Release Notes for Cisco Identity Services Engine, Release 3.5

Contents

Cisco ISE, Release 3.5

Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. An administrator can then use this information to make proactive governance decisions by creating access control policies for the various network elements, including access switches, wireless controllers, Virtual Private Network (VPN) gateways, Private 5G networks, and data center switches. Cisco ISE acts as the policy manager in the Cisco Group Based Policy solution and supports TrustSec software-defined segmentation.

Cisco ISE is available on Cisco Secure Network Server appliances with different performance characterizations, virtual machines (VMs), and on public clouds.

Cisco ISE has a scalable architecture with centralized management and control. It supports both standalone with high availability and distributed deployment. It also enables the configuration and management of distinct personas and services, thereby giving you the ability to create and apply services where needed in a network but operate the Cisco ISE deployment as a complete and coordinated system.

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

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

This document describes the features, issues, and limitations for Cisco ISE.

Table 1. New and changed information

Date	Description
June 18, 2025	Beta release of Cisco ISE Release 3.5.

New software features

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

New features for Cisco ISE, release 3.5

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. For more information, see the Cisco pxGrid API Guide.
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 newly introduced **ipv6 default-gateway** command allows you to specify a default gateway using an IPv6 address. For more information, see the topic "Run the Setup Program of Cisco ISE" in the chapter "Install Cisco ISE" in the *Cisco ISE Installation Guide, Release 3.5*.

Product impact	Feature	Description
Ease of setup	Enable protocols engine	A separate service protocols engine validates certificates in selected scenarios for better efficiency of operations. Protocols Engine communicates with Cisco ISE application server through API calls. To enable or disable this option, use the Enable/Disable Protocols Engine option (option 40) in the **application configure ise** command. For more information, see the topic " Enable Protocols Engine" in the chapter " Cisco ISE CLI Commands in EXEC Mode" in the *Cisco ISE CLI Reference Guide, Release 3.5.*

Product impact	Feature	Description
Ease of setup	Support for IPv6	If you choose to run Cisco ISE in IPv6 mode, these features are supported: • Portals > Admin Portals • Portals > Certificate Provisioning • Portals > Guest (Self-registered, Sponsor, and Sponsored Guest) • Portals > MDM • Portals > Posture – Client Provisioning • ISE Cloud Deployment > AWS, OCI and Azure • RADIUS > Authentication, Accounting Authorization, Attributes, Audit/Debug logs, Proxy, CoA, and Policy • RADIUS > OSCP • RADIUS > Secure Syslog Targets • RADIUS > DACL download • CARS Services > SSH, NTP • CARS Services > External Repos: FTP, SFTP, TFTP, NFS, HTTP and HTTPS • CARS Services > TCP dump, DNS • CARS Services > IPSec • Identity Stores > Active Directory • Identity Stores > LDAP(S) • Identity Stores > EntraID • Communication > RMQ • Communication > between ISE nodes • Communication > Endpoints DB (node-to-node communication) • Communication > ProtocolsEngine • APIs > ERS • APIs > Open API • APIs > API Gateway • APIs > MnT REST API • External Services > Posture Feed • External Services > Smart Licensing • TrustSec > SGACL definition • TrustSec > Policy downloads via HTTP

Product impact	Feature	Description
Ease of use	Cisco pxGrid Cloud new region support	Cisco pxGrid Cloud is now supported in Europe, Asia Pacific and Japan in addition to the U.S. For more information, see the pxGrid Cloud Solution Guide and the pxGrid Cloud Onboarding Guide.
Ease of use	Integrate Cisco pxGrid Cloud applications using **Integration Catalog**	From Cisco ISE Release 3.4 Patch 1, you can use a native integration catalog interface in Cisco ISE to integrate with Cisco pxGrid Cloud applications for a simplified integration experience. Cisco pxGrid Cloud apps can be integrated with Cisco ISE using the **Integration Catalog** (**Administration** > **System** > **Deployment** > **Integration Catalog**). You can integrate both single-instance and multi-instance Cisco pxGrid Cloud apps. For more information, see the Cisco pxGrid Cloud Solution Guide
Ease of use	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 OCSP servers. This enhancement ensures compatibility with such servers while maintaining HTTP 1.0 as the underlying protocol. For more information, see the topic "OCSP and CRL service ports" in the chapter Cisco ISE ports reference in the Cisco Identity Services Installation Guide, release 3.5.
Ease of use	Assign dedicated resources for join points	You can reserve resources for the join points in each PSN. This resource segmentation will help reduce the performance impact caused by resource sharing among the join points. For more information, see the topic "Assign dedicated resources for join points" in the Chapter "Asset Visibility" in the Cisco ISE Administrator Guide, Release 3.5.
Ease of use	Addition of country code dropdown when resetting the guest password	From Cisco ISE release 3.5, the password reset process for self-registered guests includes a new country code drop-down list. 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. For more information, see the topic "Login Page Settings for Credentialed Guest Portals" in the chapter " Guest and Secure WiFi" in the Cisco ISE Administrator Guide, Release 3.5.
Ease of use	Common criteria NTP upgrade	From Cisco ISE release 3.5, 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. For more information, see the topic "ntp authentication-key" in the chapter "Cisco ISE CLI Commands in Configuration Mode" in the Cisco ISE CLI guide, Release 3.5.

