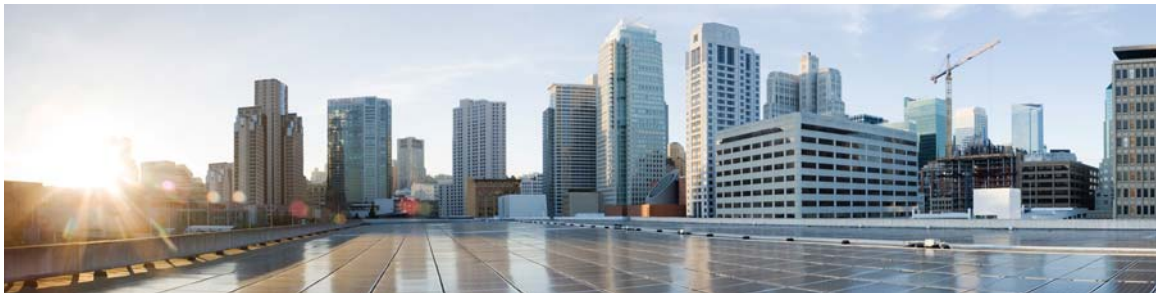

Cisco Identity Services Engine Network Component Compatibility, Release 2.2

Revised: February 12, 2021

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

This document describes Cisco Identity Services Engine (ISE) validated compatibility with switches, wireless LAN controllers, and other policy enforcement devices as well as operating systems with which Cisco ISE interoperates.

Cisco Systems, Inc.
www.cisco.com

Validated Network Access Devices

Cisco ISE supports interoperability with any Cisco or non-Cisco RADIUS client network access device (NAD) that implements common RADIUS behavior (similar to Cisco IOS 12.x) for standards-based authentication. For a list of supported authentication methods, see the "Manage Authentication Policies" chapter of the *Cisco Identity Services Engine Admin Guide, Release 2.2*.

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.

RFC Standards

Cisco ISE conforms to the following RFCs:

- *RFC 2138—Remote Authentication Dial In User Service (RADIUS)*
- *RFC 2139—RADIUS Accounting*
- *RFC 2865—Remote Authentication Dial In User Service (RADIUS)*
- *RFC 2866—RADIUS Accounting*
- *RFC 2867—RADIUS Accounting Modifications for Tunnel Protocol Support*
- *RFC 5176—Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*

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.

Note 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.

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 Admin Guide, Release 2.2*.

For information about third-party NAD profiles, see the ISE Community Resources.

Note Some switch models and IOS versions may have reached the end-of-life date and interoperability may not be supported by Cisco TAC.

Caution To support the Cisco ISE profiling service, use the latest version of NetFlow, which has additional functionality that is needed to operate the profiler. If you use NetFlow version 5, then you can use version 5 only on the primary NAD at the access layer, as it will not work anywhere else.

For Wireless LAN Controllers, note the following:

- MAB supports MAC filtering with RADIUS lookup.
- Support for session ID and COA with MAC filtering provides MAB-like functionality.
- DNS based ACL feature will be supported in WLC 8.0. Not all Access Points support DNS based ACL. Refer to Cisco Access Points Release Notes for more details.

The following tables list the support for the devices as follows:

- ***✓*** — Fully supported
- ***✗*** — Not supported
- **!** — Limited support, some functionalities are not supported

The following are the functionalities supported by each feature:

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

This section lists the following:

Table 1 Validated Cisco Access Switches

Device	Validated OS[1] Minimum OS [3]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
IE2000 IE3000	IOS 15.2(2)E4	✓	✓	✓	✓	✓	✓	✓	✗
	IOS 15.0(2)EB	✓	✓	✓	✓	✗	✓	✓	✗
IE4000 IE5000	IOS 15.2(2)E5 IOS 15.2(4)E2	✓	✓	✓	✓	✓	✓	✓	✓
	IOS 15.0.2A-EX5	✓	✓	✓	✓	✓	✓	✓	✓
IE4010	IOS 15.2(2)E5 IOS 15.2(4)E2	✓	✓	✓	✓	✓	✓	✓	✓
	IOS 15.0.2A-EX5	✓	✓	✓	✓	✓	✓	✓	✓
CGS 2520	IOS 15.2(3)E3	✓	✓	✓	✓	✗	✓	✓	✓
	IOS 15.2(3)E3	✓	✓	✓	✓	✗	✓	✓	✓
Catalyst 2960 LAN Base	IOS 12.2(55)SE10	✓	✓	✓	✓	✗	✓	✓	✗
	IOS v12.2(55)SE5	✓	✓	✓	✓	✗	✓	✓	✗
Catalyst 2960-C	IOS 15.2(2)E4	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 3560-C	IOS 12.2(55)EX3	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 2960-Plus Catalyst 2960-SF	IOS 15.2(2)E4	✓	✓	✓	✓	✓	✓	✓	✓
	IOS 15.0(2)SE7	✓	✓	✓	✓	✓	✓	✓	✗
Catalyst 2960-S	IOS 15.0.2-SE10a	✓	✓	✓	✓	✓	✓	✓	✗
	IOS 12.2.(55)SE5	✓	✓	✓	✓	✓	✓	✓	✗
Catalyst 2960–XR Catalyst 2960–X	IOS 15.2(2)E5 IOS 15.2(4)E2	✓	✓	✓	✓	✓	✓	✓	✓
	IOS 15.0.2A-EX5	✓	✓	✓	✓	✓	✓	✓	✗
Catalyst 2960-CX Catalyst 3560-CX	IOS 15.2(3)E1	✓	✓	✓	✓	✓	✓	✓	✓
	IOS 15.2(3)E	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 3560-G Catalyst 3750-G	IOS 12.2(55)SE10	✓	✓	✓	✓	✓	✓	✓	✓
	IOS 12.2(55)SE5	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 3560V2 Catalyst 3750V2	IOS 12.2(55)SE10	✓	✓	✓	✓	✓	✓	✓	✓
	IOS 12.2(55)SE5	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 3560-E Catalyst 3750-E	IOS 15.0(2)SE11	✓	✓	✓	✓	✓	✓	✓	✓
	IOS 12.2(55)SE5	✓	✓	✓	✓	✓	✓	✓	✓

