **extension_<GUID>_<attributeName>** from the **User Attributes** tab.
	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.
	Grace period settings for posture policies	The **Posture General Settings** page (under Administration > System > Settings > Posture > General Settings) now provides an additional option to configure **Grace Period Settings** for posture policies. This enhancement allows you to define a time threshold for policy violations by selecting one of the two options: • Min: Displays the shortest time to resolve all issues. • Max: Displays the longest time to resolve all issues.
Software reliability	OpenID Connect authentication for self-registered guest portal	Cisco ISE supports OpenID Connect (OIDC) authentication for self-registered guest portals. You can configure Microsoft Entra ID or a generic OIDC identity provider, such as Okta, as the identity store for authenticating the endpoints in the guest flow. If you have selected Microsoft Entra ID as the identity provider, you can fetch the groups and attributes from Microsoft Entra ID using the Microsoft Graph API. You can also use the ID token or the UserInfo Endpoint API to fetch the groups and attributes from Microsoft Entra ID.
	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 3.5 new features

Table 5. New features in Cisco ISE release 3.5

Product impact	Feature	Description
API experience	New pxGrid API: Endpoint topic	The **Endpoint** topic provides access to endpoints connected to a Cisco ISE-managed network device.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
Ease of setup	Cisco ISE Data Grid Service network requirements	The Cisco ISE Data Grid Service requires these network ports to be open for optimal performance and connectivity: • Port 47500: Supports node discovery and deployment formation. • Port 47100: Enables internal communication between nodes. • Port 10800: Supports the establishment of client connections.
	Single-stack IPv6 support	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 new **`ipv6 default-gateway`** command allows you to specify a default gateway using an IPv6 address.

© 2026 Cisco and/or its affiliates. All rights reserved.

	Support for IPv6 single stack configuration	Some features supported IPv4 and IPv6 dual stack configuration prior to Cisco ISE release 3.5. If you choose to run Cisco ISE in an IPv6 single stack configuration, these are supported: • Portals > Admin portal access • Portals > CA Components EST and SCEP • Portals > My Devices • Portals > Certificate Provisioning • Portals > Guest -Hotspot • Portals > Guest – Self Register • Portals > Guest Sponsor • Portals > Sponsored Guest • Portals > MDM • Portals > Posture – Client Provisioning • IPv6 Single Stack Support Infrastructure > Infra IPv6 Single Stack • RADIUS > Authentication, Accounting Authorization, Attributes, Audit/Debug logs, Proxy, CoA, and Policy • RADIUS > OSCP • RADIUS > Secure Syslog Targets • RADIUS > DACL download • CARS Services > SSH Server, NTP • CARS Services > External Repos: FTP, SFTP, TFTP, NFS, HTTP and HTTPS • CARS Services > TCP dump • CARS Services > NNS • Identity Stores > Active Directory • Identity Stores > LDAP(S) • Identity Stores > EntraID • Identity Stores > EntraID Monitor • Communication > RMQ • Communication > between Cisco ISE nodes • Communication > Endpoints DB (node-to-node communication) • APIs > ERS • APIs > Open API