Product impact	Feature	Description
Ease of use	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. For more information, see the topic "Configure Maximum Passwords Attempts for Active Directory Account" in the Chapter "Asset Visibility" in the *Cisco ISE Administrator Guide, Release 3.5.*
Ease of use	User and device authorization using Entra ID EAP-TLS and TEAP-TLS	This feature enables Cisco ISE administrators to configure the system to authorize users, devices, or both through EAP or TEAP chaining. During authentication, Cisco ISE evaluates the certificate presented by the user or device to authenticate them, 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. For more information, see the topic "EAP-TLS and TEAP Authentication with Microsoft Entra ID" in the chapter "Asset Visibility" in the *Cisco ISE Administrator Guide, Release 3.5*.
Ease of use	Profile infrastructure devices using Simple Network Management Protocol	The Simple Network Management Protocol (SNMP) scan classifies network endpoints 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 is supported for both Cisco and third-party devices and benefits deployments that do not have asset management systems. For more information, see the topic "SNMP Scans" in the chapter "Asset Visibility" in the *Cisco ISE Administrator Guide, Release 3.5.*
Ease of use	Selecting the management interface	From Cisco ISE Release 3.5, you can select the management interface while running the initial setup program from the CLI. This option is available in Cisco SNS 3700 series appliances and Cisco SNS 3800 series appliances. This option is not applicable for virtual machines. 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, Gig-0 is set as the default management interface. For more information, see the topic "Run the Setup Program of Cisco ISE" in the "Install Cisco ISE" chapter in the *Cisco ISE Installation Guide, Release 3.5*.

Product impact	Feature	Description
Ease of use	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 external systems or excessive communication traffic from TACACS+ devices: • High ping latency between ISE nodes • Slow Active Directory detected • Slow LDAP connection detected • Slow ODBC connection detected • Excessive TACACS communication detected For more information, see the topic "Cisco ISE Alarms" in the chapter "Troubleshooting" in the *Cisco ISE Administrator Guide, Release 3.5*.
Ease of use	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. For more information, see the topic "Log Analytics" in the Chapter "Maintain and Monitor" in the *Cisco ISE Administrator Guide, Release 3.5*.
Ease of use	Time restricted debug enabling	The time restricted debug enabling feature allows you to select a log level and set a reset timer to revert to default settings. The selected node reverts to the default state after the timer expires. For more information, see the topic "Configure debug log settings" in chapter "Troubleshooting" in *Cisco ISE Administrator Guide, Release 3.5.*
Ease of use	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. For more information, see the topic "Information that telemetry gathers" in chapter "Troubleshooting" in *Cisco ISE Administrator Guide, Release 3.5.*
Ease of use	Changes in Cisco ISE licensing strategy	From Cisco ISE release 3.5, some features of the Cisco ISE Advantage licensing such as pxGrid, pxGrid Direct, Profiling services, and TrustSec will consume licenses according to the number of active endpoints using each feature. However, note that license enforcement for out-of-compliance licenses is not implemented at this time. For more information, see the Cisco ISE Licensing collection page and the topic "Tier Licenses" in the chapter "Licensing" in *Cisco ISE Administrator Guide, Release 3.5.*

Product impact	Feature	Description
Ease of use	Use enhanced Endpoint Topics Settings to share Cisco ISE data	You can enhance network visibility and security by sharing endpoint attribute data with Cisco AI Endpoint Analytics and Cisco pxGrid Cloud using the enhanced Endpoint Topics Settings feature. You can use the Enable Endpoint Attributes to Topics option to forward endpoint attributes from Cisco ISE to analytic platforms through integration. You can also publish AI Endpoint Analytics profile data to Cisco ISE for network access authorization and endpoint control by using the Consume Endpoint Profiles from AI Endpoint Analytics option. For more information, see the topic "Create Authorization Policies with Endpoint-Analytics Attributes" in the "Segmentation" chapter in the *Cisco ISE Administrator Guide, Release 3.5.*
Ease of use	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 remote repository. An email with instructions on how to access the exported data is sent to the registered email address. For more information, see the topic "Export Network Devices from Cisco ISE" in the Chapter "Secure Access" in the *Cisco ISE Administrator Guide, Release 3.5.*
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 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) 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 appliance can be configured with one hard disk or four hard disks. It is recommended to enable only the PSN or pxGrid persona if your Cisco SNS 3855 appliance is configured with only one hard disk. For more information, see the *Cisco Secure Network Server 3800 Series Appliance Hardware Installation Guide*.

