

Cisco Identity Services Engine Network Component Compatibility, Release 3.2

Understanding Cisco ISE interoperability 2

Supported network access devices 2

System requirements 5

Verified client machine operating systems, supplicants, and agents 15

Verified operating systems and browsers for Sponsor, Guest, and My Devices portals 22

Verified devices for BYOD onboarding and certificate provisioning 22

Verified security product integrations over Cisco pxGrid 24

Verified Cisco Catalyst Center release 28

Verified Cisco Prime Infrastructure release 28

Verified Cisco Firepower Management Center release 28

Verified Cisco Secure Network Analytics release 28

Verified Cisco WAN Service Administrator release 28

Verified support for Threat Centric NAC 28

Revised: August 5, 2026

Understanding Cisco ISE interoperability

Cisco ISE supports protocol standards like RADIUS, its associated RFC Standards, and TACACS+. For more information, refer to the ISE Community Resources.

Cisco ISE supports interoperability with any Cisco or non-Cisco RADIUS client network access device (NAD) that implements common RADIUS behavior for standards-based authentication.

Cisco ISE interoperates fully with third-party TACACS+ client devices that adhere to the governing protocols. Support for TACACS+ functions depends on the device-specific implementation.

Supported network access devices

RADIUS

Cisco ISE interoperates fully with third-party RADIUS devices that adhere to the standard protocols. Support for RADIUS functions depends on the device-specific implementation.

Certain advanced use cases, such as those that involve posture assessment, profiling, and web authentication, are not consistently available with non-Cisco devices or may provide limited functionality. We recommend that you validate all network devices and their software for hardware capabilities or bugs in a particular software release.

If the network device does not support both dynamic and static URL redirects, Cisco ISE provides an Auth VLAN configuration by which URL redirect is simulated. For more information, refer to the "Third-Party Network Device Support in Cisco ISE" section in chapter "Secure Wired Access" in the Cisco Identity Services Engine Administrator Guide.

TACACS+

Cisco ISE interoperates fully with third-party TACACS+ client devices that adhere to the governing protocols. Support for TACACS+ functions depends on the device-specific implementation.

For information on enabling specific functions of Cisco ISE on network switches, refer to the “Switch and Wireless LAN Controller Configuration Required to Support Cisco ISE Functions” chapter in Cisco Identity Services Engine Administrator Guide.

ISE Community Resource

Does ISE Support My Network Access Device?

For information about third-party NAD profiles, refer to ISE Third-Party NAD Profiles and Configs.

For information on how to configure TACACS+ for Nexus devices, refer to Cisco ISE Device Administration Prescriptive Deployment Guide.

Wireless LAN controllers

For Wireless LAN controllers, MAC authentication bypass (MAB) supports MAC filtering with RADIUS lookup. There is also additional support for session ID and COA with MAC filtering provides MAB-like functionality.

DNS-based ACL feature is supported for WLC 8.0 and above. Not all Access Points support DNS-based ACL. Refer to the *Cisco Access Points Release Notes* for more details.

Restriction

- Some switch models and IOS versions may have reached the end-of-life date and interoperability may not be supported by Cisco TAC.
- You must use the latest version of NetFlow for the Cisco ISE profiling service. If you use NetFlow Version 5, you can use it only on the primary NAD at the access layer.

Cisco verified device support

For information about the devices that are verified and supported with Cisco ISE, refer to Network Device Capabilities Validated with Cisco Identity Services Engine.

Verified protocol standards, RFCs, and IETF drafts

Cisco ISE conforms to these protocol standards, Requests for Comments (RFCs), and IETF drafts:

Verified IEEE standards

- IEEE802.1X-Std-2001
- IEEE802.1X-Std-2004

Verified IETF RFC

- RFC2138 - RADIUS
- RFC2246 - TLSv1.0
- RFC2548 - Microsoft Vendor-specific RADIUS Attributes
- RFC2759 - Microsoft PPP CHAP Extensions, Version 2
- RFC2865 - RADIUS
- RFC2866 - RADIUS Accounting
- RFC2867 - RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC2868 - RADIUS Attributes for Tunnel Protocol Support
- RFC2869 - RADIUS Extensions
- RFC3579 - RADIUS Support For EAP
- RFC3580 - IEEE 802.1X RADIUS Usage Guidelines
- RFC3748 - EAP
- RFC4017 - EAP Method Requirements for Wireless LANs
- RFC4851 - EAP-FAST
- RFC5176 - Dynamic Authorization Extensions to RADIUS
- RFC5216 - EAP-TLS Authentication Protocol

- RFC5281 - Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)
- RFC5422 - Dynamic Provisioning Using Flexible Authentication via Secure Tunneling Extensible Authentication Protocol (EAP-FAST)
- RFC5425 - Transport Layer Security (TLS) Transport Mapping for Syslog
- RFC6587 - Transmission of Syslog Messages over TCP
- RFC7360 - Datagram Transport Layer Security (DTLS) as a Transport Layer for RADIUS

Partially-supported RFC

These RFCs are partially supported:

