Cisco Identity Services Engine Network Component Compatibility, Release 2.6

Revised: June 30, 2023

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.

Validated 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, 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.

The following notations are used to mark the device support:

- √ : Fully supported
- X : Not supported
- ! : Limited support, some functionalities are not supported.

The following functionalities are supported by each feature:

Table 1: Features and Functionalities

Feature	Functionality
AAA	802.1X, MAB, VLAN Assignment, dACL
Profiling	RADIUS CoA and Profiling Probes
BYOD	RADIUS CoA, URL Redirection and SessionID
Guest	RADIUS CoA, Local Web Auth, URL Redirection and SessionID
Guest Originating URL	RADIUS CoA, Local Web Auth, URL Redirection and SessionID
Posture	RADIUS CoA, URL Redirection and SessionID
MDM	RADIUS CoA, URL Redirection and SessionID
TrustSec	SGT Classification

Validated Cisco Access Switches

Table 2: Validated Cisco Access Switches

Device	Validated OS [1] Minimum OS [3]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
IE2000 IE3000	Cisco IOS 15.2(2)E4 Cisco IOS 15.2(4)EA6	√	√	√	√	√	√	√	√
	Cisco IOS 15.0(2)EB	√	√	√	√	*X*	√	√	√

Device	Validated OS [1] Minimum OS [3]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
IE4000 IE5000	Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2 Cisco IOS 15.2(4)EA6	√	√	√	√	√	√	√	√
	Cisco IOS 15.0.2A-EX5	√	√	√	√	√	√	√	√
IE4010	Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2	√	√	√	√	√	√	√	√
	Cisco IOS 15.0.2A-EX5	√	√	√	√	√	√	√	√
CGS 2520	Cisco IOS 15.2(3)E3	√	√	√	√	*X*	√	√	√
	Cisco IOS 15.2(3)E3	√	√	√	√	*X*	√	√	√
Catalyst 1000	Cisco IOS 15.2(7)E3	√	√	√	√	√	√	√	—
	Cisco IOS 15.2(7)E3	√	√	√	√	√	√	√	—
Catalyst 2960 LAN Base	Cisco IOS 15.0(2)SE11	√	√	√	√	*X*	√	√	*X*
	Cisco IOS v12.2(55)SE5 [4]	√	√	√	!	*X*	!	!	*X*
Catalyst 2960-C Catalyst 3560-C	Cisco IOS 15.2(2)E4	√	√	√	√	√	√	√	√
	Cisco IOS 12.2(55)EX3	√	√	√	√	√	√	√	√
Catalyst 2960-L	Cisco IOS 15.2(6.1.27)E2	√	√	√	√	√	√	√	*X*
	Cisco IOS 15.2(6)E2	√	√	√	√	√	√	√	*X*
Catalyst 2960-Plus Catalyst 2960-SF	Cisco IOS 15.2(2)E4	√	√	√	√	√	√	√	√
	Cisco IOS 15.0(2)SE7	√	√	√	√	√	√	√	*X*

Device	Validated OS [1] Minimum OS [3]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
Catalyst 2960-S	Cisco IOS 15.2(2)E6	√	√	√	√	√	√	√	√
	Cisco IOS 15.2(2)E9	√	√	√	√	√	√	√	*X*
	Cisco IOS 15.0.2SE10a Cisco IOS 15.0(2)SE11	√	√	√	√	√	√	√	*X*
	Cisco IOS 12.2.(55)SE5	√	√	√	√	√	√	√	*X*
Catalyst 2960–XR Catalyst 2960–X	Cisco IOS 15.2(2)E6 Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2 Cisco IOS 15.2.6E1(ED) Cisco IOS 15.2(2)E9	√	√	√	√	√	√	√	√
	Cisco IOS 15.0.2A-EX5	√	√	√	√	√	√	√	√
Catalyst 2960-CX Catalyst 3560-CX	Cisco IOS 15.2(3)E1	√	√	√	√	√	√	√	√
	Cisco IOS 15.2(3)E	√	√	√	√	√	√	√	√
Catalyst 3560-G Catalyst 3750-G Cat 3750-E	Cisco IOS 15.2(2) E6 Cisco IOS 12.2(55)SE5 Cisco IOS 12.2(55)SE10 Cisco IOS 12.2(55)SE11	√	√	√	√	√	√	√	√
	Cisco IOS 12.2(55)SE5	√	√	√	√	√	√	√	√
Catalyst 3560V2	Cisco IOS 12.2(55)SE10	√	√	√	√	√	√	√	√
Catalyst 3750V2	Cisco IOS 12.2(55)SE5	√	√	√	√	√	√	√	√

Device	Validated OS [1] Minimum OS [3]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
Catalyst 3560-E	Cisco IOS 15.0(2)SE11	√	√	√	√	√	√	√	√
	Cisco IOS 12.2(55)SE5	√	√	√	√	√	√	√	√
Catalyst 3560-X	Cisco IOS 15.2(2)E5 Cisco IOS 15.2(2)E6	√	√	√	√	√	√	√	√
	Cisco IOS 12.2(55)SE5	√	√	√	√	√	√	√	√
Catalyst 3650 Catalyst 3650-X	Cisco IOS XE 16.3.3 Cisco IOS XE 3.6.5E Cisco IOS 16.6.2 ES Cisco IOS 16.9.1 ES Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 3.3.5.SE	√	√	√	√	√	√	√	√
Catalyst 3750-E	Cisco IOS 15.2(2) E6 Cisco IOS 15.0(2)SE11	√	√	√	√	√	√	√	√
	Cisco IOS 12.2(55)SE5	√	√	√	√	√	√	√	√
Catalyst 3750-X	Cisco IOS 15.2(2) E6 Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2	√	√	√	√	√	√	√	√
	Cisco IOS 12.2(55)SE5	√	√	√	√	√	√	√	√