Product impact	Feature	Description
Software reliability	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. For more information, see the topic "Create a URL Fetcher Connector Type" in the "Asset Visibility" chapter in the *Cisco ISE Administrator Guide, Release 3.5*.
Software reliability	Remote 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, UI or both to troubleshoot and gather information. This access must be explicitly authorized by the Cisco ISE administrator and can be provided for one or more nodes within the Cisco ISE deployment. For more information, see the topic "Remote Support Authorization" in the chapter "Troubleshooting" in the *Cisco ISE Administrator Guide, Release 3.5*.
Software reliability	Cloud Multi-Factor Classification Profiler	The Cloud Multi-Factor Classification (MFC) Profiler in Cisco ISE 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. To register the Cisco ISE instance on the cloud, go to Administration > FeedService > 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. For more information, see the topic "Cloud Multi-Factor Classification Profiler" in the chapter "Asset Visibility" in the *Cisco ISE Administrator Guide, Release 3.5*.
Software reliability	Federal or security certification	Cisco ISE Release 3.5 enhances its support for key federal and security certifications. This release aligns 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. For more information, see the topic "Federal or security certification" in the chapter "Basic Setup" in the *Cisco ISE Administrator Guide, Release 3.5*.

Product impact	Feature	Description
Software reliability	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. For more information, see the topic "Federal or security certification" in the chapter "Basic Setup" in the Cisco ISE Administrator Guide, Release 3.5.
Software reliability	FIPS 140-3 support	Cisco ISE now supports FIPS 140-3 mode. This mode enhances cryptographic security and compliance. It enforces FIPS-compliant protocols, algorithms, and key sizes. FIPS mode disables non-compliant cipher suites and protocols, including EAP-TLS, PEAP, SSHv2, LDAPS, pxGrid, EAP-MD5, PAP, CHAP, MS-CHAPv1/v2, and LEAP. For more information, see the topic "Federal Information Processing Standards Mode Support" in the chapter "Basic Setup" in the Cisco ISE Administrator Guide, Release 3.5.
Software reliability	Monitor profiler traffic probes	These enhancements are introduced to 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. For more information, see the topic "Monitor profiler traffic probes" in the chapter "Asset Visibility" in the *Cisco ISE Administrator Guide, Release 3.5*.
Software reliability	New profiling service for improved efficacy	You can create Multi-Factor Classification (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: Allow you to define profiling criteria specific to specific organizational needs, providing precise control over classification based on tailored attributes. • Direct Mapping Rules: Allow you to use specific attributes or identifiers (e.g., mdmOSVersion or mdmManufacturer) to classify devices directly. Additionally, Cisco ISE continues to support AI/ML and system rules from earlier releases for enhanced profiling capabilities. For more information, see the topic "Profiling policies" in the chapter "Asset Visibility" in the *Cisco ISE Administrator Guide, Release 3.5.*