- RFC2548 - Microsoft Vendor-specific RADIUS Attributes
- RFC2882 - Network Access Servers Requirements: Extended RADIUS Practices
- RFC7030 - Enrollment over Secure Transport (EST) (Verified and supported as part of BYOD flow)
- RFC7170 - Tunnel Extensible Authentication Protocol (TEAP) Version 1

Verified IETF drafts

- IETF Draft - PEAP Version 0
- IETF Draft - PEAP Version 1
- IETF Draft - PEAP Version 2
- IETF Draft - Microsoft EAP CHAP Extensions Version 2

AAA attributes used in Cisco ISE services

AAA attributes for RADIUS proxy service

For RADIUS proxy service, these AAA attributes must be included in the RADIUS communication:

- Calling-Station-ID (IP or MAC_ADDRESS)
- RADIUS::NAS_IP_Address
- RADIUS::NAS_Identifier

AAA attributes for third-party VPN concentrators

For VPN concentrators to integrate with Cisco ISE, these AAA attributes should be included in the RADIUS communication:

- Calling-Station-ID (tracks individual client by MAC or IP address)
- User-Name (tracks remote client by login name)
- NAS-Port-Type (helps to determine connection type as VPN)
- RADIUS Accounting Start (triggers official start of session)

- RADIUS Accounting Stop (triggers official end of session and releases ISE license)
- RADIUS Accounting Interim Update on IP address change (for example, SSL VPN connection transitions from Web-based to a full-tunnel client)

For VPN devices, the RADIUS Accounting messages must have the Framed-IP-Address attribute set to the client's VPN-assigned IP address to track the endpoint while on a trusted network.

System requirements

To ensure uninterrupted Cisco ISE configuration, it is essential to meet the specified system requirements. These requirements include using verified hardware platforms and following installation guidelines detailed in the Cisco Identity Services Engine Hardware Installation Guide. Adhering to these prerequisites helps maintain stable and reliable Cisco ISE operations without disruption.

For information on hardware platforms and installation for this Cisco ISE release, refer to the *Cisco Identity Services Engine Hardware Installation Guide*.

For information on the SSM On-Premises server releases that support smart licensing, refer to the Cisco ISE Licensing collection.

Verified hardware

Cisco ISE release 3.2, can be installed on these Cisco Secure Network Server (SNS) platforms:

Table 1: Verified Platforms

Hardware Platform	Configuration
Cisco SNS-3595-K9 (large)	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)*	

After installation, you can configure Cisco ISE with specific component personas such as Administration, Monitoring, or pxGrid on the platforms that are listed in the above table. In addition to these personas, Cisco ISE contains other types of personas within Policy Service, such as Profiling Service, Session Services, Threat-Centric NAC Service, SXP Service for TrustSec, TACACS+ Device Admin Service, and Passive Identity Service.

Caution

- *Cisco ISE release 3.1 patch 6 and above, and Cisco ISE release 3.2 patch 2 and above versions support Cisco SNS 3700 series appliances.
- Cisco ISE release 3.1 and later releases do not support Cisco Secured Network Server (SNS) 3515 appliance.
- Memory allocation of less than 16 GB is not supported for VM appliance configurations. In the event of a Cisco ISE behavior issue, all the users will be required to change the allocated memory to at least 16 GB before opening a case with the Cisco Technical Assistance Center.
- Legacy Access Control Server (ACS) and Network Access Control (NAC) appliances (including the Cisco ISE 3300 Series) are not supported in Cisco ISE, Release 2.0, and later.

Verified virtual environments

Cisco ISE supports these virtual environment platforms:

Table 2: Verified virtual environments

Virtual environment	Support details
VMware	• VMware 7.0.3 or later. • ISO files support ESXi 7.0 and ESXi 8.0. • OVA templates support VMware version 14 or later on ESXi 7.0 and ESXi 8.0. • In the case of vTPM devices, you must upgrade to VMware ESXi 7.0.3 or later releases. • You can use the VMware migration feature to migrate VM instances (running any persona) between hosts. Cisco ISE supports both hot and cold migration. Hot migration is also called live migration or **vMotion**. Cisco ISE need not be shut down or powered off during the hot migration. You can migrate the Cisco ISE VM without any interruption in its availability.
VMware Cloud Solutions on public cloud platforms	• AWS: Host Cisco ISE on a software-defined data center provided by VMware Cloud on AWS. • Azure VMware Solution: Runs VMware workloads natively on Microsoft Azure. • Google Cloud VMware Engine: Runs software-defined data center by VMware on Google Cloud.

Virtual environment	Support details
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 QEMU	• Supports QEMU 2.12.0-99 and later.
Nutanix	• Supported and verified Nutanix versions: AOS 7.0 AHV 10.0, AOS 6.8 AHV 20230302.100169, AOS 6.5.2.7 AHV 20220304.392.
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.

Federal Information Processing Standard (FIPS) mode support

Cisco ISE uses embedded Federal Information Processing Standard (FIPS) 140-2-validated cryptographic module, Cisco FIPS Object Module Version 7.2a (Certificate #4036). For details about the FIPS compliance claims, refer to Global Government Certifications.