Table 1 Validated Cisco Access Switches (continued)

Device	Validated OS[1] Minimum OS[3]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec[2]
Catalyst 3560-X	IOS 15.2(2)E5	✓	✓	✓	✓	✓	✓	✓	✓
	IOS 12.2(55)SE5	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 3650	IOS XE 16.3.3 IOS XE 3.6.5E IOS XE 16.12.1	✓	✓	✓	✓	✓	✓	✓	✓
	IOS XE 3.3.5.SE	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 3750-X	IOS 15.2(2)E5 IOS 15.2(4)E2	✓	✓	✓	✓	✓	✓	✓	✓
	IOS 12.2(55)SE5	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 3850	IOS XE 16.3.3 IOS XE 3.6.5E IOS XE 16.12.1	✓	✓	✓	✓	✓	✓	✓	✓
	IOS XE 3.3.5.SE	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 4500-X	IOS 15.2(2)E5 IOS 15.2(4)E2	✓	✓	✓	✓	✓	✓	✓	✓
	IOS XE 3.4.4 SG	✓	✓	✓	✓	✗	✓	✓	✓
Catalyst 4500 Supervisor 7-E, 7L-E	IOS XE 3.6.4	✓	✓	✓	✓	✓	✓	✓	✓
	IOS XE 3.4.4 SG	✓	✓	✓	✓	✗	✓	✓	✓
Catalyst 4500 Supervisor 6-E, 6L-E	IOS 15.2(2)E4	✓	✓	✓	✓	✗	✓	✓	✓
	IOS 15.2(2)E	✓	✓	✓	✓	✗	✓	✓	✓
Catalyst 4500 Supervisor 8-E	IOS XE 3.6.4	✓	✓	✓	✓	✗	✓	✓	✓
	IOS XE 3.3.2 XO	✓	✓	✓	✓	✗	✓	✓	✓
Catalyst 5760	IOS XE 3.7.4	✓	✓	✓	✓	✗	✓	✓	✓
	—	—	—	—	—	—	—	—	—
Catalyst 6500-E (Supervisor 32)	IOS 12.2(33)SXJ10	✓	✓	✓	✓	✗	✓	✓	✓
	IOS 12.2(33)SXI6	✓	✓	✓	✓	✗	✓	✓	✓
Catalyst 6500-E (Supervisor 720)	IOS 15.1(2)SY7	✓	✓	✓	✓	✗	✓	✓	✓
	IOS v12.2(33)SXI6	✓	✓	✓	✓	✗	✓	✓	✓
Catalyst 6500-E (VS-S2T-10G)	IOS 152-1.SY1a	✓	✓	✓	✓	✗	✓	✓	✓
	IOS 15.0(1)SY1	✓	✓	✓	✓	✗	✓	✓	✓
Catalyst 6807-XL Catalyst 6880-X (VS-S2T-10G)	IOS 152-1.SY1a	✓	✓	✓	✓	✗	✓	✓	✓
	IOS 15.0(1)SY1	✓	✓	✓	✓	✗	✓	✓	✓

Table 1 Validated Cisco Access Switches (continued)

Device	Validated OS[1] / Minimum OS [3]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
Catalyst 6500-E (Supervisor 32)	IOS 12.2(33)SXJ10	✓	✓	✓	✓	✗	✓	✓	✓
	IOS 12.2(33)SXI6	✓	✓	✓	✓	✗	✓	✓	✓
Catalyst 6848ia	IOS 152-1.SY1a	✓	✓	✓	✓	✗	✓	✓	✓
	IOS 15.1(2) SY+	✓	✓	✓	✓	✗	✓	✓	✓
Catalyst 9200	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	✓	✓	✓	✓	✓	✓	✓	✓
	IOS XE 16.12.1	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 9300[4]	IOS XE 16.11.1 IOS 16.6.2 ES IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	✓	✓	✓	✓	✓	✓	✓	✓
	IOS 16.6.2 ES	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 9300L Catalyst 9300 24H	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	✓	✓	✓	✓	✓	✓	✓	✓
	IOS XE 16.12.1	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 9400[4] Catalyst 9400 LC Catalyst 9400 PoE	IOS XE 16.11.1 IOS 16.6.2 ES IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	✓	✓	✓	✓	✓	✓	✓	✓
	IOS 16.6.2 ES	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 9500[4]	IOS 16.6.2 ES	✓	✓	✓	✓	✓	✓	✓	✓
	IOS 16.6.2 ES	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 9500H	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	✓	✓	✓	✓	✓	✓	✓	✓
	IOS XE 16.12.1	✓	✓	✓	✓	✓	✓	✓	✓

Table 1 Validated Cisco Access Switches (continued)

Device	Validated OS[1] Minimum OS [3]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
Catalyst 9600 Catalyst 9600 LC	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	✓	✓	✓	✓	✓	✓	✓	✓
	IOS XE 16.12.1	✓	✓	✓	✓	✓	✓	✓	✓
Meraki MS Platforms	Latest Version	✓	✓	✗	!	✗	✗	✗	✗
	Latest Version	✓	✓	✗	!	✗	✗	✗	✗

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. Catalyst 9000 Series Switches are validated with Cisco ISE, Release 2.2 Patch 4.