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		• APIs > API Gateway • APIs > MnT REST API • External Services > Posture Feed • External Services > Smart Licensing • TrustSec > SGACL definition • TrustSec > SXP mapping attributes • TrustSec > Policy downloads via HTTP • TrustSec > TrustSec servers via HTTP • TrustSec > CoA via RADIUS • pxGrid > Service • Posture > Posture flow • Posture > Agentless • Observability > Live logs or sessions • Observability > Log analytics, Kibana, and Grafana • Observability > MnT reports • Custom attributes > Internal Users • Custom attributes > Internal Endpoints • Endpoint Profiling > DHCPv6 • Endpoint Profiling > RADIUS attributes • Endpoint Profiling > SNMP probe to endpoint • Endpoint Profiling > SNMP probe to NAD • Telemetry > Telemetry
Ease of use	Cisco ISE license strategy enhancements	License consumption for profiling services, TrustSec, pxGrid, and pxGrid Direct is now accurately tracked per license tier based on feature usage. Consumption for each tier is determined by the number of active endpoints utilizing features associated with that specific tier. However, note that license enforcement for out-of-compliance licenses is not implemented at this time. For licensing questions, email, ise-license-escalation@external.cisco.com.
	Cisco pxGrid Cloud new region support	Cisco pxGrid Cloud is now supported in Europe, Asia Pacific, and Japan, in addition to the U.S.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	Integrate Cisco pxGrid Cloud applications using **Integration Catalog**	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.
	Host header support for OCSP in Cisco ISE	Cisco ISE now supports the Host header field specified in the HTTP 1.1 protocol when required by the Online Certificate Status Protocol (OCSP) servers. This enhancement ensures compatibility with such servers while maintaining HTTP 1.0 as the underlying protocol.
	Assign dedicated resources for Microsoft Active Directory join points	You can reserve resources for the Microsoft Active Directory join points in each PSN. This resource segmentation helps reduce the performance impact caused by resource sharing among the Microsoft Active Directory join points.
	Addition of country code drop-down when resetting the guest password	The password reset process for self-registered guests includes a drop-down list with new country codes. Now, when a self-registered guest selects the **Phone** option to reset their password, the system displays a country code drop-down. The guest user can select an appropriate country code before entering their phone number.
	NTP authentication-key support	The `ntp authentication-key` command in Cisco ISE CLI configuration mode offers support for encryption types, specifically including AES128 and AES256. The command supports both hashed and plaintext key values. For successful NTP synchronization with authentication, the configured key must be added to the trusted list before being associated with an NTP server.
	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.
	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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	Profile network and IoT devices using Simple Network Management Protocol scans	The Simple Network Management Protocol (SNMP) scan classifies IoT and network devices and creates profiling policies. It uses probe data to perform scheduled or on-demand SNMP scans across specific subnets or IP address ranges. It collects detailed OS and hardware information using SNMP. This scan supports Cisco and third-party devices and benefits deployments without asset management systems.
	Selecting the management interface	While running the initial setup program to configure the appliance, you can now select the interface to be configured as the management interface for that appliance. If only one interface is available, Gig0 is set as the default management interface. You can also change the management interface using the `reset-config` command from the Cisco ISE CLI. This option is available in Cisco SNS 3700 and Cisco SNS 3800 series appliances. You can select any Ethernet interface from eth0 to eth5 as the management interface on Cisco SNS 3700 and 3800 series appliances. For example, if you select eth2 as the management interface, it becomes the default interface for all portals. This also allows assigning the management interface to a fiber port on these appliances. This option is not applicable for virtual machines.
	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.
	Probe Status dashboard	The **Probe Status** dashboard in **Operations > System 360 > Log Analytics > Dashboards** displays all the active profiling probes, network access device (NAD) probe status, and endpoint probe details received by Cisco ISE. Use the filters to choose a specific PSN, PSN group, or NAD for more granular results. You can verify whether the NADs are configured properly by analyzing the probes generated for each PSN or NAD. You can analyze the probe packets generated and update the probe and NAD configurations accordingly.
	Time restricted debug enabling	The time-restricted debug enabling feature allows you to select a log level and set a timer to revert to the default settings. The selected node reverts to the default state after the timer expires.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	New TrustSec telemetry attributes	New TrustSec telemetry attributes have been added to enhance the monitoring of your deployment and collect data on how TrustSec and Cisco ISE are used. Some of them are: • Number of created SGACLs • Number of security groups • Number of network devices configured with TrustSec • Number of policies assigning SGTs, number of policies using SGTs, • Other related TrustSec monitoring telemetry attributes, and so on.
	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.
	Cisco ISE integration enhancements	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.
	Export all network devices to repository	While exporting network devices in Cisco ISE, you can choose **Export All to Repository** to export all the network devices to a repository. An email with instructions on how to access the exported data is sent to the registered email address.
	ROPC support for TACACS+	Cisco ISE now supports the TACACS+ workflow for configuring the Resource Owner Password Credentials (ROPC) flow, enabling user authentication with Microsoft Entra ID. This is in addition to the previously supported EAP-TLS and TEAP workflows.
	Support for USGv6 command	You can enable, disable, or check the U.S. Government IPv6 (USGv6) compliance status of a Cisco ISE node with the underlying operating system using the `usgv6` command in EXEC mode.
	Support for osquery condition	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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	OAuth2 authentication support for pxGrid Direct	Cisco pxGrid Direct now supports three authentication methods– Basic, API Key, and OAuth2–when creating a URL Fetcher pxGrid Direct Connector through the Cisco ISE GUI. A URL Fetcher pxGrid Direct Connector uses URLs that you configure for data synchronization. Cisco pxGrid Direct OAuth2 supports both Client Credentials and Password to obtain an access token. The Client Credentials flow uses the client ID and secret, while the Password flow requires both the client credentials and your username and password. When the token expires, a refresh token is used to acquire a new access token.