Product impact	Feature	Description
Software reliability	Send Change of Authorization after EntraID attribute is changed	Cisco ISE allows you to monitor changes in user or device attributes within your Microsoft Entra ID instance and dynamically enforce updated network access policies. By defining authorization policies with monitored attributes and using SAML to fetch them, Cisco ISE can detect attribute changes, trigger a Change of Authorization (CoA), and reapply updated access permissions after reauthentication. This ensures alignment between authorization decisions and the latest attribute changes. For more information, see the topic "Change of authorization based on Microsoft Entra ID attribute updates" in the chapter "Asset Visibility" in the *Cisco ISE Administrator Guide, Release 3.5*.
Software reliability	SSHD service cryptographic algorithms enhancement	From Cisco ISE release 3.5, you can use the new algorithms under **service sshd** to manage a service using the Cisco ISE CLI. The following algorithms are newly added. • MAC-algorithm • Hostkey • Hostkey-algorithm • Key-exchange-algorithm • SSH-client-hostkey-algorithm For more information, see the topic "service sshd" in the chapter "Cisco ISE CLI Commands in Configuration Mode" in the *Cisco ISE CLI Reference Guide, Release 3.5*.
Software reliability	Blast RADIUS vulnerability fix	To address the Blast RADIUS vulnerability reported in CSCwk67747, the **Message Authenticator Required On Response** check box has been introduced in **External RADIUS Server**, **RADIUS Token ID Store**, and **Device Profile**. This checkbox is not enabled by default after upgrade. Once the checkbox is enabled, Cisco ISE will invalidate any packet that lacks a **Message-Authenticator** attribute in the response, causing the flow to fail. For more information, see the topics "Network Device Profiles Settings" and "External RADIUS Server Settings" in the chapter "Threat Containment" and the topic "Add a RADIUS Token Server" in the chapter Asset Visibility in *Cisco ISE Administrator Guide, Release 3.5.*
Software reliability	Change of Authorization for dictionary attributes using pxGrid Direct	From Cisco ISE release 3.5, 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. For more information, see the topic "Change of Authorization (CoA) for dictionary attributes using pxGrid Direct" in the chapter "Asset Visibility" chapter in the *Cisco ISE Administrator Guide, Release 3.5.*

Product impact	Feature	Description
Software reliability	Support for TACACS over TLS	You can enable TACACS over TLS authentication for the network devices to enforce additional security. Cisco ISE supports validating the IP address (iPAddress), DNS name (dNSName), and directory name (directoryname) attributes of the certificate. If any of these attributes match, validation is successful, otherwise, validation fails. For each SAN attribute, multiple values are supported. You can view whether TACACS or TACACS over TLS authentication is enabled for a network device in the **Network Devices** page. For more information, see the topic "Network Device Definition Settings" in the Chapter "Secure Access" in *Cisco ISE Administrator Guide, Release 3.5*.
Software reliability	TLS 1.3 support for additional Cisco ISE workflows	Cisco ISE release 3.5 allows TLS 1.3 for administrator HTTPS access over port 443 for: • Portals (Self-Registered Guest portal, Sponsor portal, and Hotspot portal) • pxGrid • TACACS When the Allow TLS 1.3 option is enabled, TLS 1.3 is used for Cisco Catalyst Center integration, Cisco Meraki integration, Cisco Duo integration, and posture feed service communication. For more information, see the topic "Configure Security Settings" in the Chapter "Segmentation" in the *Cisco ISE Administrator Guide, Release 3.5*.
Software reliability	Security Identifiers in certificates will not be used for authentication	From Cisco ISE release 3.5, Cisco ISE supports a new format of certificates with Security Identifiers (SID). The SIDs present in the Subject Alternative Name (SAN) fields will not be used for authentication in Cisco ISE. This enhancement prevents authentication failures caused due to incorrect SID parsing in the authentication process.

New and changed APIs in Cisco ISE

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

Change in behavior

Change in behavior for Cisco ISE, release 3.5

Table 3. Deprecated features for Cisco ISE release 3.5

Feature	Description
Cognitive Threat Analytics (CTA) adapter	From Cisco ISE release 3.5, the Cognitive Threat Analytics (CTA) adapter is no longer supported for Threat Centric Network Access Control (TC-NAC) flows.

Resolved issues

This section lists the resolved issues that apply to the current release and might apply to releases earlier than Cisco ISE 3.5. To see additional information about the issues, click the bug ID to access the Bug Search Tool (BST).

Resolved issues for Cisco ISE, release 3.5

Table 4. Resolved issues for Cisco ISE, release 3.5

Bug ID	Description
CSCwo43799	The new SNMP scan feature in Cisco ISE release 3.5 is not functioning as expected on IPv6-only Cisco ISE setups.
CSCwo57332	Smart licensing registration using HTTPS proxy fails on IPv6 setups with an IPv6 proxy due to the proxy configuration page not accepting square brackets, which are necessary for IPv6 environments.
CSCwo55285	Live logs do not appear in Cisco ISE for authenticated users despite successful authentication from NAD to Cisco ISE when IPv6 auto configuration is enabled on the interface.
CSCwo02712	In the **Probe Status** dashboard, the NAD counts are inaccurate.
CSCwo63322	The **Probe Status** dashboard fails to display radius probe data when the PSN filter is applied, despite the expectation that this data should be visible.
CSCwo78312	The full upgrade option on the Cisco ISE GUI is not working as expected when performing a full upgrade from Cisco ISE release 3.4 patch 1 to Cisco ISE release 3.5.
CSCwo76053	The HEAD method fails when performing API key authorisation for ServiceNow.
CSCwn54074	After reverting to the Cisco ISE release 3.4 patch 1 upgrade setup, the legacy patch page fails to load.
CSCwn62873	Persistent issue with Cisco ISE integration with Active Directory on Windows Server 2025.