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

Table 2 Validated Third Party Access Switches

Device	Validated OS[1] Minimum OS [3]	AAA	Profiling	BYOD	Guest	Posture	MDM	TrustSec[2]
Third Party Access Switches								
Avaya ERS 2526T	4.4	✓	!	✗	✗	✗	✗	✗
	4.4	✓	!	✗	✗	✗	✗	✗
Brocade ICX 6610	8.0.20	✓	✓	✓	✓	✓	✗	✗
	8.0.20	✓	✓	✓	✓	✓	✗	✗
HP H3C	5.20.99	✓	✓	✓	✓	✓	✗	✗
HP ProCurve	5.20.99	✓	✓	✓	✓	✓	✗	✗
HP ProCurve 2900	WB.15.18.0007	✓	✓	✓	✓	✓	✗	✗
	WB.15.18.0007	✓	✓	✓	✓	✓	✗	✗
Juniper EX3300	12.3R11.2	✓	✓	✓	✓	✓	✗	✗
	12.3R11.2	✓	✓	✓	✓	✓	✗	✗

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.

Table 3 Validated Cisco Wireless LAN Controllers

Device	Validated OS[1]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
Cisco Wireless LAN Controllers [3] Refer to the Cisco Wireless Solutions Software Compatibility Matrix for a complete list of supported operating systems.									
WLC 2100	AireOS 7.0.252.0	!	✓	✗	!	✗	✗	✗	✗
	AireOS 7.0.116.0 (minimum)	!	✓	✗	!	✗	✗	✗	✗
WLC 3504	AireOS 8.5.105.0	✓	✓	✓	✓	✓	✓	✓	Not validated
WLC 4400	AireOS 7.0.252.0	!	✓	✗	!	✗	✗	✗	✗
	AireOS 7.0.116.0 (minimum)	!	✓	✗	!	✗	✗	✗	✗
WLC 2500	AireOS 8.0.140.0	✓	✓	✓	✓	✗	✓	✓	✗
	AireOS 8.2.121.0	✓	✓	✓	✓	✗	✓	✓	✓
	AireOS 8.3.102.0	✓	✓	✓	✓	✗	✓	✓	✓
	AireOS 8.4.100.0	✓	✓	✓	✓	✗	✓	✓	✓
	AireOS 7.2.103.0 (minimum)	!	✓	✓	✓	✗	✓	✓	✗
WLC 5508	AireOS 8.0.140.0	✓	✓	✓	✓	✗	✓	✓	✗
	AireOS 8.2.121.0	✓	✓	✓	✓	✗	✓	✓	✓
	AireOS 8.3.102.0	✓	✓	✓	✓	✗	✓	✓	✓
	AireOS 8.4.100.0	✓	✓	✓	✓	✗	✓	✓	✓
	AireOS 7.0.116.0 (minimum)	!	✓	✗	!	✗	✗	✗	✓
WLC 5520	AireOS 8.0.140.0	✓	✓	✓	✓	✗	✓	✓	✗
	AireOS 8.2.121.0	✓	✓	✓	✓	✗	✓	✓	✓
	AireOS 8.3.102.0	✓	✓	✓	✓	✗	✓	✓	✓
	AireOS 8.4.100.0	✓	✓	✓	✓	✗	✓	✓	✓
	AireOS 8.1.122.0 (minimum)	✓	✓	✓	✓	✗	✓	✓	✓
WLC 7500	AireOS 8.0.140.0	✓	✓	✓	✓	✗	✓	✓	✗
	AireOS 8.2.121.0	✓	✓	✓	✓	✗	✓	✓	✓
	AireOS 8.3.102.0	✓	✓	✓	✓	✗	✓	✓	✓
	AireOS 8.4.100.0	✓	✓	✓	✓	✗	✓	✓	✓
	AireOS 7.2.103.0 (minimum)	!	✓	✗	✗	✗	✗	✗	✗

Table 3 Validated Cisco Wireless LAN Controllers

Device	Validated OS[1]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
WLC 8510	AireOS 8.6.1.x	✓	✓	✓	✓	✓	✓	✓	✓
	AireOS 8.0.135.0	✓	✓	✓	✓	✗	✓	✓	✗
	AireOS 7.4.121.0 (minimum)	✓	✓	✗	✗	✗	✗	✓	✗
WLC 8540	AireOS 8.1.131.0	✓	✓	✓	✓	✗	✓	✓	✗
	AireOS 8.1.122.0 (minimum)	✓	✓	✓	✓	✗	✓	✓	✗
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	✓	✓	✓	✓	✗	✓	✓	✗
	AireOS 7.4.121.0 (minimum)	✓	✓	✓	✓	✗	✓	✓	✗
WiSM1 6500	AireOS 7.0.252.0	!	✓	✗	!	✗	✗	✗	✗
	AireOS 7.0.116.0 (minimum)	!	✓	✗	!	✗	✗	✗	✗

Table 3 Validated Cisco Wireless LAN Controllers

Device	Validated OS[1]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
WiSM2 6500	AireOS 8.0.135.0	✓	✓	✓	✓	✗	✓	✓	✓
	AireOS 7.2.103.0 (minimum)	!	✓	✓	✓	✗	✓	✓	✓
WLC 5760	IOS XE 3.6.4	✓	✓	✓	✓	✓	✓	✓	✓
	IOS XE 3.3 (minimum)	✓	✓	✓	✓	✗	✓	✓	✓
WLC for ISR (ISR2 ISM, SRE700, and SRE900)	AireOS 7.0.116.0	!	✓	✗	!	✗	✗	✗	✗
	AireOS 7.0.116.0 (minimum)	!	✓	✗	!	✗	✗	✗	✗
Meraki MR Platforms	Public Beta	✓	✓	✓	✓	✗	✓	✓	✗
	Latest Version (minimum)	✓	!	✗	!	✗	✗	✗	✗
Cisco Embedded Wireless Controller on Catalyst Access Point-C9117A XI	IOS XE 16.12.1 IOS XE 17.1.1	✓	✓	✓	✓	✓	✓	✓	✗
	IOS XE 16.12.1	✓	✓	✓	✓	✓	✓	✓	✗
Cisco Embedded Wireless Controller on Catalyst Access Point-C9115	IOS XE 16.12.1 IOS XE 17.1.1	✓	✓	✓	✓	✓	✓	✓	✗
	IOS XE 16.12.1	✓	✓	✓	✓	✓	✓	✓	✗
WLC 9800	IOS XE 16.12.1	✓	✓	✓	✓	✓	✓	✓	✗
	IOS XE 16.12.1	✓	✓	✓	✓	✓	✓	✓	✗

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. 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.