Device	Validated OS [1] Minimum OS [3]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
Catalyst 3850	Cisco IOS XE 16.3.3 Cisco IOS XE 3.6.5E Cisco IOS XE 3.6.7E Cisco IOS XE 3.6.9E Cisco IOS 16.6.2 ES Cisco IOS 16.9.1 ES Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 3.3.5.SE	√	√	√	√	√	√	√	√
Catalyst 4500-X	Cisco IOS XE 3.6.6 E Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2 Cisco IOS 15.2(6)E	√	√	√	√	√	√	√	√
	Cisco IOS XE 3.4.4 SG	√	√	√	√	*X*	√	√	√
Catalyst 4500 Supervisor 7-E, 7L-E	Cisco IOS XE 3.6.4	√	√	√	√	√	√	√	√
	Cisco IOS XE 3.4.4 SG	√	√	√	√	*X*	√	√	√
Catalyst 4500 Supervisor 6-E, 6L-E	Cisco IOS 15.2(2)E4	√	√	√	√	*X*	√	√	√
	Cisco IOS 15.2(2)E	√	√	√	√	*X*	√	√	√
Catalyst 4500 Supervisor 8-E	Cisco IOS XE 3.6.4 Cisco IOS XE 3.6.8E Cisco IOS 15.2(6)E	√	√	√	√	*X*	√	√	√
	Cisco IOS XE 3.3.2 XO	√	√	√	√	*X*	√	√	√
Catalyst 5760	Cisco IOS XE 3.7.4	√	√	√	√	*X*	√	√	√
	—	—	—	—	—	—	—	—	—
Catalyst 6500-E (Supervisor 32)	Cisco IOS 12.2(33)SXJ10	√	√	√	√	*X*	√	√	√
	Cisco IOS 12.2(33)SXI6	√	√	√	√	*X*	√	√	√

Device	Validated OS [1] Minimum OS [3]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
Catalyst 6500-E (Supervisor 720)	Cisco IOS 15.1(2)SY7	√	√	√	√	*X*	√	√	√
	Cisco IOS v12.2(33)SXI6	√	√	√	√	*X*	√	√	√
Catalyst 6500-E (VS-S2T-l0G)	Cisco IOS 152-1.SY1a	√	√	√	√	*X*	√	√	√
	Cisco IOS 15.0(1)SY1	√	√	√	√	*X*	√	√	√
Catalyst 6807-XL Catalyst 6880-X (VS-S2T-l0G)	Cisco IOS 152-1.SY1a	√	√	√	√	*X*	√	√	√
	Cisco IOS 15.0(1)SY1	√	√	√	√	*X*	√	√	√
Catalyst 6500-E (Supervisor 32)	Cisco IOS 12.2(33)SXJ10	√	√	√	√	*X*	√	√	√
	Cisco IOS 12.2(33)SXI6	√	√	√	√	*X*	√	√	√
Catalyst 6848ia	Cisco IOS 152-1.SY1a	√	√	√	√	*X*	√	√	√
	Cisco IOS 15.1(2) SY+	√	√	√	√	*X*	√	√	√
Catalyst 9200	Cisco IOS XE 16.10.1 Cisco IOS XE 16.12.1 Cisco IOS XE 17.1.1 Cisco IOS XE 17.2.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.9.2	√	√	√	√	√	√	√	√
Catalyst 9200-H	Cisco IOS XE 16.10.1 Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.9.2	√	√	√	√	√	√	√	√
Catalyst 9200-L	Cisco IOS XE 16.10.1 Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.9.2	√	√	√	√	√	√	√	√

Device	Validated OS [1] Minimum OS [3]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
Catalyst 9300	Cisco IOS XE 16.6.2 ES Cisco IOS XE 16.8.1a Cisco IOS 16.9.1 Cisco IOS XE 16.12.1 Cisco IOS XE 17.1.1 Cisco IOS XE 17.2.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.6.2 ES	√	√	√	√	√	√	√	√
Catalyst 9300L Catalyst 9300 24H	Cisco IOS XE 16.12.1 Cisco IOS XE 17.1.1 Cisco IOS XE 17.2.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
Catalyst 9400 Catalyst 9400 LC Catalyst 9400 PoE	Cisco IOS XE 16.6.2 ES Cisco IOS XE 16.8.1a Cisco IOS XE 16.9.1 Cisco IOS XE 16.12.1 Cisco IOS XE 17.1.1 Cisco IOS XE 17.2.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.6.2 ES	√	√	√	√	√	√	√	√
Catalyst 9500	Cisco IOS XE 16.6.2 ES Cisco IOS XE 16.8.1a Cisco IOS XE 16.6.4	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.6.2 ES	√	√	√	√	√	√	√	√
Catalyst 9500H	Cisco IOS XE 16.12.1 Cisco IOS XE 17.1.1 Cisco IOS XE 17.2.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√

Device	Validated OS [1] / Minimum OS [3]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
Catalyst 9600 Catalyst 9600 LC	Cisco IOS XE 16.12.1 Cisco IOS XE 17.1.1 Cisco IOS XE 17.2.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
Latest Version	!	√	√	!	*X*	√	!	*X*	

1 Validated OS is the version tested for compatibility and stability.
2 See the Cisco TrustSec Product Bulletin for a complete list of Cisco TrustSec feature support.
3 Minimum OS is the version in which the features got introduced.
4 The IOS 12.x version does not fully support the Posture and Guest flows because of CSCsx97093. As a workaround, when you configure URL redirect in Cisco ISE, assign a value to "coa-skip-logical-profile."

