Cisco Identity Services Engine Network Component Compatibility, Release 3.5

Revised: September 19, 2025

Overview

Cisco ISE supports protocol standards like RADIUS, its associated RFC Standards, and TACACS+. For more information, see 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.

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, see "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, see 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, see ISE Third-Party NAD Profiles and Configs. For information on how to configure TACACS+ for Nexus devices, see Cisco ISE Device Administration Prescriptive Deployment Guide.

Note

- 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.

For Wireless LAN Controllers, note the following:

- MAC authentication bypass (MAB) supports MAC filtering with RADIUS lookup.

- 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. See the *Cisco Access Points Release Notes* for more details.

For information about the devices that are validated with Cisco ISE, see Network Device Capabilities Validated with Cisco Identity Services Engine.

Supported protocol standards, RFCs, and IETF drafts

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

- **Supported IEEE standards**
  - IEEE802.1X-Std-2001
  - IEEE802.1X-Std-2004
- **Supported 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

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) (supported as part of BYOD flow)
- RFC7170 - Tunnel Extensible Authentication Protocol (TEAP) Version 1

- **Supported 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 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)

Note 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

For an uninterrupted Cisco ISE configuration, ensure that these system requirements are fulfilled.

For more details on hardware platforms and installation for this Cisco ISE release, see the *Cisco Identity Services Engine Hardware Installation Guide*.

For information on the SSM On-Prem server releases that support smart licensing, see the topic Configure Smart Software Manager On-Prem for Smart Licensing in the Chapter "Licensing", in the Cisco ISE Administrator Guide for your release.

Supported hardware

Cisco ISE 3.5 can be installed on these Secure Network Server (SNS) hardware platforms:

Table 1: Supported platforms

Hardware platform	Configuration
Cisco SNS-3615-K9 (small)	For appliance hardware specifications, see the *Cisco Secure Network Server Appliance Hardware Installation Guide*.
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

Cisco ISE supports these virtual environment platforms:

- VMware ESXi 7.0.3 and later releases

  In the case of vTPM devices, you must upgrade to VMware ESXi 7.0.3 or later releases.

  - OVA templates: VMware version 14 or later on ESXi 7.0 and ESXi 8.0.
  - ISO file supports ESXi 7.0 and ESXi 8.0.

  You can deploy Cisco ISE on VMware cloud solutions on these public cloud platforms:

  - VMware cloud in Amazon Web Services (AWS): Host Cisco ISE on a software-defined data center provided by VMware Cloud on AWS.
  - Azure VMware Solution: Azure VMware Solution runs VMware workloads natively on Microsoft Azure. You can host Cisco ISE as a VMware virtual machine.

- Google Cloud VMware Engine: Google Cloud VMware Engine runs software defined data center by VMware on the Google Cloud. You can host Cisco ISE as a VMware virtual machine on the software-defined data center provided by the VMware Engine.

Note From Cisco ISE 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 for compute and storage. 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.

- Microsoft Hyper-V on Microsoft Windows Server 2012 R2 and later

  Cisco ISE supports Azure Stack HCI 23H2 and later versions. The virtual machine requirements and the installation procedure for the Cisco ISE VMs in the Azure Stack HCI are the same as that of Microsoft Hyper-V.

- KVM on QEMU 2.12.0-99 and later

Note Cisco ISE cannot be installed on OpenStack.

- Nutanix 20230302.100169
- 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.

You can deploy Cisco ISE natively on these public cloud platforms:

- Amazon Web Services (AWS)
- Microsoft Azure Cloud
- Oracle Cloud Infrastructure (OCI)

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

Federal Information Processing Standard 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, see Global Government Certifications.

When FIPS mode is enabled on Cisco ISE, consider the following:

- 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.
- The following protocols are not supported in FIPS mode for RADIUS:
  - EAP-MD5
  - PAP
  - CHAP
  - MS-CHAPv1
  - MS-CHAPv2
  - LEAP

Validated browsers

Cisco ISE 3.5 is supported 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

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

Validated external identity sources

Note The supported Active Directory versions are the same for both Cisco ISE and Cisco ISE-PIC.

Cisco ISE supports Microsoft Entra ID.

Table 2: Validated External Identity Sources

External Identity Source	Version
Active Directory	
Microsoft Windows Active Directory 2012	Windows Server 2012
Microsoft Windows Active Directory 2012 R2 [1]	Windows Server 2012 R2
Microsoft Windows Active Directory 2016	Windows Server 2016
Microsoft Windows Active Directory 2019	Windows Server 2019

External Identity Source	Version
Microsoft Windows Active Directory 2022	Windows Server 2022 with Patch Windows10.0-KB5025230-x64-V1.006.msu
Microsoft Windows Active Directory 2025 **Important** 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
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

External Identity Source	Version
PostgreSQL	9.0
Sybase	16.0
MySQL	6.3
Social Login (for Guest User Accounts)	
Facebook	Latest

[1] 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.