Table 4 Validated Third Party Wireless LAN Controllers

Device	Validated OS[1] / Minimum OS[3]	AAA	Profiling	BYOD	Guest	Posture	MDM	TrustSec[2]
Third Party Wireless LAN Controllers								
Aruba 3200[4]	6.4	✓	✓	✓	✓	✓	✗	✗
Aruba 3200XM	6.4	✓	✓	✓	✓	✓	✗	✗
Aruba 650	6.4	✓	✓	✓	✓	✓	✗	✗
Aruba 7000	6.4.1.0	✓	✓	✓	✓	✓	✗	✗
Aruba IAP	6.4.1.0	✓	✓	✓	✓	✓	✗	✗
Motorola RFS	5.5	✓	✓	✓	✓	✓	✗	✗
4000	5.5	✓	✓	✓	✓	✓	✗	✗
HP 830	35073P5	✓	✓	✓	✓	✓	✗	✗
	35073P5	✓	✓	✓	✓	✓	✗	✗
Ruckus ZD1200	9.9.0.0	✓	✓	✓	✓	✓	✗	✗
	9.9.0.0	✓	✓	✓	✓	✓	✗	✗

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. Aruba 3200 is supported for ISE 2.2 patch 2 and above.

Table 5 Validated Cisco Routers

Device	Validated OS[1] Minimum OS [3]	AAA	Profiling	BYOD	Guest	Posture	MDM	TrustSec [2]
Cisco Routers								
ISR 88x, 89x Series	IOS 15.3.2T(ED)	✓	!	✗	!	✗	✗	✓
	IOS 15.2(2)T	!	!	✗	!	✗	✗	✓
ISR 19x, 29x, 39x Series	IOS 15.3.2T(ED)	✓	!	✗	!	✗	✗	✓
	IOS 15.2(2)T	✓	!	✗	!	✗	✗	✓
SGR 2010	IOS 15.3.2T(ED)	✓	!	✗	!	✗	✗	✓
	IOS 15.3.2T(ED)	✓	!	✗	!	✗	✗	✓
4451-X SM-X L2/L3 Ethermodule	IOS XE 3.11	✓	✓	✓	✓	✓	✓	✓
	IOS XE 3.11	✓	✓	✓	✓	✓	✓	✓
CE 9331	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	✓	✗	✗	✗	✗	✗	✓
	IOS XE 16.12.1	✓	✗	✗	✗	✗	✗	✓
C959-2PLTEUS	IOS XE 16.12.1	✓	✗	✗	✗	✗	✗	✓
	IOS XE 16.12.1	✓	✗	✗	✗	✗	✗	✓
ASR 1201	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	✓	✗	✗	✗	✗	✗	✓
	IOS XE 16.12.1	✓	✗	✗	✗	✗	✗	✓
ASR 1202	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	✓	✗	✗	✗	✗	✗	✓
	IOS XE 16.12.1	✓	✗	✗	✗	✗	✗	✓

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.

Table 6 Validated Cisco Remote Access

Device	Validated OS[1] Minimum OS [3]	AAA	Profiling	BYOD	Guest	Posture	MDM	TrustSec [2]
Cisco Remote Access								

Table 6 Validated Cisco Remote Access (continued)

Device	Validated OS[1] Minimum OS [3]	AAA	Profiling	BYOD	Guest	Posture	MDM	TrustSec [2]
ASA 5500, ASA 5500-X (Remote Access Only)	ASA 9.2.1	NA	NA	✓	NA	✓	✗	✓
	ASA 9.1.5	NA	NA	✗	NA	✗	✗	✗
Meraki MX Platforms	Latest Version	✓	!	✗	!	✗	✗	✗
	Latest Version	✓	!	✗	!	✗	✗	✗

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.

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

Refer to *Cisco Identity Services Engine Administrator Guide, Release 2.2* for more information.

Table 7 Validated External Identity Sources

External Identity Source	OS/Version
Active Directory[1, 2]	
Microsoft Windows Active Directory 2003[3]	—
Microsoft Windows Active Directory 2003 R2[21]	—
Microsoft Windows Active Directory 2008	—
Microsoft Windows Active Directory 2008 R2	—
Microsoft Windows Active Directory 2012	—
Microsoft Windows Active Directory 2012 R2[4]	—
Microsoft Windows Active Directory 2016	—
LDAP Servers	
SunONE LDAP Directory Server	Version 5.2
OpenLDAP Directory Server	Version 2.4.23
Token Servers	
RSA ACE/Server	6.*x* series
RSA Authentication Manager	7.*x* and 8.*x* series
Any RADIUS RFC 2865-compliant token server	—
Security Assertion Markup Language (SAML) Single Sign-On (SSO)	
Microsoft Azure	—
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	—
Secure Auth	8.1.1
Any SAMLv2-compliant Identity Provider	—
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

1. Cisco ISE OCSP functionality is available only on Microsoft Windows Active Directory 2008 and later.
2. Microsoft Windows Active Directory version 2000 or its functional level are not supported by Cisco ISE.
3. Microsoft has ended support for Windows Server 2003 and 2003 R2. We recommend that you upgrade Windows Server to a supported version.
4. Cisco ISE supports all the legacy features in Microsoft Windows Active Directory 2012 R2; however, the new features in 2012 R2, such as Protective User Groups, are not supported.