When FIPS mode is enabled on Cisco ISE, follow these considerations:

- All non-FIPS-compliant cipher suites will be disabled.
- Certificates and private keys must use only FIPS-compliant hash and encryption algorithms.
- RSA private keys must be 2048 bits or greater.
- Elliptical Curve Digital Signature Algorithm (ECDSA) private keys must be 224 bits or greater.
- Diffie–Hellman Ephemeral (DHE) ciphers work with Diffie–Hellman (DH) parameters of 2048 bits or greater.
- SHA1 is not allowed to generate ISE local server certificates.
- The anonymous PAC provisioning option in EAP-FAST is disabled.
- The local SSH server operates in FIPS mode.

  These protocols are not supported in FIPS mode for RADIUS:

  - EAP-MD5
  - PAP
  - CHAP

- MS-CHAPv1
- MS-CHAPv2
- LEAP

Verified and supported browsers

Cisco ISE release 3.2 is supported on these browsers:

- Mozilla Firefox versions 123, 125, 128, 136, 138, 139, 145, 146, and 147
- Google Chrome versions 126, 127, 134, 135, 137, 139, 140, 141, and 142
- Microsoft Edge versions 122, 124, 125, 128, 134, 135, 140, 141, and 142



Restriction Currently, you cannot access the Cisco ISE GUI on mobile devices.

Verified external identity sources

Table 3: Verified external identity sources

External identity source	Version
Active Directory The supported Active Directory versions are the same for both Cisco ISE and Cisco ISE-PIC.	
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 Entra ID	—
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

External identity source	Version
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 Identity Provider version that is SAMLv2 compliant
Open Database Connectivity (ODBC) identity source	
Microsoft SQL Server	Microsoft SQL Server 2012 Microsoft SQL Server 2022
Oracle	Enterprise Edition Release 12.1.0.2.0
PostgreSQL	9.0
Sybase	16.0
MySQL	6.3
Social Login (for guest user accounts)	
Facebook	Latest

Verified Unified Endpoint Management and Mobile Device Management servers

Verified UEM and MDM servers include products from these vendors:

- Absolute
- Blackberry - BES
- Blackberry - Good Secure EMM
- Cisco Meraki Systems Manager
- Citrix XenMobile 10.x (On-premises)
- Globo
- IBM MaaS360

- Ivanti (previously MobileIron UEM), core and cloud UEM services

  For the use case of handling random and changing MAC Addresses in Cisco ISE, you must integrate MobileIron Core 11.3.0.0 Build 24 and later releases to receive GUID values.

  Restriction Some versions of MobileIron do not work with Cisco ISE. MobileIron is aware of this problem, and have a solution. Contact MobileIron for more information.

- JAMF Casper Suite
- Microsoft Endpoint Configuration Manager
- Microsoft Endpoint Manager Intune
- Mosyle
- SAP Afaria
- Sophos
- SOTI MobiControl
- Symantec
- Tangoe
- VMware Workspace ONE (previously AirWatch)
- 42Gears

For the configurations that you must perform in your endpoint management servers to integrate the servers with Cisco ISE, refer to Integrate UEM and MDM Servers With Cisco ISE.

References

ISE Community Resource
How To: Meraki EMM / MDM Integration with ISE

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 and supported ciphers

In a clean or fresh install of Cisco ISE, SHA1 ciphers are disabled by default. However, if you upgrade from an existing version of Cisco ISE, the SHA1 ciphers retain the options from the earlier version. You can view and change the SHA1 ciphers settings using the **Allow SHA1 Ciphers** field (**Administration** > **System** > **Settings** > **Security Settings**).

Restriction This does not apply to the Admin portal. When running in Federal Information Processing Standard Mode (FIPS), an upgrade does not remove SHA1 ciphers from the Admin portal.

Cisco ISE supports TLS versions 1.0, 1.1, and 1.2.

Cisco ISE supports RSA and ECDSA server certificates. These elliptic curves are supported:

- secp256r1
- secp384r1
- secp521r1

Cisco ISE does not support intermediate certificates having SHA256withECDSA signature algorithm for any of the elliptical curves due to the limitations in the current implementation of OpenJDK 1.8.

This table lists the supported cipher suites:

Table 4: Verified and supported cipher suites on Cisco ISE

Cipher suite	**When Cisco ISE is configured as an EAP server** **When Cisco ISE is configured as a RADIUS DTLS server**	**When Cisco ISE downloads CRL from HTTPS or a secure LDAP server** **When Cisco ISE is configured as a secure syslog client or a secure LDAP client** **When Cisco ISE is configured as a RADIUS DTLS client for CoA**
TLS 1.0 support	When TLS 1.0 is allowed (DTLS server supports only DTLS 1.2) Allow TLS 1.0 option is disabled by default in Cisco ISE 2.3 and above. TLS 1.0 is not supported for TLS based EAP authentication methods (EAP-TLS, EAP-FAST/TLS) and 802.1X supplicants when this option is disabled. If you want to use the TLS based EAP authentication methods in TLS 1.0, check the Allow TLS 1.0 check box in the **Security Settings** window. In the Cisco ISE GUI, navigate to **Administration** > **System** > **Settings** > **Protocols** > **Security Settings**.	When TLS 1.0 is allowed (DTLS client supports only DTLS 1.2)
TLS 1.1 support	When TLS 1.1 is allowed	When TLS 1.1 is allowed
ECC DSA ciphers		
ECDHE-ECDSA-AES256-GCM-SHA384	Yes	Yes
ECDHE-ECDSA-AES128-GCM-SHA256	Yes	Yes
ECDHE-ECDSA-AES256-SHA384	Yes	Yes
ECDHE-ECDSA-AES128-SHA256	Yes	Yes
ECDHE-ECDSA-AES256-SHA	When SHA-1 is allowed	When SHA-1 is allowed