	Send Change of Authorization after EntraID attribute is changed	Cisco ISE enables you to monitor changes in user or device attributes within your Microsoft Entra ID instance. When predefined rules detect any changes, Cisco ISE triggers reauthentication of the affected endpoint sessions to ensure that updated network access policies are enforced. By configuring authorization policies to monitor specific attributes and using SAML to retrieve them, Cisco ISE can identify attribute changes, issue a Change of Authorization (CoA), and reapply updated access permissions after reauthentication. This process ensures that authorization decisions always reflect the latest attribute information.
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. **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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
Software reliability	API keys and certificate authentication support for Tenable Security Center	From Cisco ISE release 3.5, 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.
	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 details about the live workload sessions. To view this page, in the Cisco ISE GUI, click the Menu icon and choose **Operations > Workloads > Workloads > Workloads Live Session**.
	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.
	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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	Support ACI for global security group	The naming convention for External EPGs (EEPGs) has changed in Cisco ISE release 3.5. In Cisco ISE release 3.4, EEPGs were named using the format: "ISE_SGT_<SGT_TAG>". Here, "ISE_SGT_" is a constant prefix and <SGT_TAG> refers to the Security Group Tag. From Cisco ISE release 3.5, the naming convention changes to "ISE_<SG_NAME>". Now, "ISE_" is the constant prefix, followed by the Security Group (SG) name. There is no automatic migration support for this naming change. Existing EFT customers must disable outbound rules before upgrading to Cisco ISE release 3.5, and reenable them after the upgrade is complete to avoid potential issues.
	Remote TAC support authorization	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, GUI, 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.
	Cloud Multi-Factor Classification Profiler	The Cloud Multi-Factor Classification (MFC) Profiler enhances endpoint classification by sharing observed attributes with the cloud for analysis. It improves endpoint labeling, grouping, and policy application, supporting both standalone and distributed deployments. In comparison to Cisco ISE release 3.4, it provides improved classification labels during cloud onboarding and adds support for both Custom and Direct rules. To enable the Cloud MFC Profiler, go to **Administration > Feed Service > Cloud Multi-Factor Classification Profiler**, select the region, and click **Enable**. You will then be redirected to the Cisco authentication portal and prompted to enter Cisco login credentials.
	Protocols engine for certificate validation	A separate service protocols engine validates certificates in selected scenarios for better efficiency of operations. The protocols engine communicates with the Cisco ISE application server through API calls. A new service called **Protocols Engine** runs when you enter the **show application status ise** command in the CLI.
	Dynamic Reauthorization Scheduler	With Dynamic Reauthorization Scheduler, 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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	Federal and security certification	Federal and security certifications are enhanced in alignment with the Network Device Collaborative Protection Profile (NDcPP) v3.0e for Common Criteria certification, with testing including secure shell (SSH) and authentication server PP-Modules. Additionally, Cisco ISE release 3.5 is planned for: • DoDIN APL certification • FIPS 140-3 compliance review • USGv6 certification and IPv6 ready logo certification in the host category
	DoDIN APL support	Cisco ISE release 3.5 undergoes testing for Department of Defence Approved Products List (DoDIN APL) certification in the Network Access Controller (NAC) category. After Cisco completes testing and receives certification, Cisco posts the certification details on the DoDIN APL website.
	FIPS 140-3 support	Cisco ISE supports FIPS 140-3 mode. This mode enhances cryptographic security and compliance. It enforces FIPS-compliant protocols, algorithms, and key sizes. FIPS mode disables noncompliant cipher suites and protocols in the following components: IPsec, SSHv2, LDAPS, EAP-TLS, EAP-FAST, pxGrid, pxGrid Direct, TC-NAC Tenable, and pxGrid Cloud components.
	Monitor profiler traffic probes	These enhancements improve the resiliency and stability of Cisco ISE profiler: • 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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	Profiling policy enhancements	You can create MFC-based profiling policies in Cisco ISE to categorize unidentified endpoints using rule-based classification. Labels are automatically assigned through custom or direct mapping rules, ensuring a consistent endpoint categorization process: • Custom Rules: Allows you to define profiling criteria for specific organizational needs, providing precise control over classification based on tailored attributes. • Direct Mapping Rules: Allows you to use specific attributes or identifiers (such as, mdmOSVersion or mdmManufacturer) to classify devices directly. Cisco ISE continues to support AI/ML and system rules from previous releases, providing advanced profiling capabilities along with an enhanced user experience and interface.
	SSHD service cryptographic algorithms enhancement	You can use these new algorithms under `service sshd` to manage a service using the Cisco ISE CLI: • MAC-algorithm • Hostkey • Hostkey-algorithm • Key-exchange-algorithm • SSH-client-hostkey-algorithm
	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 **Network Device Profile**. After an upgrade, the check box is not enabled by default, but it is automatically enabled when new resources are added. After the check box is enabled, Cisco ISE invalidates any packet that lacks a **Message-Authenticator** attribute in the response, causing the flow to fail.
	Change of Authorization for dictionary attributes using pxGrid Direct	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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	Support for TACACS+ over TLS 1.3	You can enable TACACS+ over TLS 1.3 authentication on network devices to enhance security. For NAD certificate validation, Cisco ISE supports validation of these SAN attributes: • IP address (iPAddress) • DNS name (dNSName) • directory name (directoryName) If any of these attributes match, validation is successful; otherwise, validation fails. For each SAN attribute, multiple values are supported. You can view the authentication status and configure TACACS+ over TLS 1.3 authentication from the **Network Devices** page.
	TLS 1.3 support for additional Cisco ISE workflows	Cisco ISE release 3.5 supports TLS 1.3 for: • Portals (Self-Registered Guest portal, Sponsor portal, and Hotspot portal) • pxGrid • TACACS+ • Cisco Catalyst Center integration • Cisco Meraki integration • Cisco Duo integration • PEAP workflows • Posture feed service communication
	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.
	Red Hat OpenShift platform support	Cisco ISE release 3.5 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.