Validated MDM Servers

Validated MDM servers include products from the following vendors:

- Absolute
- 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 69 and earlier versions
- Mozilla Firefox ESR 60.9 and earlier versions
- Google Chrome 77 and earlier versions
- Microsoft Internet Explorer 10.*x* and 11.*x*

  If you are using Internet Explorer 10.*x*, enable TLS 1.1 and TLS 1.2, and disable SSL 3.0 and TLS 1.0 (Internet Options > Advanced).

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, to support RHEL 7 as the Guest OS, update the VMware hardware version to 9 or later. RHEL 7 is supported with VMware hardware version 9 and later.

The ISE 2.2 OVA templates are not compatible with VMware web client for vCenter 6.5. As a workaround, use the VMware OVF tool to import the OVA templates.

- KVM on RHEL 7.0
- Microsoft Hyper-V on Microsoft Windows Server 2012 R2 and later

Validated Cisco Mobility Services Engine Release

Cisco ISE integrates with Cisco Mobility Services Engine (MSE), Release 8.0 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) ISE 2.0*
- *Cisco Identity Services Engine Administrator Guide, Release 2.2*

Validated Cisco Prime Infrastructure Release

Cisco Prime Infrastructure, Release 3.1 integrates with Cisco ISE, Release 2.2 to leverage the monitoring and reporting capabilities of Cisco ISE.

Validated Lancope Stealthwatch Release

Cisco ISE is validated with Lancope Stealthwatch, Release 6.8.

Support for Threat Centric NAC

Cisco ISE is validated with the following adapters:

- SourceFire FireAMP
- Qualys

Note Only the Qualys Enterprise Edition is currently supported for TC-NAC flows.

Validated Client Machine and Personal Device Operating Systems, Supplicants, and Agents

Client Machine Operating Systems and Agent Support in Cisco ISE, page 17 lists the supported client machine operating systems, browsers, and agent versions supporting each client machine type. For all devices, you must also have cookies enabled in the web browser.

Note All standard 802.1X supplicants can be used with Cisco ISE, Release 2.2 standard and advanced features as long as they support the standard authentication protocols supported by Cisco ISE. (For information on allowed authentication protocols, see the "Manage Authentication Policies" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 2.2*). For the VLAN change authorization feature to work in a wireless deployment, the supplicant must support IP address refresh on VLAN change.

Cisco NAC Agent Interoperability Between Cisco NAC Appliance and Cisco ISE

The Cisco NAC Agent versions 4.9.5.3 and later can be used on both Cisco NAC Appliance Releases 4.9(3), 4.9(4), 4.9(5) and Cisco ISE Releases 1.1.3-patch 11, 1.1.4-patch 11, 1.2, 1.3, 1.4, 2.0, 2.1, 2.2. This is the recommended model of deploying the NAC agent in an environment where users will be roaming between ISE and NAC deployments.

Note The new features introduced in Cisco ISE 1.4 and later releases, such as the Service Check (MAC OS X), File Check (MAC OS X), Application Check (MAC OS X), and Patch Management Check (MAC OS X and Windows), are available only with AnyConnect 4.1.00028 or later.
The new features introduced in Cisco ISE 2.2 and later releases, such as Application Visibility Monitoring, Firewall Check, and File Check enhancements (checks for SHA-256 checksum) are available only with AnyConnect 4.4.*x* or later.
Refer to the *Cisco Identity Services Engine Administrator Guide, Release 2.2* for more information.

Client Machine Operating Systems and Agent Support in Cisco ISE

- Google Android
- Apple iOS
- Apple Mac OS X
- Microsoft Windows
- Google Chromebook
- Others

Table 8 Google Android [1]

Client Machine Operating System	Web Browser	Supplicants (802.1X)
Google Android 9.x	• Native browser • Mozilla Firefox	Google Android Supplicant 9.x
Google Android 8.x	• Native browser • Mozilla Firefox	Google Android Supplicant 8.x
Google Android 7.x	• Native browser • Mozilla Firefox	Google Android Supplicant 7.x
Google Android 6.x	• Native browser • Mozilla Firefox	Google Android Supplicant 6.x

Table 8 Google Android [1]

Client Machine Operating System	Web Browser	Supplicants (802.1X)
Google Android 5.x	• Native browser • Mozilla Firefox	Google Android Supplicant 5.x
Google Android 4.x	• Native browser • Mozilla Firefox	Google Android Supplicant 4.x
Google Android 3.x	• Native browser	Google Android Supplicant 3.x
Google Android 2.3.x	• Native browser • Mozilla Firefox	Google Android Supplicant 2.3.x
Google Android 2.2.x	• Native browser	Google Android Supplicant 2.2.x

1. Because of the open access-nature of Android implementation on available devices, Cisco ISE may not support certain Android OS version and device combinations.

Android 9 changes require:

- Update the posture feed in ISE to get the NSA for Android 9.
- 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 certificate by entering either domain name or IP Address option in the SAN field.