Cipher suite	When Cisco ISE is configured as an EAP server When Cisco ISE is configured as a RADIUS DTLS server	When Cisco ISE downloads CRL from HTTPS or a secure LDAP server When Cisco ISE is configured as a secure syslog client or a secure LDAP client When Cisco ISE is configured as a RADIUS DTLS client for CoA
ECDHE-ECDSA-AES128-SHA	When SHA-1 is allowed	When SHA-1 is allowed
ECC RSA ciphers		
ECDHE-RSA-AES256-GCM-SHA384	When ECDHE-RSA is allowed	When ECDHE-RSA is allowed
ECDHE-RSA-AES128-GCM-SHA256	When ECDHE-RSA is allowed	When ECDHE-RSA is allowed
ECDHE-RSA-AES256-SHA384	When ECDHE-RSA is allowed	When ECDHE-RSA is allowed
ECDHE-RSA-AES128-SHA256	When ECDHE-RSA is allowed	When ECDHE-RSA is allowed
ECDHE-RSA-AES256-SHA	When ECDHE-RSA/SHA-1 is allowed	When ECDHE-RSA/SHA-1 is allowed
ECDHE-RSA-AES128-SHA	When ECDHE-RSA/SHA-1 is allowed	When ECDHE-RSA/SHA-1 is allowed
DHE RSA ciphers		
DHE-RSA-AES256-SHA256	No	Yes
DHE-RSA-AES128-SHA256	No	Yes
DHE-RSA-AES256-SHA	No	When SHA-1 is allowed
DHE-RSA-AES128-SHA	No	When SHA-1 is allowed
RSA ciphers		
AES256-SHA256	Yes	Yes
AES128-SHA256	Yes	Yes
AES256-SHA	When SHA-1 is allowed	When SHA-1 is allowed
AES128-SHA	When SHA-1 is allowed	When SHA-1 is allowed
3DES ciphers		
DES-CBC3-SHA	When 3DES/SHA-1 is allowed	When 3DES/DSS and SHA-1 are enabled
DSS ciphers		
DHE-DSS-AES256-SHA	No	When 3DES/DSS and SHA-1 are enabled

Cipher suite	When Cisco ISE is configured as an EAP server When Cisco ISE is configured as a RADIUS DTLS server	When Cisco ISE downloads CRL from HTTPS or a secure LDAP server When Cisco ISE is configured as a secure syslog client or a secure LDAP client When Cisco ISE is configured as a RADIUS DTLS client for CoA
DHE-DSS-AES128-SHA	No	When 3DES/DSS and SHA-1 are enabled
EDH-DSS-DES-CBC3-SHA	No	When 3DES/DSS and SHA-1 are enabled
Weak RC4 ciphers		
RC4-SHA	When "Allow weak ciphers" option is enabled in the Allowed Protocols page and when SHA-1 is allowed	No
RC4-MD5	When "Allow weak ciphers" option is enabled in the Allowed Protocols page	No
EAP-FAST anonymous provisioning only: ADH-AES-128-SHA	Yes	No
Peer certificate restrictions		
Validate KeyUsage	Client certificate should have KeyUsage=Key Agreement and ExtendedKeyUsage=Client Authentication for the following ciphers: • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	

Cipher suite	When Cisco ISE is configured as an EAP server When Cisco ISE is configured as a RADIUS DTLS server	When Cisco ISE downloads CRL from HTTPS or a secure LDAP server When Cisco ISE is configured as a secure syslog client or a secure LDAP client When Cisco ISE is configured as a RADIUS DTLS client for CoA
Validate ExtendedKeyUsage	Client certificate should have KeyUsage=Key Encipherment and ExtendedKeyUsage=Client Authentication for the following ciphers: • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA • DHE-RSA-AES128-SHA • DHE-RSA-AES256-SHA • DHE-RSA-AES128-SHA256 • DHE-RSA-AES256-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES256-SHA • ECDHE-RSA-AES128-SHA • EDH-RSA-DES-CBC3-SHA • DES-CBC3-SHA • RC4-SHA • RC4-MD5	Server certificate should have ExtendedKeyUsage=Server Authentication

Verified OpenSSL version

Cisco ISE release 3.2 is verified with OpenSSL 1.1.1k.

Verified client machine operating systems, supplicants, and agents

This section lists the verified client machine operating systems, browsers, and agent versions for each client machine type. For all devices, you must also have cookies enabled in the web browser.