Open issues

This section lists the open issues that apply to the current release and might apply to releases earlier than Cisco ISE 3.5. An issue that is open for an earlier release and is still unresolved applies to all future releases until it is resolved

Open issues for Cisco ISE, release 3.5

Table 5. Open issues for Cisco ISE, release 3.5

Bug ID	Description
CSCwp35088	There's a mismatch of licensing details between Live Logs Details and Live Sessions pages. Licensing information in the Live Logs Details page is incorrect.
CSCwo63322	Unable to view RADIUS probe data when data is filtered for the PSN on the Probe status dashboard.
CSCwo58442	SXP service engine is stuck in the initialisation state following a database restore operation in Cisco ISE release 3.5.

Bug ID	Description
CSCwp22660	A GuestFullAccess issue is seen in endpoint sessions after SAML-based login for guest users..
CSCwp10096	When using a single-stack configuration, an admin user cannot add a REST ID store to the deployment.
CSCwp60188	After a PAN failover, the deployment status indicates that the nodes in the deployment are not synchronized.
CSCwp33820	An upgrade failure was encountered when upgrading from Cisco ISE release 3.3 patch 3 to Cisco ISE release 3.5.
CSCwp63354	Certificate-based authentication flow using Active Directory CA server does not work as expected.
CSCwp66253	In Cisco IS release 3.5, the authorization policy for AzureEntraID user attribute with the matching condition works as expected only when using the SAML flow.

Known issues

Known issues in Cisco ISE, release 3.5

Table 6. Known issues for Cisco ISE release 3.5

Feature	Known issue
Downgrade from Cisco ISE release 3.5 to Cisco ISE release 3.3	Downgrading from Cisco ISE 3.5 to Cisco ISE releases 3.3 or 3.4 fails after installing the SNS application.

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

The 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 7. 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. • From Cisco ISE Release 3.1, you can use the VMware migration feature to migrate virtual machine (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	• Amazon Web Services (AWS): Host Cisco ISE on a software-defined data center provided by VMware Cloud on AWS. • Azure VMware Solution: Runs VMware workloads natively on Microsoft Azure. • Google Cloud VMware Engine: Runs software-defined data center by VMware on Google Cloud.
Microsoft Hyper-V	• Supports Microsoft Windows Server 2012 R2 and later. • Supports Azure Stack HCI 23H2 and later versions. The virtual machine requirements and the installation procedure for the Cisco ISE VMs in the Azure Stack HCI are the same as that of Microsoft Hyper-V.

Virtual environment	Support details
KVM on QEM	• Supports QEMU 2.12.0-99 and later. • Cisco ISE cannot be installed on OpenStack.
Nutanix	• Supports Nutanix 20230302.100169.
Public cloud platforms	• Native support for Amazon Web Services (AWS), Microsoft Azure Cloud, and Oracle Cloud Infrastructure (OCI).

Browser compatibility

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

Cisco ISE release 3.5 is validated on:

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

Validated external identity sources

Table 8. 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

External identity source	Details	Version
LDAP servers	SunONE LDAP Directory server	Version 5.2
	OpenLDAP Directory server	Version 2.4.23
	Any LDAP v3-compliant server	Any version that is LDAP v3 compliant
	AD as LDAP	Windows Server 2022 with patch Windows10.0-KB5025230-x64-V1.006.msu
Token servers	RSA ACE/server	6.x series
	RSA authentication manager	7.x and 8.x series
	Any RADIUS RFC 2865-compliant token server	Any version that is RFC 2865 compliant
Security Assertion Markup Language (SAML) Single Sign-On (SSO)	Microsoft Azure MFA	Latest
	Oracle Access Manager (OAM)	Version 11.1.2.2.0
	Oracle Identity Federation (OIF)	Version 11.1.1.2.0
	PingFederate server	Version 6.10.0.4
	PingOne Cloud	Latest
	Secure Auth	8.1.1
	Any SAMLv2-compliant identity provider	Any SAMLv2 compliant identity provider version
Open Database Connectivity (ODBC) identity source	Microsoft SQL server	Microsoft SQL servers 2012 and 2022
	Oracle	Enterprise Edition Release 12.1.0.2.0
	PostgreSQL	9.0
	Sybase	16.0
	MySQL	6.3
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 7.3.410 based on OpenSSL 1.1.1za.

Related documentation

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

Legal information