Table 9 Apple iOS [1]

Client Machine Operating System	Web Browser	Supplicants (802.1X)
Apple iOS 12.x	• Safari	Apple iOS Supplicant 12.x
Apple iOS 11.x	• Safari	Apple iOS Supplicant 11.x
Apple iOS 10.x	• Safari	Apple iOS Supplicant 10.x
Apple iOS 9.x	• Safari	Apple iOS Supplicant 9.x
Apple iOS 8.x	• Safari	Apple iOS Supplicant 8.x
Apple iOS 7.x	• Safari	Apple iOS Supplicant 7.x
Apple iOS 6.x	• Safari	Apple iOS Supplicant 6.x
Apple iOS 5.x	• Safari	Apple iOS Supplicant 5.x

1. When Apple iOS devices use Protected Extensible Authentication Protocol (PEAP) with Cisco ISE or 802.1x, certificate warnings might be displayed even for publicly trusted certificates. This usually occurs when the public certificate includes a Certificate Revocation List (CRL) distribution point that the iOS device needs to verify. The iOS device cannot verify the CRL without network access. Click Confirm or Accept in the iOS device to authenticate to the network.

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.

Table 10 Apple Mac OS X

Client Machine Operating System	Web Browser	Supplicants (802.1X)	Cisco ISE	Mac OS X Agent	AnyConnect
Apple macOS 10.14	• Apple Safari • Mozilla Firefox • Google Chrome	Apple macOS Supplicant 10.14	2.2	4.9.5.3	4.4.*x or later*
Apple macOS 10.13	• Apple Safari • Mozilla Firefox • Google Chrome	Apple macOS Supplicant 10.13	2.2	4.9.5.3	4.4.*x or later*
Apple macOS 10.12	• Apple Safari [1] • Mozilla Firefox • Google Chrome [2]	Apple macOS Supplicant 10.12	2.2	4.9.5.3	4.4.*x or later*
Apple Mac OS X 10.11	• Apple Safari • Mozilla Firefox • Google Chrome	Apple Mac OS X Supplicant 10.11	2.2	4.9.5.3	4.4.*x or later*
Apple Mac OS X 10.10	• Apple Safari • Mozilla Firefox • Google Chrome	Apple Mac OS X Supplicant 10.10	2.2	4.9.5.3	4.4.*x or later*
Apple Mac OS X 10.9	• Apple Safari • Mozilla Firefox • Google Chrome	Apple Mac OS X Supplicant 10.9	2.2	4.9.5.3	4.4.*x or later*

1. Apple Safari version 6.0 is supported only on Mac OS X 10.7.4 and later versions of the operating system.
2. If you are using Mac OS X clients with Java 7, you cannot download the Agents using Google Chrome browser. Java 7 runs only on 64-bit browsers and Chrome is a 32-bit browser. It is recommended to use either previous versions of Java or other browsers while downloading the Agents.

Table 11 Microsoft Windows [1]

Client Machine Operating System	Web Browser	Supplicants (802.1X)	Cisco ISE	Cisco NAC Agent[2]	Cisco NAC Web Agent[15]	AnyConnect[3]
Microsoft Windows 10						
Windows 10	• Microsoft IE 11 • Mozilla Firefox • Google Chrome	• Microsoft Windows 10 802.1X Client • AnyConnect Network Access Manager	2.2	4.9.5.8 4.9.5.7 4.9.5.6	4.9.5.9 4.9.5.8 4.9.5.4 4.9.5.3	4.4.*x or later*
Microsoft Windows 8 [4,5,6]						

Table 11 Microsoft Windows [1]

Client Machine Operating System	Web Browser	Supplicants (802.1X)	Cisco ISE	Cisco NAC Agent[2]	Cisco NAC Web Agent[15]	AnyConnect[3]
Windows 8.1 Windows 8 Windows 8 x64 Windows 8 Professional Windows 8 Professional x64 Windows 8 Enterprise Windows 8 Enterprise x64	• Microsoft IE 11 • Mozilla Firefox • Google Chrome	• Microsoft Windows 8 802.1X Client • AnyConnect Network Access Manager	2.2	4.9.5.8 4.9.5.7 4.9.5.6	4.9.5.9 4.9.5.8 4.9.5.4 4.9.5.3	4.4.*x or later*
Windows 7 Professional Windows 7 Professional x64 Windows 7 Ultimate Windows 7 Ultimate x64 Windows 7 Enterprise Windows 7 Enterprise x64 Windows 7 Home Premium Windows 7 Home Premium x64 Windows 7 Home Basic Windows 7 Starter Edition	• Microsoft IE 11 • Mozilla Firefox • Google Chrome	• Microsoft Windows 7 802.1X Client • AnyConnect Network Access Manager	2.2	4.9.5.8 4.9.5.7 4.9.5.6	4.9.5.9 4.9.5.8 4.9.5.4 4.9.5.3	4.4.*x or later*

1. It is recommended to use the Cisco NAC/Web Agent versions along with the corresponding Cisco ISE version.
2. Cisco NAC Agent and Cisco NAC Web Agent do not support Google Chrome version 45 and later. See CSCuw19276 for more information. We recommend that you use another supported browser.
3. 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.
4. In Windows 8, Internet Explorer 10 has two modes: Desktop and Metro. In Metro mode, the ActiveX plugins are restricted. You cannot download the Cisco NAC Agent in Metro mode. You must switch to Desktop mode, ensure ActiveX controls are enabled, and then launch Internet Explorer to download the Cisco NAC Agent. (If users are still not able to download Cisco NAC agent, check and enable "compatibility mode.")
5. When you create a Cisco ISE client provisioning policy to accommodate Windows 8, you must specify the "Windows All" operating system option.
6. Windows 8 RT is not supported.

Table 12 Google Chromebook[1]

Client Machine Operating System	Web Browser	Supplicants (802.1X)	Cisco ISE
Google Chromebook	Google Chrome version 49 or later	Google Chromebook supplicant	2.2

1. Google Chromebook is a managed device and does not support the Posture service. Refer to the *Cisco Identity Services Engine Administration Guide, Release 2.2* for more information.

Note Cisco ISE BYOD or Guest portal will 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.