These client machine types have been verified for Bring Your Own Device (BYOD) and Posture workflows:

- Apple iOS
- Apple macOS
- Google Android
- Google Chromebook
- Linux
- Microsoft Windows

Cisco ISE supports both AnyConnect and Cisco Secure Client for Windows, macOS, and Linux operating systems.

You can use all standard 802.1X supplicants with Cisco ISE 2.4 and later standard and advanced features, provided they support the standard authentication protocols supported by Cisco ISE. In a wireless deployment, the VLAN change authorization feature works only if the supplicant supports IP address refresh on VLAN change.

Posture and Bring Your Own Device (BYOD) flows are supported by the General Availability releases of the operating systems that are listed in the Cisco ISE UI, based on the latest Posture Feed Update. The Posture and BYOD flows may also work in the Beta macOS releases that are listed in the Cisco ISE UI. For example, if **macOS 12 Beta (all)** appears in the Cisco ISE GUI, Posture and BYOD flows may operate on macOS 12 Beta endpoints. Support is provided on a best-effort basis. Beta operating system releases often undergo significant changes between the initial and general availability (GA) releases.

After you update your operating system to a new version, support and reflection of the updated OS version in the Posture Feed Server may be delayed by a few hours or a day.

References

Refer to the Cisco Secure Client Posture Support Charts for additional information.

Apple iOS

These Apple iOS versions have been verified with Cisco ISE for BYOD and posture workflows.:

- Apple iOS 26.x
- Apple iOS 18.x
- Apple iOS 17.x
- Apple iOS 16.x
- Apple iOS 15.x
- Apple iOS 14.x
- Apple iOS 13.x
- Apple iOS 12.x

- Apple iOS 11.x

While Apple iOS devices use Protected Extensible Authentication Protocol (PEAP) with Cisco ISE or 802.1x, the public certificate includes a CRL distribution point that the iOS device needs to verify but it cannot do it without network access. Click “confirm/accept” on the iOS device to authenticate to the network.

For Apple iOS 12.2 and later, manually install the downloaded profile through **Settings** > **General** > **Profile**. After the first profile installation, choose **Settings** > **General** > **About** > **Certificate Trust Settings** > **Enable Full Trust For Root Certificate** for the installed profile. To ensure successful installation, verify that your RSA key size is at least 2048 bits. For iOS 13 and later, you must also regenerate the self-signed certificate for the portal role, ensuring the FQDN is included in the SAN field and the signature algorithm is set to SHA-256 or higher.

Apple macOS

These Apple macOS versions have been verified for BYOD and posture workflows.

Table 5: Apple macOS

Client machine operating system	AnyConnect
Apple macOS 26.x	5.0.04032 or later
Apple macOS 15.x	5.0.04032 or later
Apple macOS 14.x	5.0.04032 or later
Apple macOS 13.x	4.10.05111 or later
Apple macOS 12.6	4.10.05111 or later
Apple macOS 12.5	4.10.04071 or later
Apple macOS 11.6	4.9.04043 or later
Apple macOS 10.15	4.8.01090 or later
Apple macOS 10.14	4.8.01090 or later
Apple macOS 10.13	4.8.01090 or later

Cisco ISE does work with earlier release of AnyConnect 4.x. However, only newer AnyConnect releases support newer features.



Restriction For Apple macOS 11, you must use Cisco AnyConnect 4.9.04043 or above and MAC OSX compliance module 4.3.1466.4353 or above.

If you are using Apple macOS 11, you might see a prompt to install the profiles manually when you are installing the Cisco Network Setup Assistant. In this case, follow these steps:

1. Navigate to the Downloads folder.
2. Double-click the cisco802dot1xconfiguration.mobileconfig file.
3. Choose **System** > **Preferences**.

4. Click **Profiles**.
5. Install the profiles.
6. Click **OK** in the prompt that is displayed in the Cisco Network Setup Assistant to proceed with installation.

Because browsers limit reported macOS versions to 10.15.7 to enhance user privacy, Apple macOS 11 endpoints cannot be uniquely identified during provisioning or classification. This limitation impacts CP policy matching in Posture and BYOD flows, as well as profiling policy matching. As a workaround, map CP policies for macOS 11 endpoints to "macOS All."

You can use the Agentless Posture feature with all the supported Apple macOS releases. Refer to the topic "Agentless Posture" in the chapter "Compliance" in the *Cisco ISE Administrators Guide* for your Cisco ISE release.

The Supplicant Provisioning Wizard bundle for MAC OSX version 3.1.0.1 is common for all Cisco ISE releases.

For information about the Windows and MAC OSX anti-malware, patch management, disk encryption, and firewall products that are supported by the Cisco ISE Posture agent, refer to the Cisco Secure Client Posture Support Charts.

Google Android

These Google Android versions have been verified with Cisco ISE for BYOD and posture workflows:

- Google Android 16.x
- Google Android 15.x
- Google Android 14.x
- Google Android 13.x
- Google Android 12.x
- Google Android 11.x
- Google Android 10.x
- Google Android 9.x
- Google Android 8.x
- Google Android 7.x

Cisco ISE may not support certain Android OS version and device combinations due to the open access-nature of Android implementation on certain devices.