© 2026 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>**.
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.

New and changed APIs in Cisco ISE

For detailed information on new, changed, and deprecated APIs, refer to the Cisco ISE API Reference Guide.

Changes in behavior

Cisco ISE release 3.5 patch 4: Changes in behavior

Table 6. Features with changes in behavior in Cisco ISE release 3.5 patch 4

© 2026 Cisco and/or its affiliates. All rights reserved.

Feature	Description
Profiler Licensing Changes	This change reverts profiler licensing behavior to how it worked before Cisco ISE release 3.5. Profiler-related license consumption is now driven through explicit authorization-policy evaluation paths. Licensing for Profiled Endpoint Groups is applied to non-static group assignments, whereas static group assignments do not trigger the Profiled group license requirement. This prevents unexpected Advantage license consumption caused only by profiler-derived endpoint updates while preserving authorization-policy-driven licensing behavior. Refer to CSCwu22569 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 Cisco 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.
OCSP validation for pxGrid client certificates	From Cisco ISE release 3.5 patch 4, 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 3.5 patch 4, 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 3.5 patch 3: Changes in behavior

Table 7. Features with changes in behavior in Cisco ISE release 3.5 patch 3

Feature	Description
EKU support for Cisco pxGrid and IMS	Cisco ISE additionally permits the use of server certificates containing only the Server Authentication Extended Key Usage (EKU) for both Cisco pxGrid and IMS services. Cisco ISE will allow the import or bind of Cisco pxGrid and IMS certificates that contain Server Authentication EKU. In addition, Cisco ISE will continue to accept certificates containing both Server Authentication and Client Authentication EKU. Switching to Server-only EKU certificates after an upgrade may cause compatibility issues if you roll back to an older version of Cisco ISE that requires both EKUs. To avoid this, always back up your original certificates or ensure you can regenerate them from a private CA before making changes.

© 2026 Cisco and/or its affiliates. All rights reserved.