Table 13 Others

Client Machine Operating System	Web Browser[1]	Supplicants (802.1X)
Red Hat Enterprise Linux (RHEL)	• Google Chrome • Mozilla Firefox	Not tested extensively[2]

1. Google Chrome does not support 32-bit Linux systems.
2. 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 14 Validated Operating Systems and Browsers

Supported Operating System[1]	Browser Versions
Google Android [2] 9.x, 8.x, 7.x, 6.x, 5.x, 4.x, 3.x, 2.3.x, 2.2.x	• Native browser • Mozilla Firefox
Apple iOS 12.x, 11.x, 10.x, 9.x, 8.x, 7.x, 6.x, 5.x	• Safari

Table 14 Validated Operating Systems and Browsers

Supported Operating System[1]	Browser Versions
Apple Mac OS X 10.14, 10.13, 10.12, 10.11, 10.10, 10.9	• Mozilla Firefox • Safari • Google Chrome
Microsoft Windows 10, 8.1, 8[3], 7	• Microsoft IE 11 • Mozilla Firefox • Google Chrome
Red Hat Enterprise Linux (RHEL)	• Mozilla Firefox • Google Chrome

1. 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.
2. Because of the open access-nature of Android implementation on available devices, Cisco ISE may not support certain Android OS version and device combinations.
3. In Windows 8, Internet Explorer 10 has two modes: Desktop and Metro. In Metro mode, the ActiveX plugins are restricted. You cannot download the Cisco NAC Agent in Metro mode. You must switch to Desktop mode, ensure ActiveX controls are enabled, and then launch Internet Explorer to download the Cisco NAC Agent. (If users are still not able to download Cisco NAC agent, check and enable "compatibility mode.")

Validated Devices for On-Boarding and Certificate Provisioning

Cisco Wireless LAN Controller (WLC) 7.2 or above support is required for the BYOD feature. Refer to the *Release Notes for the Cisco Identity Services Engine, Release 2.2* for any known issues or caveats.

Note To get the latest Cisco-supported client OS versions, check the posture update information (Administration > System > Settings > Posture > Updates) and click **Update Now**, if needed or if you have not recently updated the posture feeds.

Table 15 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 12.x, 11.x, 10.x[1], 9.x, 8.x, 7.x, 6.x, 5.x	Yes	Yes[2]	Apple profile configurations (native)
Android	2.2 and above[3, 4]	Yes[5]	Yes	Cisco Network Setup Assistant
Barnes & Noble Nook (Android) HD/HD+ [6]	—	—	—	—
Windows	Windows 10, 8.1, 8, 7	Yes[7]	Yes	2.2.1.53 or later
Windows	Mobile 8, Mobile RT, Surface 8, and Surface RT	No	No	—

Table 15 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
MAC OS X[8]	Mac OS X 10.12, 10.11, 10.10, 10.9	Yes	Yes	2.2.1.43 or later
Chrome OS	Chrome OS 76, 73	Yes	Yes	—

1. Tested with Cisco ISE, Release 2.1 patch 1.
2. Connect to secure SSID after provisioning
3. There are known EAP-TLS issues with Android 4.1.1 devices. Contact your device manufacturer for support.
4. Android 6.0 requires May 2016 patch to support ECC certificates; does not support the P-192 ECC curve type.
5. Beginning from Android version 6.0, the Cisco supplicant provisioning wizard (SPW) can no longer modify the system-created SSIDs. When the SPW prompts you to forget the network, you must choose to forget the network and press the Back button to continue the provisioning flow.
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 or if you check this option, ensure that you select the correct root certificate.
8. If you are using Mac OS X clients with Java 7, you cannot download the SPWs using Google Chrome browser. Java 7 runs only on 64-bit browsers and Chrome is a 32-bit browser. It is recommended to use either previous versions of Java or other browsers while downloading the SPWs.

Validated OpenSSL Version

Cisco ISE, Release 2.2 supports OpenSSL 1.0.2.x (CiscoSSL 6.0).

Supported Cipher Suites

Cisco ISE 2.2 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

Table 16 lists the supported cipher suites for Cisco ISE 2.2.

Table 16 Supported Cipher Suites for Cisco ISE 2.2

Cipher Suite	EAP	Download CRL from HTTPS, Download CRL from LDAPS, Secure TCP Syslog Client, Secure LDAP Client, Admin Certificate Authentication[1]
Common Criteria Restrictions Enabled	No	Yes
ECC RSA Ciphers		
ECDHE-RSA-AES256-GCM-SHA384	Yes	No
ECDHE-RSA-AES128-GCM-SHA256	Yes	No

Table 16 Supported Cipher Suites for Cisco ISE 2.2 (continued)

Cipher Suite	EAP	Download CRL from HTTPS, Download CRL from LDAPS, Secure TCP Syslog Client, Secure LDAP Client, Admin Certificate Authentication[1]
ECDHE-RSA-AES256-SHA384	Yes	No
ECDHE-RSA-AES128-SHA256	Yes	No
ECDHE-RSA-AES256-SHA	Yes	No
ECDHE-RSA-AES128-SHA	Yes	No
DHE RSA Ciphers (only for EAP-FAST anonymous provisioning)		
DHE-RSA-AES256-SHA256	No	Yes
DHE-RSA-AES128-SHA256	No	Yes
DHE-RSA-AES256-SHA	No	Yes (only when SHA-1 is enabled)
DHE-RSA-AES128-SHA	No	Yes (only when SHA-1 is enabled)
Standard Ciphers		
AES256-SHA256	Yes	Yes
AES128-SHA256	Yes	Yes
AES256-SHA	Yes	Yes (only when SHA-1 is enabled)
AES128-SHA	Yes	Yes (only when SHA-1 is enabled)
3DES Ciphers		
EDH-RSA-DES-CBC3-SHA	Yes	Yes (only when SHA-1 and 3DES/DSS are enabled)
DES-CBC3-SHA	Yes	Yes (only when SHA-1 and 3DES/DSS are enabled)
DSS Ciphers		
DHE-DSS-AES256-SHA	No	Yes (only when SHA-1 and 3DES/DSS are enabled)
DHE-DSS-AES128-SHA	No	Yes (only when SHA-1 and 3DES/DSS are enabled)
EDH-DSS-DES-CBC3-SHA	No	Yes (only when SHA-1 and 3DES/DSS are enabled)
Weak RC4 Ciphers		
RC4-SHA	Yes (when "Allow weak ciphers" is enabled)	No
RC4-MD5	Yes (when "Allow weak ciphers" is enabled)	No
ADH Cipher (only for EAP-FAST anonymous provisioning)		
ADH-AES-128-SHA	Yes	No