Ensure that the Location service is enabled on the Android 9.x and 10.x devices before starting the supplicant provisioning wizard (SPW).

Android no longer uses Common Name (CN). The hostname must be in the subjectAltName (SAN) extension, or trust fails. If you are using self-signed certificates, regenerate the Cisco ISE self-signed certificate by selecting the Domain Name or IP Address option from the SAN drop-down list for Portals. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **System Certificates**.

If you are using Android 9.x, you must update the posture feed in Cisco ISE to get the NSA for Android 9.

Google Chromebook

Google Chromebook is a managed device and does not support the Posture service. Refer to the *Cisco Identity Services Engine Administration Guide* for more information.

Google Chromebooks require Google Chrome version 49 or later for BYOD and posture workflows in Cisco ISE. If the Cisco ISE BYOD or Guest portal fails to launch in Chrome OS 73 despite a successful URL redirection, you can resolve the issue by manually importing a self-signed certificate. To do this, generate a new self-signed certificate in the Cisco ISE GUI, ensuring both the DNS and IP address are included in the **Subject Alternative Name** (SAN) field. Export and copy the certificate to the Chromebook, navigate to **Settings** > **Advanced** > **Privacy and Security** > **Manage certificates** > **Authorities** to import the file, and then open your browser to attempt the portal redirection.

In Chromebook 76 and later, if you are configuring EAP-TLS settings using an internal CA for EAP, upload the CA certificate chain with SAN fields to the Google Admin Console **Device Management** > **Network** > **Certificates**. Once the CA chain is uploaded, the Cisco ISE generated certificate with SAN fields is mapped under **Chromebook Authorities** section to consider your Cisco ISE certificate as trusted.

If you are using a third-party CA, you do not have to import CA chain to Google Admin Console. Choose **Settings** > **Advanced** > **Privacy and Security** > **Manage certificates** > **Server certificate Authority** and select **Use any default Certificate Authority** from the drop-down list.

Linux

These Linux versions has been verified for BYOD and posture workflows.

Table 6: Verified and supported Linux versions

Client Machine Operating System	Cisco AnyConnect
Red Hat Enterprise Linux (RHEL)	Cisco AnyConnect Release 5.1.2.04 and later
RHEL 7.5 and later	
RHEL 8.1 and later	
RHEL 9.0	
RHEL 9.3	
RHEL 9.4	
RHEL 9.5	
RHEL 9.6	
SUSE Linux Enterprise Server (SLES)	
SLES 12.3 and later	
SLES 15.x	
Ubuntu	
Ubuntu 18.04	
Ubuntu 20.04	
Ubuntu 22.04	
Ubuntu 23.04	
Ubuntu 23.10.1	
Ubuntu 24.04	

Microsoft Windows

This section provides compatibility information for Microsoft Windows operating systems with various Cisco ISE components including supplicants, Cisco Temporal Agent, and AnyConnect versions

Table 7: Verified and supported Microsoft Windows operating systems

Client Machine Operating System	Supplicants (802.1X)	Cisco Temporal Agent	AnyConnect[1]
Microsoft Windows 11			

Client Machine Operating System	Supplicants (802.1X)	Cisco Temporal Agent	AnyConnect[1]
• Windows 25H2 • Windows 24H2 • Windows 23H2 • Windows 22H2 • Windows 11 Enterprise • Windows 11 Pro • Windows 11 Education • Windows 11 Home	• Microsoft Windows 802.1x Client • AnyConnect Network Access Manager	4.10.04065 or later	4.10.5075 and later
Microsoft Windows 10			

Client Machine Operating System	Supplicants (802.1X)	Cisco Temporal Agent	AnyConnect[1]
• Windows 22H2 • Windows 21H2 • Windows 21H1 • Windows 20H2 • Windows 20H1 • Windows 19H2 • Windows 19H1 • Windows 10 Enterprise • Windows 10 Enterprise N • Windows 10 Enterprise E • Windows 10 Enterprise LTSB • Windows 10 Enterprise N LTSB • Windows 10 Pro • Windows 10 Pro N • Windows 10 Pro E • Windows 10 Education • Windows 10 Home • Windows 10 Home Chinese • Windows 10.0 SLP (Single Language Pack)	• Microsoft Windows 10 802.1X Client • AnyConnect Network Access Manager	4.5 or later	4.10.5075 and later

[1] If you have AnyConnect Network Access Manager (NAM) installed, NAM takes precedence over Windows native supplicant as the 802.1X supplicant and it does not support the BYOD flow. You must disable NAM completely or on a specific interface. See the Cisco AnyConnect Secure Mobility Client Administration Guide for more information.

Follow these steps to enable wireless redirection in Firefox 70 for BYOD, Guest, and Client Provisioning portals:

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Security Settings**.
2. Check the **Allow SHA1 ciphers** check box. SHA1 ciphers are disabled by default.
3. In your Firefox browser, choose **Options** > **Privacy & Settings** > **View Certificates** > **Servers** > **Add Exception**.
4. Add *https://<FQDN>:8443/* as exception.