Cisco ISE supports SNMP CoA for Cisco Catalyst switches. The following features are supported with SNMP CoA for Cisco Catalyst switches:

- Posture
- BYOD
- Guest

For information about the supported Catalyst platforms for device sensors, see https://communities.cisco.com/docs/DOC-72932.

Validated Third Party Access Switches

Table 3: Validated Third Party Access Switches

Device	Validated OS [5] / Minimum OS [7]	AAA	Profiling	BYOD	Guest	Posture	MDM	TrustSec [6]
Avaya ERS 2526T	4.4	√	!	*X*	*X*	*X*	*X*	*X*
	4.4	√	!	*X*	*X*	*X*	*X*	*X*
Brocade ICX 6610	8.0.20	√	√	√	√	√	*X*	*X*
	8.0.20	√	√	√	√	√	*X*	*X*
Extreme X440-48p	ExtremeXOS 15.5	√	*X*	√	√	√	*X*	*X*
	ExtremeXOS 15.5	√	*X*	√	√	√	*X*	*X*

Device	Validated OS [5] / Minimum OS [7]	AAA	Profiling	BYOD	Guest	Posture	MDM	TrustSec [6]
HP H3C	5.20.99	√	√	√	√	√	X	X
HP ProCurve	5.20.99	√	√	√	√	√	X	X
HP ProCurve 2900	WB.15.18.0007	√	√	√	√	√	X	X
	WB.15.18.0007	√	√	√	√	√	X	X
Juniper EX3300	12.3R11.2	√	√	√	√	√	X	X
	12.3R11.2	√	√	√	√	√	X	X

[5] Validated OS is the version tested for compatibility and stability.
[6] See the Cisco TrustSec Product Bulletin for a complete list of Cisco TrustSec feature support.
[7] Minimum OS is the version in which the features got introduced.

For more information on third-party device support, see https://communities.cisco.com/docs/DOC-64547

Validated Cisco Wireless LAN Controllers

Table 4: Validated Cisco Wireless LAN Controllers

Device	Validated OS [8]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [9]
WLC 2100	AireOS 7.0.252.0	!	√	X	!	X	X	X	X
	AireOS 7.0.116.0 (minimum)	!	√	X	!	X	X	X	X
WLC 2504	AirOS 8.5.120.0(ED)	√	√	√	√	√	√	√	√
WLC 3504	AirOS 8.5.105.0	√	√	√	√	√	√	√	Not validated
WLC 4400	AireOS 7.0.252.0	!	√	X	!	X	X	X	X
	AireOS 7.0.116.0 (minimum)	!	√	X	!	X	X	X	X
WLC 2500	AireOS 8.0.140.0	√	√	√	√	X	√	√	X
	AireOS 8.2.121.0	√	√	√	√	X	√	√	√
	AireOS 8.3.102.0	√	√	√	√	X	√	√	√
	AireOS 8.4.100.0	√	√	√	√	X	√	√	√
	AireOS 7.2.103.0 (minimum)	!	√	√	√	X	√	√	X

Device	Validated OS [8]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [9]
WLC 5508	AireOS 8.0.140.0	√	√	√	√	*X*	√	√	*X*
	AireOS 8.2.121.0	√	√	√	√	*X*	√	√	√
	AireOS 8.3.102.0	√	√	√	√	*X*	√	√	√
	AireOS 8.3.114.x	√	√	√	√	*X*	√	√	√
	AireOS 8.3.140.0	√	√	√	√	*X*	√	√	√
	AireOS 8.4.100.0	√	√	√	√	*X*	√	√	√
	AireOS 7.0.116.0 (minimum)	**!**	√	*X*	**!**	*X*	*X*	*X*	√
WLC 5520	AireOS 8.0.140.0	√	√	√	√	*X*	√	√	*X*
	AireOS 8.2.121.0	√	√	√	√	*X*	√	√	√
	AireOS 8.3.102.0	√	√	√	√	*X*	√	√	√
	AireOS 8.4.100.0	√	√	√	√	*X*	√	√	√
	AireOS 8.5.1.x	√	√	√	√	√	√	√	√
	AireOS 8.6.1.x	√	√	√	√	√	√	√	√
	AirOS 8.6.101.0(ED)	√	√	√	√	√	√	√	√
	AireOS 8.1.122.0 (minimum)	√	√	√	√	*X*	√	√	√
WLC 7500	AireOS 8.0.140.0	√	√	√	√	*X*	√	√	*X*
	AireOS 8.2.121.0	√	√	√	√	*X*	√	√	√
	AireOS 8.2.154.x	√	√	√	√	*X*	√	√	√
	AireOS 8.3.102.0	√	√	√	√	*X*	√	√	√
	AireOS 8.4.100.0	√	√	√	√	*X*	√	√	√
	AirOS 8.5.120.0(ED)	√	√	√	√	√	√	√	√
	AireOS 7.2.103.0 (minimum)	**!**	√	*X*	*X*	*X*	*X*	*X*	*X*
WLC 8540	AireOS 8.1.131.0	√	√	√	√	*X*	√	√	*X*
	AireOS 8.1.122.0 (minimum)	√	√	√	√	*X*	√	√	*X*