Feature	Description
Updates to Posture Assessment data exports	In Posture Assessment, if you utilize custom scripts to process export files or Data Connect data, review these changes to ensure your automation remains compatible with these updates. • The nomenclature for the agent has been updated. The phrase "Posture Agent" has been replaced with "Cisco Secure Client." For example, "Posture Agent for Windows 5.1.16.194" is now displayed as "Cisco Secure Client for Windows 5.1.16.194." • In scenarios where Periodic Reassessment (PRA) is not enabled for an endpoint, the values in the PRA_INTERVAL and PRA_GRACE_TIME columns have been changed from 0 to N/A. • The nomenclature for POSTURE_AGENT_VERSION column has been updated. The phrase "Posture Agent" has been replaced with "Cisco Secure Client." For example, "Posture Agent for Windows 5.1.16.194" is now displayed as "Cisco Secure Client for Windows 5.1.16.194."
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 for more information.
OCSP validation for pxGrid client certificates	From Cisco ISE release 3.5 patch 4, 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.

Cisco ISE release 3.5 patch 2: Changes in behavior

There are no features with changes in behavior in Cisco ISE release 3.5 patch 2.

Cisco ISE release 3.5 patch 1: Changes in behavior

There are no features with changes in behavior in Cisco ISE release 3.5 patch 1.

Cisco ISE release 3.5: Changes in behavior

Table 8. Features with changes in behavior in Cisco ISE release 3.5

Feature	Description
Cognitive Threat Analytics (CTA) adapter	Cognitive Threat Analytics (CTA) adapter is no longer supported for Threat Centric Network Access Control (TC-NAC) flows.

© 2026 Cisco and/or its affiliates. All rights reserved.

Feature	Description
Endpoint Replication page depreciation	The **Endpoint Replication** page (Administration > System > Settings > Endpoint Replication) is deprecated in the Cisco ISE GUI.
Change to API Gateway cipher support	The API Gateway now uses the latest version of CiscoSSL. As a result, some of the SHA1 ciphers that are not recommended for Cisco ISE are blocked in the API Gateway, even if they remain enabled in the Cisco ISE GUI. This security enhancement enforces stronger encryption standards for API communications.
Certificate requirements for Cisco ISE release 3.5 upgrade	Before upgrading to Cisco ISE release 3.5, replace any SHA1 certificates used for Admin services with certificates that use a secure algorithm like SHA256 or higher, as SHA1 is no longer supported for Admin services under the latest CiscoSSL security requirements. If these certificates are not updated, Admin services may not function properly. While SHA1 certificates can still be imported for other services, they must not be used for Admin services.
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 3.5, 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 3.5.
Cisco ISE password security enhancements	Cisco ISE passwords are secured using strong SHA-512 hashing paired with 128-bit salt.
Enhanced certificate validation and SAN requirement for pxGrid Cloud connectivity	pxGrid Cloud is upgraded to use Go 1.24.x, improving security and ensuring FIPS compliance. As part of this update, TLS certificate validation is enhanced and all certificates used for pxGrid Cloud connectivity must now include a Subject Alternative Name (SAN). Certificates without a SAN will no longer be accepted for secure connections in either FIPS or non-FIPS modes. To avoid Cisco ISE service disruption, update your pxGrid service certificates to include a SAN that matches the Cisco ISE node hostname. To learn how to generate and install certificates, refer to Generate a Self-Signed Certificate.
Authentication and authorization policy evaluation issue with null attributes	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. Refer to CSCwo12680 for more information.

© 2026 Cisco and/or its affiliates. All rights reserved.

Feature	Description
New Cisco ISE configuration options	Cisco ISE release 3.5 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.

Resolved issues

Cisco ISE release 3.5 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 this release.

Cisco ISE release 3.5 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.

Cisco ISE release 3.5 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 3.5 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 3.5: Resolved issues

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

Open issues

Cisco ISE release 3.5 patch 4: Open issues

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

Table 9. Open issues in Cisco ISE release 3.5 cumulative patch 4

Bug ID	Description
CSCww39425	Saving a new Microsoft Entra ID configuration on the OIDC page may fail, and authentication requests for existing configurations may not match the Entra-related rules configured in Cisco ISE. To resolve both issues, enable “Trust for authentication within ISE and Client-Server communication” for the DigiCert Global Root G2 CA on the Trusted Certificates page.
CSCwt34939	Extracting the GUID from the SAN URI causes an incorrect EPID assignment.

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
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.