5. Click **Add Certificate** and then refresh your Firefox browser.

You can use the Agentless Posture feature with all the supported Microsoft releases. Refer to the topic "Agentless Posture" in the chapter "Compliance" in the *Cisco ISE Administrators Guide* for your Cisco ISE release.

Verified operating systems and browsers for Sponsor, Guest, and My Devices portals

These Cisco ISE portals support these operating system and browser combinations. These portals require that you have cookies enabled in your web browser.

Table 8: Verified operating systems and browsers

Supported operating system	Browser versions
Google Android[2] 16.x, 15.x, 14.x, 13.x, 12.x, 11.x, 10.x, 9.x, 8.x, 7.x	• Native browser • Mozilla Firefox • Google Chrome
Apple iOS 26.x, 18.x, 17.x, 16.x, 15.x, 14.x, 13.x, 12.x, 11.x	• Safari
Apple macOS 26.x, 15.x, 14.x, 13, 12.6, 12.5, 11.6, 10.15, 10.14, 10.13	• Mozilla Firefox • Safari • Google Chrome
Microsoft Windows 10, 11	• Microsoft IE 11.x • Microsoft Edge • Mozilla Firefox • Google Chrome

[2] Cisco ISE may not support certain Android OS version and device combinations due to the open access-nature of Android implementation on certain devices.

Verified devices for BYOD onboarding and certificate provisioning

These devices have been verified for BYOD onboarding and certificate provisioning with Cisco ISE.

Table 9: BYOD onboarding and certificate provisioning - Verified devices and operating systems

Device	Operating system	Single SSID	Dual SSID (open > PEAP (no cert) or open > TLS)	Onboard method	Supported Browsers
Apple iDevice	Apple iOS 26.x, 18.x, 17.x, 16.x, 15.x, 14.x, 13.x, 12.x, 11.x Apple iPad OS 13.x	Yes	Yes[3]	Apple profile configurations (native)	**Supported:** Safari. **Not Supported:** Mozilla Firefox and Google Chrome.
Google Android	16.x, 15.x, 14.x, 13.x, 12.x, 11.x, 10.x, 9.x, 8.x, 7.x	Yes[4]	Yes	Cisco Network Setup Assistant[5]	**Supported**: Firefox and Google Chrome.
Barnes & Noble Nook (Android) HD/HD+[6]	—	—	—	—	—
Microsoft Windows	Microsoft Windows 10, 11 Microsoft Windows 10 Version 2004 (OS build 19041.1) and higher is required for EAP TEAP.	Yes[7]	Yes	2.2.1.53 or later	**Supported:** Firefox and Google Chrome.
Windows	Mobile 8, Mobile RT, Surface 8, and Surface RT	No	No	—	**Supported:** Firefox and Google Chrome.
Apple macOS	Apple macOS 26.x, 15.x, 14.x, 13, 12.6, 12.5, 11.6, 10.15, 10.14, 10.13	Yes	Yes	2.2.1.43 or later	**Supported:** Google Chrome and Safari.

[3] Connect to secure SSID after provisioning.

[4] You cannot modify the system-created SSIDs using the Cisco supplicant provisioning wizard (SPW), if you are using Android version 6.0 or above. When the SPW prompts you to forget the network, you must choose this option and press the Back button to continue the provisioning flow.

[5] You must use Native Supplicant Protocol 3.1.7 for Android 11 and earlier versions. You must use Native Supplicant Protocol 3.1.9 for Android 12 and later versions.

[6] Barnes & Noble Nook (Android) works when it has Google Play Store 2.1.0 installed.

[7] While configuring the wireless properties for the connection (**Security > Auth Method > Settings > Validate Server Certificate**), uncheck the valid server certificate option. If you check this option, ensure that you select the correct root certificate.

To ensure the successful implementation of the BYOD feature, Cisco Wireless LAN Controller (WLC) version 7.2 or later is required. Refer to the Release Notes for the Cisco Identity Services Engine for any known issues or caveats. To maintain compatibility with the latest Cisco-supported client operating systems, you must check the posture update information. To do this, navigate to **Administration** > **System** > **Settings** > **Posture** > **Updates** in the Cisco ISE GUI and click **Update Now**.

Verified security product integrations over Cisco pxGrid

All pxGrid connections must be based on pxGrid 2.0. pxGrid 1.0-based (XMPP-based) integrations are not supported in the latest Cisco ISE releases.