Device	Validated OS [8]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [9]
Catalyst 9800-CL	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	√	√	√	√	√	√	√	√
	IOS XE 16.10.1	√	√	√	√	√	√	√	√
Catalyst 9800-L	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	√	√	√	√	√	√	√	√
	IOS XE 16.10.1	√	√	√	√	√	√	√	√
Catalyst 9800-40	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	√	√	√	√	√	√	√	√
	IOS XE 16.10.1	√	√	√	√	√	√	√	√
Catalyst 9800-80	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	√	√	√	√	√	√	√	√
	IOS XE 16.10.1	√	√	√	√	√	√	√	√
Catalyst 9800 on Catalyst 9300	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	√	√	√	√	√	√	√	√
	IOS XE 16.10.1	√	√	√	√	√	√	√	√
vWLC	AireOS 8.0.135.0	√	√	√	√	X	√	√	X
	AireOS 7.4.121.0 (minimum)	√	√	√	√	X	√	√	X
WiSM1 6500	AireOS 7.0.252.0	!	√	X	!	X	X	X	X
	AireOS 7.0.116.0 (minimum)	!	√	X	!	X	X	X	X
WiSM2 6500	AireOS 8.0.135.0	√	√	√	√	X	√	√	√
	AireOS 7.2.103.0 (minimum)	!	√	√	√	X	√	√	√
WLC 5760	IOS XE 3.6.4	√	√	√	√	√	√	√	√
	IOS XE 3.3 (minimum)	√	√	√	√	X	√	√	√

Device	Validated OS [8]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [9]
WLC for ISR (ISR2 ISM, SRE700, and SRE900)	AireOS 7.0.116.0	!	√	X	!	X	X	X	X
	AireOS 7.0.116.0 (minimum)	!	√	X	!	X	X	X	X
Latest Version (minimum)	√	√	√	√	√	√	√	X	
Cisco Embedded Wireless Controller on Catalyst Access Point-C9117AXI	IOS XE 16.12.1	√	√	√	√	√	√	√	X
	IOS XE 16.12.1 IOS XE 17.1.1	√	√	√	√	√	√	√	X
Cisco Embedded Wireless Controller on Catalyst Access Point-C9115	IOS XE 16.12.1 IOS XE 17.1.1	√	√	√	√	√	√	√	X
	IOS XE 16.12.1	√	√	√	√	√	√	√	X

[8] Validated OS is the version tested for compatibility and stability.
[9] See the Cisco TrustSec Product Bulletin for a complete list of Cisco TrustSec feature support.

Refer to the Cisco Wireless Solutions Software Compatibility Matrix for a complete list of supported operating systems.

Note

- Some of the OS versions for Android, Apple, and Windows devices might require additional access to the ISE servers for CWA and BYOD flows post authentication. In such cases, you must allow access to the PSN in the post authentication ACL using the same TCP port where the portal is hosted.
- Due to CSCvi10594, IPv6 RADIUS CoA fails in AireOS Release 8.1 and later. As a workaround, you can use IPv4 RADIUS or downgrade Cisco Wireless LAN Controller to AireOS Release 8.0.
- Cisco Wireless LAN Controllers (WLCs) and Wireless Service Modules (WiSMs) do not support downloadable ACLs (dACLs), but support named ACLs. Autonomous AP deployments do not support endpoint posturing. Profiling services are supported for 802.1X-authenticated WLANs starting from WLC release 7.0.116.0 and for MAB-authenticated WLANs starting from WLC 7.2.110.0. FlexConnect, previously known as Hybrid Remote Edge Access Point (HREAP) mode, is supported with central authentication configuration deployment starting from WLC 7.2.110.0. For additional details regarding FlexConnect support, refer to the release notes for the applicable wireless controller platform.

Supported Cisco Access Points

Table 5: Supported Cisco Access Points

Cisco Access Point	Minimum Cisco Mobility Express Version	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec
Cisco Aironet 1540 Series	Cisco Mobility Express 8.7.106.0	√	*X*	√	√	*X*	*X*	*X*	*X*
Cisco Aironet 1560 Series	Cisco Mobility Express 8.7.106.0	√	*X*	√	√	*X*	*X*	*X*	*X*
Cisco Aironet 1815i	Cisco Mobility Express 8.7.106.0	√	*X*	√	√	*X*	*X*	*X*	*X*
Cisco Aironet 1815m	Cisco Mobility Express 8.7.106.0	√	*X*	√	√	*X*	*X*	*X*	*X*
Cisco Aironet 1815w	Cisco Mobility Express 8.7.106.0	√	*X*	√	√	*X*	*X*	*X*	*X*
Cisco Aironet 2800 Series	Cisco Mobility Express 8.7.106.0	√	*X*	√	√	*X*	*X*	*X*	*X*
Cisco Aironet 3800 Series	Cisco Mobility Express 8.7.106.0	√	*X*	√	√	*X*	*X*	*X*	*X*