Cisco ISE release 3.5 patch 3: Open issues

Table 10. Open issues in Cisco ISE release 3.5 cumulative patch 3

Bug ID	Description
CSCwt93615	These columns are currently unavailable in the POSTURE_ASSESSMENT_BY_ENDPOINT Data Connect view: • Report Type • Report SubType • Continuous Reassessment Kept Alive Timer Continuous Reassessment Max Inactivity Timer
CSCwu08645	In the Cisco ISE Posture Assessment by Endpoint report (Operations > Reports > Endpoints and Users > Posture Assessment by Endpoint > Details), the Periodic Reassessment Enforcement attribute incorrectly displays "N/A" instead of "0" when continuous reassessment is enabled.
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.
CSCwt15886	Cisco ISE may report misleading authentication latency spikes in KPM metrics on Policy Administration Nodes (PAN) when Change of Authorization (CoA) requests time out. This occurs because the 15 second wait time for a CoA response is incorrectly logged as request latency, even on nodes without the Policy Service Node (PSN) persona. This behavior can create the false perception of performance degradation. To address this issue, contact Cisco TAC for support.
CSCwt81251	Executing the "no ipv6 enable" command globally on the Primary Policy Administration Node (PPAN) followed by a node reboot results in a failure of deployment replication. This occurs because the firewall configuration incorrectly drops traffic on port 12001 instead of accepting it. To prevent this, refer to the workaround of applying the "no ipv6 enable" command at the interface level. If the issue has already occurred, refer to the recovery steps of re-enabling IPv6 globally on the PAN and rebooting the node to restore replication.

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwu47486	EAP-FAST authentication fails when using a PAC created before upgrading to Cisco ISE release 3.5. This issue also occurs when upgrading from Cisco ISE release 3.5 or any earlier Cisco ISE patch to Cisco ISE release 3.5 patch 3 and is often accompanied by Cisco TrustSec (CTS) environment data download failures. To resolve this issue, install the hotpatch.

Cisco ISE release 3.5 patch 2: Open issues

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

Cisco ISE release 3.5 patch 1: Open issues

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

Table 11. Open issues in Cisco ISE release 3.5 cumulative patch 1

Bug ID	Description
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.
CSCws46345	When you attempt to use the OIDC workflow after rolling back and reinstalling Cisco ISE release 3.5 patch 1 without removing portal references to OIDC, you may notice a 400 Bad Request error during redirection. This happens even though the OIDC configuration and references are still present after the patch processes. To fix the issue, save the relevant portal page after completing the rollback and second patch installation. Once you save the portal page, redirection will work as expected.

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

Cisco ISE release 3.5: Open issues

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

Table 12. Open issues in Cisco ISE release 3.5

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.

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

Known issues

Cisco ISE release 3.5 patch 4: Known issues

There are no known issues in Cisco ISE release 3.5 patch 4.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco ISE release 3.5 patch 3: Known issues

Table 13. Known issues in Cisco ISE release 3.5 patch 3

Feature	Description
IPv6 Support for SXP	From Cisco ISE release 3.5 patch 3, SXP must not be enabled during the node registration process. To ensure successful registration with the Primary PAN, wait until the node reaches the **Synced** state before enabling SXP. Enabling SXP during the registration process is unsupported and may lead to instability of Cisco ISE services.

Cisco ISE release 3.5 patch 2: Known issues

Table 14. Known issues in Cisco ISE release 3.5 patch 2

Bug ID	Description
CSCws61409	Cisco ISE release 3.5 patch 2 affects various reports depending on the upgrade path as follows: • When installed on top of Cisco ISE release 3.5 or Cisco ISE release 3.5 patch 1, then the Change Configuration Audit, Posture-related reports, SXP Binding report, Active Directory Operations report, and Secure System Diagnostics report appear empty. • When upgraded from Cisco ISE release 3.4 patch 4, then the Change Configuration Audit, Posture-related report, SXP Binding report, Active Directory Operations report, and Secure System Diagnostics report appear empty. • When upgraded from Cisco ISE release 3.4 patch 1 through Cisco ISE release 3.4 patch 3, then the **SXP Binding report** and **Secure System Diagnostics report** appear empty. When 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 3.5 patch 1: Known issues

There are no known issues in Cisco ISE release 3.5 patch 1.