Supported Unified Endpoint Management and Mobile Device Management servers

Supported MDM servers include products from these vendors:

- Absolute
- Blackberry - BES
- Blackberry - Good Secure EMM
- Cisco Meraki Systems Manager
- Citrix XenMobile 10.x (On-prem)
- 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.

  

  Note Some versions of MobileIron do not work with Cisco ISE. MobileIron is aware of this problem, and have a fix. 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 (earlier known as AirWatch)
- 42Gears

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

ISE Community Resource

How To: Meraki EMM / MDM Integration with ISE

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.

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**).

Note 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, 1.2, and 1.3.

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

- secp256r1
- secp384r1
- secp521r1

Note 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:

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, click the **Menu** icon (☰) and choose **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
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
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	

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

Validated OpenSSL version

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

Validated client machine operating systems, supplicants, and agents

This section lists the validated 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. Cisco AnyConnect-ISE Posture Support Charts are available at: https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-device-support-tables-list.html

These client machine types have been validated 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.

All standard 802.1X supplicants can be used with Cisco ISE 2.4 and later standard and advanced features as long as they support the standard authentication protocols supported by Cisco ISE. For the VLAN change authorization feature to work in a wireless deployment, the supplicant must support 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)** is listed in the Cisco ISE UI, Posture and BYOD flows may work on macOS 12 Beta endpoints. Support is provided on a best-effort basis as beta operating system releases often undergo significant changes between the initial and General Availability releases.

Note that when you update your Operating System (OS) to a new version, you may experience a delay (of a few hours or a day) in support and refection of the updated OS version in the Posture Feed Server.

Apple iOS

This client machine type has been validated for BYOD and posture workflows.

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.

These Apple iOS versions have been validated with Cisco ISE:

- 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

Note

- If you are using Apple iOS 12.2 or later version, you must manually install the downloaded Certificate/Profile. To do this, choose **Settings > General > Profile** in the Apple iOS device and Click **Install**. After the first profile installation, choose **Settings** > **General** > **About** > **Certificate Trust Settings** > **Enable Full Trust For Root Certificate** for the installed profile.
- If you are using Apple iOS 12.2 or later version, RSA key size must be 2048 bits or higher. Otherwise, you might see an error while installing the BYOD profile.
- If you are using Apple iOS 13 or a later version, regenerate the self-signed certificate for portal role by adding the **<<FQDN>>** as **DNS Name** in the **SAN** field.
- If you are using Apple iOS 13 or a later version, ensure that **SHA-256** (or greater) is selected as the signature algorithm.

Apple macOS

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

Table 3: Apple macOS

Client machine operating system	AnyConnect
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.

Note 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, you must do the following:

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.

Note 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, see the Cisco AnyConnect-ISE Posture Support Charts.

Note

- All browsers have capped the reported Apple macOS version to 10.15.7 and increased user privacy.
- During provisioning we won't be able to identify Apple macOS 11 endpoints. This leads to an issue with CP policy matching in Posture and BYOD flows when client is running Apple macOS 11. As a workaround, proceed with Posture and BYOD flows for Apple macOS 11 as Map CP policy as macOS All.
- During classification we won't be able to identify Apple macOS 11 endpoints. This leads to an issue with profiling policy matching when client is running Apple macOS 11.

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

Google Android

This client machine type has been validated for BYOD and posture workflows.

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

These Google Android versions have been validated with Cisco ISE:

- 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

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 Cisco ISE self-signed certificate by selecting 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

This client machine type has been validated for BYOD and posture workflows.

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

Table 4: Google Chromebook

Client Machine Operating System	Web Browser
Google Chromebook	Google Chrome version 49 or later

Cisco ISE BYOD or Guest portal may fail to launch in Chrome Operating System 73 even though the URL is redirected successfully. To launch the portals in Chrome Operating System 73, follow the steps below:

1. Generate a new self-signed certificate from ISE GUI by filling the Subject Alternative Name field. Both DNS and IP Address must be filled.
2. Export and copy the certificate to the end client (chrome book).
3. Choose **Settings > Advanced > Privacy and Security > Manage certificates > Authorities**.
4. Import the certificate.
5. Open the browser and try to redirect the portal.

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

This client machine type has been validated for BYOD and posture workflows.