Validated Third Party Wireless LAN Controllers

Table 6: Validated Third Party Wireless LAN Controllers

Device	Validated OS [10] Minimum OS [12]	AAA	Profiling	BYOD	Guest	Posture	MDM	TrustSec [11]
Aruba 3200[13] Aruba 3200XM Aruba 650	6.4	√	√	√	√	√	*X*	*X*
	6.4	√	√	√	√	√	*X*	*X*
	6.4	√	√	√	√	√	*X*	*X*
Aruba 7000 Aruba IAP	6.4.1.0	√	√	√	√	√	*X*	*X*
	6.4.1.0	√	√	√	√	√	*X*	*X*
Motorola RFS 4000	5.5	√	√	√	√	√	*X*	*X*
	5.5	√	√	√	√	√	*X*	*X*
HP 830	35073P5	√	√	√	√	√	*X*	*X*
	35073P5	√	√	√	√	√	*X*	*X*
Ruckus ZD1200	9.9.0.0	√	√	√	√	√	*X*	*X*
	9.9.0.0	√	√	√	√	√	*X*	*X*

[10] Validated OS is the version tested for compatibility and stability.
[11] See the Cisco TrustSec Product Bulletin for a complete list of Cisco TrustSec feature support.
[12] Minimum OS is the version in which the features got introduced.
[13] Aruba 3200 is supported for ISE 2.2 patch 2 and above.

For more information on third-party device support, see https://communities.cisco.com/docs/DOC-64547

Validated Cisco Routers

Table 7: Validated Cisco Routers

Device	Validated OS Minimum OS	AAA	Profiling	BYOD	Guest	Posture	MDM	TrustSec [14]
ISR 88x, 89x Series	IOS 15.3.2T(ED)	√	*X*	*X*	*X*	*X*	*X*	*X*
	IOS 15.2(2)T	√	*X*	*X*	*X*	*X*	*X*	*X*
ASR 1001-HX ASR 1001-X	IOS XE 17.1.1 IOS XE 17.2.1	√	*X*	*X*	*X*	*X*	*X*	√
ASR 1002-HX ASR 1002-X	IOS XE 17.1.1	√	*X*	*X*	*X*	*X*	*X*	√

Device	Validated OS Minimum OS	AAA	Profiling	BYOD	Guest	Posture	MDM	TrustSec [14]
ISR 19x, 29x, 39x Series	IOS 15.3.2T(ED)	√	!	X	!	X	X	√
	IOS 15.2(2)T	√	!	X	!	X	X	√
CE 9331	IOS XE 17.1.1	√	X	X	X	X	X	√
	IOS XE 17.1.1	√	X	X	X	X	X	√
CGR 2010	IOS 15.3.2T(ED)	√	!	X	!	X	X	√
	IOS 15.3.2T(ED)	√	!	X	!	X	X	√
4451-XSM-X L2/L3 Ethermodule	IOS XE 3.11	√	√	√	√	√	√	√
	IOS XE 3.11	√	√	√	√	√	√	√

[14] See the Cisco TrustSec Product Bulletin for a complete list of Cisco TrustSec feature support.

Note For CoA to function properly, the minimum IOS version required for Cisco ISR series to work with SM-X-40G8M2X and SM-X-16G4M2X modules is IOS XE 17.4.1.

Validated Cisco Remote Access

Table 8: Validated Cisco Remote Access

Device	Validated OS [15] Minimum OS [17]	AAA	Profiling	BYOD	Guest	Posture	MDM	TrustSec [16]
ASA 5500, ASA 5500-X (Remote Access Only)	ASA 9.2.1	NA	NA	√	NA	√	X	√
	ASA 9.1.5	NA	NA	X	NA	X	X	X

[15] Validated OS is the version tested for compatibility and stability.
[16] See the Cisco TrustSec Product Bulletin for a complete list of Cisco TrustSec feature support.
[17] Minimum OS is the version in which the features got introduced.

Validated Cisco Meraki Devices

Table 9: Cisco Meraki Access Control Capabilities with ISE

Model	802.1X	MAB	VLAN	GPACL	Adaptive Policy	URL Redirect	CoA	Profiling
Wireless								

Model	802.1X	MAB	VLAN	GPACL	Adaptive Policy	URL Redirect	CoA	Profiling
MR20, MR70, MR28, MR78	√	√	√	√	*X*	√	√	*X*
MR30H, MR36, MR42/E, MR44, MR45, MR46/E, MR52, MR53E, MR56, MR74, MR76, MR86	√	√	√	√	√	√	√	*X*
Teleworker								
Z3/C	√	√	*X*	*X*	√ Transport MX18.1+	*X*	*X*	*X*
Switching								
MS120, MS125	√	√	√	*X*	*X*	*X*	√	CDP+LLDP
MS210, MS225, MS250	√	√	√	√	*X*	√	√	CDP+LLDP
MS350, MS355	√	√	√	√	*X*	√	√	CDP+LLDP
MS390	√	√	√	√	√	√	√	Full Device Sensor CDP LLDP DHCP HTTP
MS410, MS425, MS450 (aggregation)	√	√	√	√	*X*	√	√	CDP+LLDP
Security and SD-WAN								

Model	802.1X	MAB	VLAN	GPACL	Adaptive Policy	URL Redirect	CoA	Profiling
MX64/W, MX67/C/W, MX68/CW/W, MX75, MX84, MX85, MX95, MX100, MX105, MX250, MX450	√ 802.1X or MAB	√ 802.1X or MAB	*X*	*X*	√ Transport MX18.1+	*X*	*X*	*X*

AAA Attributes for RADIUS Proxy Service

For RADIUS proxy service, the following authentication, authorization, and accounting (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, the following authentication, authorization, and accounting (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.