Cisco ISE release 3.5: Known issues

Table 15. Known issues in Cisco ISE release 3.5

Bug ID	Description
CSCwq03326	Downgrading from Cisco ISE release 3.5 to Cisco ISE releases 3.3 or 3.4 fails after installing the SNS appliance.
CSCwq49897	When accounting update requests are suppressed, no entries appear in the **Misconfigured NAS** report.
CSCwr86578	Setup and reset-config operations fail when a compressed IPv6 address format (e.g., fd00::103/64) is used; only full expanded IPv6 addresses (e.g., fd00:0:0:0:0:0:0:103/64) are supported. To avoid configuration errors, use the expanded IPv6 address format during both setup and reset-configurations.

© 2026 Cisco and/or its affiliates. All rights reserved.

Compatibility

Upgrading to Cisco ISE release 3.5

You can directly upgrade to Cisco ISE release 3.5 from Cisco ISE releases 3.4, 3.3, and 3.2.

If you are on a release earlier than Cisco ISE release 3.2, you must first upgrade to one of the releases listed above and then upgrade to Cisco ISE release 3.5.

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 ISE Upgrade Guide.

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

Upgrade packages replaced

Cisco ISE release 3.5 upgrade bundle files have been replaced on the Cisco ISE Software Download site.

This entails:

- resolution of bugs CSCwt99926, CSCwt68639, CSCwt71761, CSCwt82378, and CSCws37546.
- that the filenames of the new files will have "a" appended to the build number (for example, ise-upgradebundle-3.2.x-3.4.x-to-3.5.0.527a.SPA.x86_64.tar.gz).
- that existing Cisco ISE release 3.5 cumulative patches will continue to work with this new upgrade bundle.

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 3.5 patch 3 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 3.5 patch 4. 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.

© 2026 Cisco and/or its affiliates. All rights reserved.

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 ISE Upgrade Journey.

For instructions on how to install a patch using the CLI, refer to the " Patch Install" section in the Cisco ISE CLI Reference Guide.

Verified hardware

Cisco ISE release 3.5 can be installed on these Cisco 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)
- Cisco SNS-3855-K9 (medium)
- Cisco SNS-3895-K9 (large)

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 ISE Installation Guide for your version of Cisco ISE.

Table 16. 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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Virtual environment	Support details
VMware Cloud Solutions on public cloud platforms	• AWS: Host Cisco ISE on a software-defined data center provided by VMware Cloud on AWS. • Azure VMware Solution: Runs VMware workloads natively on Microsoft Azure. • Google Cloud VMware Engine: Runs software-defined data center by VMware on Google Cloud.
Microsoft Hyper-V	• Supports Microsoft Windows Server 2012 R2 and later. • Supports Azure Stack HCI 23H2 and later. The virtual machine requirements and the installation procedure for the Cisco ISE VMs in the Azure Stack HCI are the same as that of Microsoft Hyper-V.
KVM on QEM	• Supports QEMU 2.12.0-99 and later. • Cisco ISE release 3.4 patch 4 and later releases support OpenStack.
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 3.5 is supported and verified on these browsers:

- Mozilla Firefox versions 136, 138, 139, 140, and later.
- Google Chrome versions 134, 135, 137, and later.
- Microsoft Edge versions 134, 135, and later.

Verified external identity sources

Table 17. Verified external identity sources

External identity source	Details	Version
Active Directory	Microsoft Windows Active Directory 2012	Windows Server 2012

© 2026 Cisco and/or its affiliates. All rights reserved.

External identity source	Details	Version
	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
	Microsoft Windows Active Directory 2025 **Note**: Currently, Cisco ISE integration with Microsoft Windows Active Directory 2025 requires configuration changes in the Active Directory Domain Controller. For more information, refer to CSCwn62873.	Windows Server 2025
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	Microsoft SQL server	Microsoft SQL servers 2012 and 2022
	Oracle	Enterprise Edition Release 12.1.0.2.0

© 2026 Cisco and/or its affiliates. All rights reserved.

External identity source	Details	Version
(ODBC) identity source	PostgreSQL	9.0
	Sybase	16.0
	MySQL	6.3
OpenID Connect for self-registered guest portals	Microsoft Entra ID, Okta or a generic OIDC Identity provider	-
Social Login (for Guest User Accounts)	Facebook	Latest

Verified antivirus and antimalware products

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

Verified OpenSSL version

Cisco ISE release 3.5 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. 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.