Table 10: Verified security product integrations over Cisco pxGrid

Product	Cisco ISE 3.2	Cisco ISE 3.1	Cisco ISE 3.0	Cisco ISE 2.7
Cisco Firepower Management Center	Firepower Threat Defense with Cisco Firepower Management Center 7.1 Firepower Threat Defense with Firepower Device Management 7.1 Firepower Threat Defense with Cisco Firepower Management Center 7.2 Firepower Threat Defense with Firepower Device Management 7.3 Firepower Threat Defense with Cisco Firepower Management Center 7.3	Firepower Threat Defense with Cisco Firepower Management Center 7.0.1 Firepower Threat Defense with Firepower Device Management 7.0.1 Firepower Threat Defense with Cisco Firepower Management Center 7.1 Firepower Threat Defense with Firepower Device Management 7.1 Firepower Threat Defense with Cisco Firepower Management Center 7.2 Firepower Threat Defense with Firepower Device Management 7.2		Firepower Threat Defense with Cisco Firepower Management Center 6.6.7 Firepower Threat Defense with Firepower Device Management 6.6.7 Firepower Threat Defense with Cisco Firepower Management Center 7.0 Firepower Threat Defense with Firepower Device Management 7.0

Product	Cisco ISE 3.2	Cisco ISE 3.1	Cisco ISE 3.0	Cisco ISE 2.7
			Firepower Threat Defense with Cisco Firepower Management Center 6.6.5 Firepower Threat Defense with Firepower Device Management 6.6.5 Firepower Threat Defense with Cisco Firepower Management Center 6.6.7 Firepower Threat Defense with Firepower Device Management 6.6.7 Firepower Threat Defense with Cisco Firepower Management Center 7.0 Firepower Threat Defense with Firepower Device Management 7.0 Firepower Threat Defense with Cisco Firepower Management Center 7.0.1 Firepower Threat Defense with Firepower Device Management 7.0.1 Firepower Threat Defense with Cisco Firepower Management Center 7.0.2 Firepower Threat Defense with Firepower Device Management 7.0.2 Firepower Threat Defense with Cisco Firepower Management Center 7.1 Firepower Threat	

Product	Cisco ISE 3.2	Cisco ISE 3.1	Cisco ISE 3.0	Cisco ISE 2.7
			Defense with Firepower Device Management 7.1 Firepower Threat Defense with Cisco Firepower Management Center 7.2 Firepower Threat Defense with Firepower Device Management 7.2	
Cisco Secure Network Analytics	Cisco Secure Network Analytics 7.3.2 Cisco Secure Network Analytics 7.4.1	Cisco Secure Network Analytics 7.4.1 Cisco Secure Network Analytics 7.4.2	Cisco Secure Network Analytics 7.3.1 Cisco Secure Network Analytics 7.3.2 Cisco Secure Network Analytics 7.4	Cisco Secure Network Analytics 7.3.0 Cisco Secure Network Analytics 7.3.1 Cisco Secure Network Analytics 7.3.2 Cisco Secure Network Analytics 7.4
Cisco Web Security Appliance	Cisco Web Security Appliance 14.5.0* Cisco Web Security Appliance 14.5.1	Cisco Web Security Appliance 11.5.1 Cisco Web Security Appliance 12.5.4 Cisco Web Security Appliance 14.0.2 Cisco Web Security Appliance 14.5.0	Cisco Web Security Appliance 11.5.1 Cisco Web Security Appliance 12.0.5 Cisco Web Security Appliance 12.5.3 Cisco Web Security Appliance 12.5.4 Cisco Web Security Appliance 14.0.2 Cisco Web Security Appliance 14.0.3 Cisco Web Security Appliance 14.5.0	Cisco Web Security Appliance 11.5.1 Cisco Web Security Appliance 11.8.3 Cisco Web Security Appliance 12.0.3 Cisco Web Security Appliance 12.5.3 Cisco Web Security Appliance 12.5.4 Cisco Web Security Appliance 14.0.0 Cisco Web Security Appliance 14.0.2 Cisco Web Security Appliance 14.5.0



Restriction *For successful Cisco Web Security Appliance 14.5.0 integration, Cisco ISE release 3.2 must have External RESTful Services (ERS) in a disabled state. This is a known limitation and can be tracked through the caveat CSCwc91516.

Verified Cisco Catalyst Center release

Cisco ISE can integrate with Cisco Catalyst Center. For information about configuring Cisco ISE to work with Cisco Catalyst Center, refer to the *Cisco DNA Center documentation*.

For information about Cisco ISE compatibility with Cisco Catalyst Center, refer to *Cisco SD-Access Compatibility Matrix*.

Verified Cisco Prime Infrastructure release

Cisco Prime Infrastructure release 3.6 and later can be integrated with Cisco ISE to leverage the monitoring and reporting capabilities of Cisco ISE.

Verified Cisco Firepower Management Center release

Cisco Firepower Management Center release 6.4 and later can be integrated with Cisco ISE.

Verified Cisco Secure Network Analytics release

Cisco Secure Network Analytics release 6.9 and later can be integrated with Cisco ISE.

Verified Cisco WAN Service Administrator release

Cisco WAN Service Administrator release 11.5.1 and later can be integrated with Cisco ISE.

Verified support for Threat Centric NAC

Cisco ISE is verified with these Threat Centric NAC (TC-NAC) adapters:

- SourceFire FireAMP
- Cognitive Threat Analytics (CTA) adapter
- Rapid7 Nexpose
- Tenable Security Center
- Qualys (Only the Qualys Enterprise Edition is currently supported for TC-NAC flows)

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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)

© 2022 Cisco Systems, Inc. All rights reserved.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.