Validated External Identity Sources

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

Table 10: Validated External Identity Sources

External Identity Source	Version
Active Directory [18] [19]	
Microsoft Windows Active Directory 2012	Windows Server 2012
Microsoft Windows Active Directory 2012 R2 [20]	Windows Server 2012 R2
Microsoft Windows Active Directory 2016	Windows Server 2016
Microsoft Windows Active Directory 2019 [21]	Windows Server 2019
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
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	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

External Identity Source	Version
Open Database Connectivity (ODBC) Identity Source	
Microsoft SQL Server	Microsoft SQL Server 2012
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

[18] Cisco ISE OCSP functionality is available only on Microsoft Windows Active Directory 2008 and later.

[19] You can only add up to 200 Domain Controllers on Cisco ISE. On exceeding the limit, you will receive the following error:

```
Error creating <DC FQDN> - Number of DCs Exceeds allowed maximum of 200
```

[20] 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 Protective User Groups, are not supported.

[21] Cisco ISE 2.6 Patch 4 and later support all the legacy features in Microsoft Windows Active Directory 2019.

See the *Cisco Identity Services Engine Administrator Guide* for more information.

Validated MDM Servers

Validated Mobile Device Management (MDM) servers include products from the following vendors:

- Absolute
- VMware AirWatch
- Citrix XenMobile
- Globo
- Good Technology
- IBM MaaS360
- JAMF Software
- Meraki SM/EMM
- MobileIron
- SAP Afaria
- SOTI
- Symantec
- Tangoe

- Microsoft Intune - for mobile devices
- Microsoft SCCM - for desktop devices

Supported Browsers for the Admin Portal

- Mozilla Firefox 96 and earlier versions from version 82
- Mozilla Firefox ESR 91.3 and earlier versions
- Google Chrome 97 and earlier versions from version 86
- Microsoft Internet Explorer 11.x
- Microsoft Edge, the latest version and one version earlier than the latest version

Supported Hardware

Cisco ISE, Release 2.6, can be installed on the following platforms:

Caution For Cisco Secure Network Server (SNS) 3600 series appliance support (SNS-3615-K9, SNS-3655-K9, and SNS-3695-K9), you must use only the new ISO file (ise-2.4.0.357.SPA.x86_64_SNS-36x5_APPLIANCE_ONLY.iso). Cisco ISE 2.4 Patch 9 or above must be applied after installation. We recommend that you do not use this ISO file for SNS 3500 series appliance, VMware, KVM, or Hyper-V installation.

Table 11: Supported Platforms

Hardware Platform	Configuration
Cisco SNS-3515-K9 (small)	For appliance hardware specifications, see the *Cisco Secure Network Server Appliance Hardware Installation Guide*.
Cisco SNS-3595-K9 (large)	
Cisco SNS-3615-K9 (small)	
Cisco SNS-3655-K9 (medium)	
Cisco SNS-3695-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 3.1 and later releases do not support Cisco Secured Network Server (SNS) 3515 appliance.
- Cisco SNS 3400 Series appliances are not supported in Cisco ISE, Release 2.4, and later.
- 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.

Validated Virtual Environments

Cisco ISE supports the following virtual environment platforms:

- VMware ESXi 5.x (5.1 U2 and later support RHEL 7), 6.x,

Note If you are installing or upgrading Cisco ISE on an ESXi 5.x server, update the VMware hardware version to 9 or later to support RHEL 7 as the Guest OS. RHEL 7 is supported with VMware hardware Version 9 and later.

- KVM on RHEL 7.1, 7.3, and 7.5
- Microsoft Hyper-V on Microsoft Windows Server 2012 R2 and later

Caution Cisco ISE does not support VMware snapshots for backing up ISE data because a VMware snapshot saves the status of a VM at a given point in time. In a multi-node Cisco ISE deployment, data in all the nodes are continuously synchronized with current database information. Restoring a snapshot might cause database replication and synchronization issues. We recommend that you use the backup functionality included in Cisco ISE for archival and restoration of data.

Using VMware snapshots to back up ISE data results in stopping Cisco ISE services. A reboot is required to bring up the ISE node.

Validated Cisco Digital Network Architecture Center Release

Table 12: Validated Cisco Digital Network Architecture Center Release

Validated Cisco DNA Center Version	Validated Cisco ISE Release
1.2.12.0	Cisco ISE 2.7
1.3.0.0	Cisco ISE 2.7
1.3.0.6	Cisco ISE 3.0

Validated Cisco DNA Center Version	Validated Cisco ISE Release
1.3.1.0	Cisco ISE 2.4 patch 9, patch 11 Cisco ISE 2.6 patch 2 Cisco ISE 2.7
1.3.1.4	Cisco ISE 2.4 patch 12 Cisco ISE 2.6 patch 6 Cisco ISE 2.7 patch 2 Cisco ISE 3.0
1.3.2.0	Cisco ISE 2.4 patch 10, patch 11 Cisco ISE 2.7
1.3.3.0	Cisco ISE 2.7 patch 1 Cisco ISE 3.0
1.3.3.4	Cisco ISE 2.6 patch 6
1.3.3.5	Cisco ISE 2.4 patch 13 Cisco ISE 2.7 patch 2
2.1.1.0	Cisco ISE 2.4 patch 12 Cisco ISE 2.6 patch 6, patch 7 Cisco ISE 2.7 patch 1, patch 2 Cisco ISE 3.0
2.1.1.1	Cisco ISE 3.0
2.1.2.0	Cisco ISE 2.4 patch 12, patch 13 Cisco ISE 2.6 patch 6, patch 8 Cisco ISE 2.7 patch 1, patch 3 Cisco ISE 3.0
2.1.2.4	Cisco ISE 3.0 patch 1
2.1.2.5	Cisco ISE 3.0 patch 1, patch 2
2.1.2.6	Cisco ISE 2.4 patch 14 Cisco ISE 2.7 patch 4
2.2.1.0	Cisco ISE 2.4 patch 13, patch 14 Cisco ISE 2.6 patch 7, patch 8, patch 9 Cisco ISE 2.7 patch 2 Cisco ISE 3.0 patch 1, patch 3