1. To enable SHA1 and 3DES/DSS, from the Admin Portal, go to Administration > System > Settings > Protocols > Security Settings.

Table 17 lists the supported Cipher Suites for Cisco ISE 2.2 patch 2.

Table 17 Supported Cipher Suites for Cisco ISE 2.2 Patch 2

Cipher suite	EAP server RADIUS DTLS server	Download CRL from HTTPS Download CRL from LDAPS Secure TCP syslog client Secure LDAP client RADIUS DTLS client for CoA
TLS 1.0 support	When TLS 1.0 is allowed (DTLS server supports only DTLS 1.2) **Note** Allow TLS 1.0 option is disabled by default in Cisco ISE 2.2 Patch 2 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 page (Administration > System > Settings > Protocols > Security Settings).	When TLS 1.0 is allowed (DTLS client supports only DTLS 1.2)
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 and SHA1 are allowed	When ECDHE-RSA and SHA1 are allowed
ECDHE-RSA-AES128-SHA	When ECDHE-RSA and SHA1 are allowed	When ECDHE-RSA and SHA1 are 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

Table 17 Supported Cipher Suites for Cisco ISE 2.2 Patch 2 (continued)

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		
EDH-RSA-DES-CBC3-SHA	When 3DES and SHA-1 are allowed	When 3DES/DSS and SHA-1 are allowed
DSS ciphers		
DHE-DSS-AES256-SHA	No	When 3DES/DSS and SHA-1 are allowed
DHE-DSS-AES128-SHA	No	When 3DES/DSS and SHA-1 are allowed
EDH-DSS-DES-CBC3-SHA	No	When 3DES/DSS and SHA-1 are allowed
Weak RC4 ciphers		
RC4-SHA	When “Allow weak ciphers” option is enabled in Allowed Protocols page and when SHA-1 is allowed	No
RC4-MD5	When “Allow weak ciphers” option is enabled in Allowed Protocols page	No
EAP-FAST anonymous provisioning only: ADH-AES-128-SHA	Yes	No
Peer certificate restrictions		

Table 17 Supported Cipher Suites for Cisco ISE 2.2 Patch 2 (continued)

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 + 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 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.

  For example, 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 also 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 However, 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:

Supported Cryptographic Algorithms:

- RSA
- ECC

Table 18 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[1, 2]		
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 Android 6.0, which does not support the P-192 curve type).

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

Related Documentation

This section includes links to ISE Community resources, release-specific documentation, and platform-specific documentation.

ISE Community Resource

Join the ISE Community to view resources, ask questions, and participate in discussions. See ISE Product Documentation, Introduction to ISE, YouTube Videos, Feature and Integration Demos, and Training Resources.

Note The examples and screenshots provided in the ISE Community resources might be from earlier releases of Cisco ISE. Check the GUI for newer or additional features and updates.

- ISE Design and Integration Guides
- ISE Location-Based Services with Mobility Services Engine
- ISE and MACSec
- Network as a Sensor and Enforcer
- Configuration Examples and Tech Notes
- Rapid Threat Containment (RTC)

Release-Specific Documents

Table 19 Product Documentation for Cisco Identity Services Engine

Document Title	Location
Release Notes for the Cisco Identity Services Engine, Release 2.2	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-release-notes-list.html
Cisco Identity Services Engine Network Component Compatibility, Release 2.2	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-device-support-tables-list.html
Cisco Identity Services Engine Admin Guide, Release 2.2	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html

Table 19 Product Documentation for Cisco Identity Services Engine (continued)

Document Title	Location
Cisco Identity Services Engine Hardware Installation Guide, Release 2.2	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html
Cisco Identity Services Engine Upgrade Guide, Release 2.2	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html
Cisco Identity Services Engine, Release 2.2 Migration Tool Guide	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html
Cisco Identity Services Engine Sponsor Portal User Guide, Release 2.2	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-user-guide-list.html
Cisco Identity Services Engine CLI Reference Guide, Release 2.2	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-command-reference-list.html
Cisco Identity Services Engine API Reference Guide, Release 2.2	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-command-reference-list.html
Regulatory Compliance and Safety Information for Cisco Identity Services Engine 3500 Series Appliance	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html
Cisco ISE In-Box Documentation and China RoHS Pointer Card	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-documentation-roadmaps-list.html

Platform-Specific Documents

Links to other platform-specific documentation are available at the following locations:

- Cisco ISE
  http://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html
- Cisco Secure ACS
  http://www.cisco.com/c/en/us/support/security/secure-access-control-system/tsd-products-support-series-home.html
- Cisco NAC Appliance
  http://www.cisco.com/c/en/us/support/security/nac-appliance-clean-access/tsd-products-support-series-home.html
- Cisco NAC Profiler
  http://www.cisco.com/c/en/us/support/security/nac-profiler/tsd-products-support-series-home.html
- Cisco NAC Guest Server
  http://www.cisco.com/c/en/us/support/security/nac-guest-server/tsd-products-support-series-home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.