Release Notes for Cisco Identity Services Engine, Release 3.5

Contents

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
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 new features

Table 2. New features for 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.
Ease of setup	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.

Product impact	Feature	Description
	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 • APIs > API Gateway

Product impact	Feature	Description
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.
	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 reduces the frequency of lockouts resulting from multiple incorrect password attempts. This option is supported for both RADIUS and TACACS+ protocols. Cisco ISE interacts with Active Directory through these protocols to manage authentication requests and limit excessive failed attempts, thereby preventing lockouts.

Product impact	Feature	Description
	User and device authorization using Entra ID EAP-TLS and TEAP-TLS	Cisco ISE now 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. In the authorization policy, a REST ID Store Attribute condition or REST ID Store Group is configured. During authorization, Cisco ISE queries Microsoft Entra ID to retrieve groups and attributes of the user or device, and device-related information. This data is used by Cisco ISE to make informed authorization decisions.
	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 `application reset-config ise` command from the Cisco ISE CLI. This option is available in Cisco SNS 3700 and Cisco SNS 3800 series 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 alarms help you identify and address issues such as delays in accessing external systems or excessive traffic communication from TACACS+ devices: • High ping or communication latency between Cisco ISE nodes • Slow Active Directory connection detected • Slow LDAP connection detected • Slow ODBC connection detected • Excessive TACACS communication detected
	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.

Product impact	Feature	Description
	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.
	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.

Product impact	Feature	Description
	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.
	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.

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.

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.

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.

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.

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
	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.

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> ◦ <ID><GUID>,<tag,sid> • SID and ID or GUID separated by a colon (in either order): ◦ <tag,sid>:<ID><GUID> ◦ <ID><GUID>:<tag,sid> • Only SID present: ◦ <tag,sid> • Only ID and GUID present: ◦ <ID><GUID> All newer Microsoft certificates include the SID in the SAN_URI with the format: **tag:microsoft.com,2022-09-14:sid:<SID>**.
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, see the Cisco ISE API Reference Guide.

Changes in behavior

Cisco ISE release 3.5: Changes in behavior

Table 3. 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.
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.

Resolved issues

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: Open issues

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

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

Known issues

Cisco ISE release 3.5: Known issues

Table 4. Known issues for 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.

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, see the Cisco ISE Upgrade Guide.

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

Cisco ISE on cloud

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

Install a new patch

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

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

Supported hardware

Cisco ISE release 3.5 can be installed on these Cisco Secure Network Server (SNS) hardware platforms. For appliance hardware specifications, see the Cisco Secure Network Server Appliance Hardware Installation Guide.

- Cisco SNS-3615-K9 (small)
- Cisco SNS-3655-K9 (medium)
- Cisco SNS-3695-K9 (large)
- Cisco SNS-3715-K9 (small)
- Cisco SNS-3755-K9 (medium)
- Cisco SNS-3795-K9 (large)
- Cisco SNS-3815-K9 (small)
- Cisco SNS-3855-K9 (medium)
- Cisco SNS-3895-K9 (large)

Supported virtual environments

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

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

Table 5. Supported virtual environments

Virtual environment	Support details
VMware	• VMware 7.0.3 or later. • In the case of vTPM devices, you must upgrade to VMware ESXi 7.0.3 or later releases. • OVA templates support VMware version 14 or later on ESXi 7.0 and ESXi 8.0. • ISO files support ESXi 7.0 and ESXi 8.0. • You can use the VMware migration feature to migrate VM instances (running any persona) between hosts. Cisco ISE supports both hot and cold migration. Hot migration is also called live migration or **vMotion**. Cisco ISE need not be shut down or powered off during the hot migration. You can migrate the Cisco ISE VM without any interruption in its availability.
VMware Cloud Solutions on public cloud platforms	• AWS: Host Cisco ISE on a software-defined data center provided by VMware Cloud on AWS. • Azure VMware Solution: Runs VMware workloads natively on Microsoft Azure. • Google Cloud VMware Engine: Runs software-defined data center by VMware on Google Cloud.
Microsoft Hyper-V	• Supports Microsoft Windows Server 2012 R2 and later. • Supports Azure Stack HCI 23H2 and later. The virtual machine requirements and the installation procedure for the Cisco ISE VMs in the Azure Stack HCI are the same as that of Microsoft Hyper-V.
KVM on QEM	• Supports QEMU 2.12.0-99 and later. • Cisco ISE cannot be installed on OpenStack.
Nutanix	• Supports Nutanix 20230302.100169 and later.
Public cloud platforms	• Native support for Amazon Web Services (AWS), Microsoft Azure Cloud, and Oracle Cloud Infrastructure (OCI).
Red Hat OpenShift	• Red Hat OpenShift container platform 4.19 and later. • Cisco ISE must be deployed on OpenShift platform using the standard Cisco ISE ISO image. Deploying Cisco ISE using OVA templates is not supported.

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 validated on these browsers:

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

Validated external identity sources

Table 6. Validated external identity sources

External identity source	Details	Version
Active Directory	Microsoft Windows Active Directory 2012	Windows Server 2012
	Microsoft Windows Active Directory 2012 R2	Windows Server 2012 R2 **Note**: Cisco ISE supports all the legacy features in Microsoft Windows Active Directory 2012 R2. However, the new features in Microsoft Windows Active Directory 2012 R2, such as Protected User Groups, are not supported.
	Microsoft Windows Active Directory 2016	Windows Server 2016
	Microsoft Windows Active Directory 2019	Windows Server 2019
	Microsoft Windows Active Directory 2022	Windows Server 2022 with patch Windows10.0-KB5025230-x64-V1.006.msu
	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, see 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

External identity source	Details	Version
	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

Supported antivirus and antimalware products

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

Validated OpenSSL version

Cisco ISE release 3.5 is validated with CiscoSSL 3.x based on OpenSSL 3.x.

Related resources

See our collection pages for additional resources that you can use when working with Cisco ISE.

Legal information