Validated Cisco DNA Center Version	Validated Cisco ISE Release
2.2.2.0	Cisco ISE 2.4 patch 14 Cisco ISE 2.6 patch 8, patch 9 Cisco ISE 2.7 patch 2, patch 3, patch 4 Cisco ISE 3.0 patch 1

For more information about Cisco ISE compatibility with Cisco Digital Network Architecture Center (Cisco DNA Center), see Cisco SD-Access Compatibility Matrix.

Validated Cisco Mobility Services Engine Release

Cisco ISE integrates with Cisco Mobility Services Engine (MSE), Release 8.0.110.0 to provide Location Service (also known as Context Aware Service). This service allows you to track the location of wireless devices.

For information on how to integrate Cisco ISE with Cisco MSE, refer to:

- Location based authorization with Mobility Services Engine (MSE) and Identity Services Engine (ISE) 2.0
- *Cisco Identity Services Engine Administrator Guide*

Validated Cisco Prime Infrastructure Release

Cisco Prime Infrastructure, Release 3.6 or above can be integrated with Cisco ISE 2.6 to leverage the monitoring and reporting capabilities of Cisco ISE.

Validated Cisco Stealthwatch Release

Cisco ISE has been validated with Cisco Stealthwatch, Release 6.9.

Support for Threat Centric NAC

Cisco ISE is validated with the following 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)

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

The following client machine types have been validated for Bring Your Own Device (BYOD) and Posture workflows:

- Apple iOS

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

Cisco ISE, Release 2.3 and later support only the Cisco AnyConnect and Cisco Temporal Agents.

All standard 802.1X supplicants can be used with Cisco ISE, Release 2.4 and above 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.

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.

The following Google Android versions have been validated with Cisco ISE:

- Google Android 12.x
- Google Android 11.x
- Google Android 10.x
- Google Android 9.x
- Google Android 8.x
- Google Android 7.x

The following Android devices have been validated with Cisco ISE. See the section for the list of devices for which BYOD flow is supported in Cisco ISE.

Table 13: Validated Android Devices

Device Model	Android Version
Google Pixel 3	10
OnePlus 6	10
Samsung S9	9
Google Nexus 6P	8.1

Device Model	Android Version
Huawei Mate Pro 10	8

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 (under **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.

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.

The following Apple iOS versions have been validated with Cisco ISE:

- Apple iOS 16.x
- Apple iOS 15.x
- Apple iOS 14.x
- Apple iOS 13.x
- Apple iOS 12.x
- Apple iOS 11.x

The following iPhone/iPad devices have been validated with Cisco ISE. See the section for the list of devices for which BYOD flow is supported in Cisco ISE.

Table 14: Validated iPhone/iPad Devices

Device Model	iOS Version
iPhone X	iOS 13
iPhone 8	iOS 12.3
iPhone 7	iOS 13.2
iPhone 6	iOS 12.6
iPhone 5s	iOS 12, iOS 10.3
iPad	iPad OS 13.1

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**.
- 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. However, you do not have to do this for Cisco ISE 2.6 and later releases because the SAN value is selected with DNS Name as default.
- 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

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

Table 15: Apple macOS

Client Machine Operating System	AnyConnect
Apple macOS 13	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. It has been verified with Cisco ISE 2.4 patch 12, Cisco ISE 2.6 patch 8, Cisco ISE 2.7 patch 3, and Cisco ISE 3.0 patch 2.

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.

Microsoft Windows

Table 16: Microsoft Windows

Client Machine Operating System	Supplicants (802.1X)	Cisco Temporal Agent	AnyConnect[22]
Microsoft Windows 11			
• 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	4.10.04065 or later
Microsoft Windows 10			

Client Machine Operating System	Supplicants (802.1X)	Cisco Temporal Agent	AnyConnect[22]
• 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	4.8.01090 or later

[22] 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:

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 17: Google Chromebook

Client Machine Operating System	Web Browser	Cisco ISE
Google Chromebook	Google Chrome version 49 or later	Cisco ISE 2.4 Patch 8

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.

Other Operating Systems

Table 18: Other Operating Systems

Client Machine Operating System	Web Browser [23]	Supplicants (802.1X)
Red Hat Enterprise Linux (RHEL)	• Google Chrome • Mozilla Firefox	Not tested extensively [24]

[23] Google Chrome does not support 32-bit Linux systems.

[24] The support for 802.1X has not been tested extensively by Cisco, but any 802.1X supplicant is supported as long as it is compliant with the IEEE 802.1X standards.