Table 5: Linux

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	
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

Table 6: Microsoft Windows

Client Machine Operating System	Supplicants (802.1X)	Cisco Temporal Agent	AnyConnect[2]
Microsoft Windows 11			
• 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[2]
• 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

[2] 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.

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. See the topic "Agentless Posture" in the Chapter "Compliance" in the *Cisco ISE Administrators Guide* for your Cisco ISE release.

Validated 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 7: Validated operating systems and browsers

Supported operating system	Browser versions
Google Android[3] 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 18.x, 17.5, 17.x, 16.x, 15.x, 14.x, 13.x, 12.x, 11.x	• Safari
Apple macOS 15.x, 14.5, 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

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

Validated devices for onboarding and certificate provisioning

Cisco Wireless LAN Controller (WLC) 7.2 or later support is required for the BYOD feature. See the Release Notes for the Cisco Identity Services Engine for any known issues or caveats.

Note To get the latest Cisco-supported client Operating System versions, check the posture update information. To do this:

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **Updates**.
2. Click **Update Now**.

Table 8: BYOD onboarding and certificate provisioning - Validated 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 18.x, 17.x, 16.x, 15.x, 14.x, 13.x, 12.x, 11.x Apple iPad OS 13.x	Yes	Yes[4]	Apple profile configurations (native)	**Supported:** Safari. **Not Supported:** Mozilla Firefox and Google Chrome.
Google Android	15.x, 14.x, 13.x, 12.x, 11.x, 10.x, 9.x, 8.x, 7.x	Yes[5]	Yes	Cisco Network Setup Assistant[6]	**Supported**: Firefox and Google Chrome.
Barnes & Noble Nook (Android) HD/HD+[7]	—	—	—	—	—
Microsoft Windows	Microsoft Windows 10, 11 Microsoft Windows 10 Version 2004 (OS build 19041.1) and higher is required for EAP TEAP.	Yes[8]	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 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.

[4] Connect to secure SSID after provisioning.

[5] 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.

[6] 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.

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

[8] 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.

Validated security product integrations (over pxGrid)

Table 9: Validated security product integrations (over pxGrid)

Product	Cisco ISE 3.5	Cisco ISE 3.4	Cisco ISE 3.3	Cisco ISE 3.2
Cisco Firepower Management Center	Firepower Threat Defense with Cisco Firepower Management Center 7.6.1 Firepower Threat Defense with Firepower Device Management 7.6.1	Firepower Threat Defense with Cisco Firepower Management Center 7.2.4 Firepower Threat Defense with Firepower Device Management 7.2.4 Firepower Threat Defense with Cisco Firepower Management Center 7.4.1 Firepower Threat Defense with Firepower Device Management 7.4.1 Firepower Threat Defense with Cisco Firepower Management Center 7.4.2 Firepower Threat Defense with Firepower Device Management 7.4.2	Firepower Threat Defense with Cisco Firepower Management Center 7.2.4 Firepower Threat Defense with Firepower Device Management 7.2.4 Firepower Threat Defense with Firepower Device Management 7.3 Firepower Threat Defense with Cisco Firepower Management Center 7.3 Firepower Threat Defense with Firepower Device Management 7.4 Firepower Threat Defense with Cisco Firepower Management Center 7.4	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
Cisco Secure Network Analytics	Cisco Secure Network Analytics 7.5.2	Cisco Secure Network Analytics 7.4.0 Cisco Secure Network Analytics 7.4.2 Cisco Secure Network Analytics 7.5.0 Cisco Secure Network Analytics 7.5.1	Cisco Secure Network Analytics 7.4.1 Cisco Secure Network Analytics 7.4.2	Cisco Secure Network Analytics 7.3.2 Cisco Secure Network Analytics 7.4.1

Product	Cisco ISE 3.5	Cisco ISE 3.4	Cisco ISE 3.3	Cisco ISE 3.2
Cisco Web Security Appliance	Cisco Web Security Appliance 15.2.2	Cisco Web Security Appliance 14.15.0 Cisco Web Security Appliance 14.15.2011 Cisco Web Security Appliance 15.2.0 Cisco Web Security Appliance 15.12.0	Cisco Web Security Appliance 14.5.1	Cisco Web Security Appliance 14.5.0* Cisco Web Security Appliance 14.5.1

*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.

Note 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.

Validated Cisco Digital Network Architecture Center release

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

For information about Cisco ISE compatibility with Cisco DNA Center, see *Cisco SD-Access Compatibility Matrix*.

Validated 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.

Validated Cisco Firepower Management Center release

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

Validated Cisco Secure Network Analytics release

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

Validated Cisco WAN Service Administrator release

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

Support for Threat Centric NAC

Cisco ISE is validated with these 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)

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.