Validated Operating Systems and Browsers for Sponsor, Guest, and My Devices Portals

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

Table 19: Validated Operating Systems and Browsers

Supported Operating System[25]	Browser Versions
Google Android[26] 12.x, 11.x, 10.x, 9.x, 8.x, 7.x	• Native browser • Mozilla Firefox • Google Chrome
Apple iOS 16.x, 15.x, 14.x, 13.x, 12.x, 11.x	• Safari
Apple macOS 13, 12.6, 12.5, 11.6, 10.15, 10.14, 10.13	• Mozilla Firefox • Safari • Google Chrome
Microsoft Windows 10	• Microsoft IE 11.x • Mozilla Firefox • Google Chrome

[25] The latest two officially-released browser versions are supported for all operating systems except Microsoft Windows; refer to Table 14 for the supported Internet Explorer versions.

[26] 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 On-Boarding 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 (**Administration > System > Settings > Posture > Updates**) and click **Update Now**.

Table 20: BYOD On-Boarding and Certificate Provisioning - Validated Devices and Operating Systems

Device	Operating System	Single SSID	Dual SSID (open > PEAP (no cert) or open > TLS)	Onboard Method
Apple iDevice	Apple iOS 16.x, 15.x, 14.x, 13.x, 12.x, 11.x Apple iPad OS 13.x	Yes	Yes[27]	Apple profile configurations (native)
Google Android	12.x, 11.x, 10.x, 9.x, 8.x, 7.x	Yes[28]	Yes	Cisco Network Setup Assistant

Device	Operating System	Single SSID	Dual SSID (open > PEAP (no cert) or open > TLS)	Onboard Method
Barnes & Noble Nook (Android) HD/HD+[29]	—	—	—	—
Windows	Windows 10 Microsoft Windows 10 Version 2004 (OS build 19041.1) and higher is required for EAP TEAP.	Yes[30]	Yes	2.2.1.53 or later
Windows	Mobile 8, Mobile RT, Surface 8, and Surface RT	No	No	—
Apple macOS	Apple macOS 13, 12.6, 12.5, 11.6, 10.15, 10.14, 10.13	Yes	Yes	2.2.1.43 or later

[27] Connect to secure SSID after provisioning.

[28] You cannot modify the system-created SSIDs using the Cisco supplicant provisioning wizard (SPW), if you 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.

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

[30] 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.

Supported Protocol Standards, RFCs, and IETF Drafts

Cisco ISE conforms to the following 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

The following 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

Validated OpenSSL Version

Cisco ISE is validated with OpenSSL 1.0.2.x (CiscoSSL 6.0).

Supported Cipher Suites

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

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

- secp256r1
- secp384r1
- secp521r1

The following 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. To view this window, 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 Allow TLS 1.1 option is disabled by default in Cisco ISE 2.3 and above. TLS 1.1 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 1.1, check the Allow TLS 1.1 check box in the Security Settings window(Administration > System > Settings > Protocols > Security Settings).	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

Requirements for CA to Interoperate with Cisco ISE

While using a CA server with Cisco ISE, make sure that the following requirements are met:

- Key size should be 1024, 2048, or higher. In CA server, the key size is defined using certificate template. You can define the key size on Cisco ISE using the supplicant profile.
- Key usage should allow signing and encryption in extension.
- While using GetCACapabilities through the SCEP protocol, cryptography algorithm and request hash should be supported. It is recommended to use RSA and SHA1.
- Online Certificate Status Protocol (OCSP) is supported. This is not directly used in BYOD, but a CA which can act as an OCSP server can be used for certificate revocation.

Note Enterprise Java Beans Certificate Authority (EJBCA) is not supported by Cisco ISE for proxy SCEP. EJBCA is supported by Cisco ISE for standard EAP authentication like PEAP, EAP-TLS, and so on.

- If you use an enterprise PKI to issue certificates for Apple iOS devices, ensure that you configure key usage in the SCEP template and enable the **Key Encipherment** option.

  If you use Microsoft CA, edit the Key Usage Extension in the certificate template. In the **Encryption** area, click the **Allow Key Exchange only with Key Encryption (Key encipherment)** radio button and check the **Allow Encryption of User Data** check box.
- Cisco ISE supports the use of RSASSA-PSS algorithm for trusted certificates and endpoint certificates for EAP-TLS authentication. When you view the certificate, the signature algorithm is listed as 1.2.840.113549.1.1.10 instead of the algorithm name.

Note If you use the Cisco ISE internal CA for the BYOD flow, the Admin certificate should not be signed using the RSASSA-PSS algorithm (by an external CA). The Cisco ISE internal CA cannot verify an Admin certificate that is signed using this algorithm and the request would fail.

Client Certificate Requirements for Certificate-Based Authentication

For certificate-based authentication with Cisco ISE, the client certificate should meet the following requirements:

Table 21: Client-Certificate Requirements for RSA and ECC

RSA		
Supported Key Sizes	1024, 2048, and 4096 bits	
Supported Secure Hash Algorithms (SHA)	SHA-1 and SHA-2 (includes SHA-256)	
ECC [31] [32]		
Supported Curve Types	P-192, P-256, P-384, and P-521	
Supported Secure Hash Algorithm (SHA)	SHA-256	
Client Machine Operating Systems and Supported Curve Types		
Windows	8 and later	P-256, P-384, and P-521

Android	4.4 and later **Note** Android 6.0 requires May 2016 patch to support ECC certificates.	All curve types (except Androidv6.0, which does not support the P-192 curve type).

[31] Windows 7 and Apple iOS do not natively support ECC for EAP-TLS authentication.
[32] This release of Cisco ISE does not support the use of ECC certificates on MAC OS X devices.

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.