Cisco Identity Services Engine Network Component Compatibility, Release 1.4

Revised: May 23, 2017

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

Supported 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 1.4*.

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, and are therefore not supported with non-Cisco devices. In addition, certain other advanced functions like central web authentication (CWA), Change of Authorization (CoA), Security

Cisco Systems, Inc.
www.cisco.com

Group Access (SGA), and downloadable access control lists (ACLs), are only supported on Cisco devices. For a full list of supported Cisco devices, see Table 1.

The NADs that are not explicitly listed in Table 1 and do not support RADIUS CoA must use inline posture.

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 1.4*.

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

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.

Table 1 lists 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 or IPN
MDM	RADIUS CoA, URL Redirection + SessionID
TrustSec	SGT Classification

Table 1 Supported Network Access Devices

Device	Recommended OS[1] / Minimum OS [4]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture [2]	MDM	TrustSec [3]
Cisco Access Switches									
IE2000 IE3000	IOS 15.2(2) E3	✓	✓	✓	✓	✓	✓	✓	✓
	IOS 15.0(2) EB	✓	✓	✓	✓	✗	✓	✓	✓
CGS 2520	IOS 15.2(3)E3	✓	✓	✓	✓	✗	✓	✓	✓
	IOS 15.0(2)EK1	✓	✓	✓	✓	✗	✓	✓	✓
Catalyst 2960 LAN Base	IOS 12.2.55-SE10	✓	✓	✓	✓	✗	✓	✓	✗
	IOS v12.2(55)SE5	✓	✓	✓	✓	✗	✓	✓	✗
Catalyst 2960-C	IOS 15.2(2)E3	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 3560-C	IOS 12.2(55) EX3	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 2960-Plus	IOS 15.2(2)E3	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 2960-SF	IOS 15.0(2)SE7	✓	✓	✓	✓	✓	✓	✓	✗
Catalyst 2960-S	IOS 15.0.2-SE10a	✓	✓	✓	✓	✓	✓	✓	✗
	IOS v12.2.(55)SE5	✓	✓	✓	✓	✓	✓	✓	✗
Catalyst 2960–XR Catalyst 2960–X	IOS 15.2(2)E3	✓	✓	✓	✓	✓	✓	✓	✓
	IOS 15.0.2A-EX5	✓	✓	✓	✓	✓	✓	✓	✗
Catalyst 2960-CX	IOS 15.2(3)E1	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 3560-CX	IOS 15.2(3)E	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 3560G Catalyst 3750G	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 12.2.(55)SE10	✓	✓	✓	✓	✓	✓	✓	✓
	IOS v12.2(55)SE5	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 3560-X	IOS 15.2(2)E3	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 3750-X	IOS 12.2.(55)SE5	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 3850	IOS XE 3.6.3	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 3650	IOS XE 3.3.5.E	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 4500-X	IOS XE 3.6.3	✓	✓	✓	✓	✓	✓	✓	✓
	IOS XE 3.4.4 SG	✓	✓	✓	✓	✗	✓	✓	✓
Catalyst 4500 Supervisor 7-E, 7L-E	IOS XE 3.6.3	✓	✓	✓	✓	✓	✓	✓	✓
	IOS XE 3.4.4 SG	✓	✓	✓	✓	✗	✓	✓	✓

Table 1 Supported Network Access Devices (continued)

Device	Recommended OS[1] / Minimum OS [4]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture [2]	MDM	TrustSec [3]
Catalyst 4500 Supervisor 6-E, 6L-E	IOS 15.2(2)E3	✓	✓	✓	✓	✗	✓	✓	✓
	IOS 15.2(2)E	✓	✓	✓	✓	✗	✓	✓	✓
Catalyst 4500 Supervisor 8-E	IOS XE 3.6.3	✓	✓	✓	✓	✗	✓	✓	✓
	IOS XE 3.3.2 XO	✓	✓	✓	✓	✗	✓	✓	✓
Catalyst 6500-E (Supervisor 32)	IOS 12.2.33-SJX9	✓	✓	✓	✓	✗	✓	✓	✓
	IOS v12.2(33)SXI6	✓	✓	✓	✓	✗	✓	✓	✓
Catalyst 6500-E (Supervisor 720)	IOS 15.1(2)SY5	✓	✓	✓	✓	✗	✓	✓	✓
	IOS v12.2(33)SXI6	✓	✓	✓	✓	✗	✓	✓	✓
Catalyst 6500-E (VS-S2T-10G)	IOS 15.1(2)SY5	✓	✓	✓	✓	✗	✓	✓	✓
	IOS 15.0(1)SY1	✓	✓	✓	✓	✗	✓	✓	✓
Catalyst 6807-XL Catalyst 6880-X (VS-S2T-10G)	IOS 15.1(2)SY5	✓	✓	✓	✓	✗	✓	✓	✓
	IOS 15.0(1)SY1	✓	✓	✓	✓	✗	✓	✓	✓
Cat 6848ia	IOS 15.1(2)SY5	✓	✓	✓	✓	✗	✓	✓	✓
	IOS 15.1(2) SY+	✓	✓	✓	✓	✗	✓	✓	✓
Meraki MS Platforms	Latest Version	✓	✓	✗	!	✗	✗	✗	✗
	Latest Version	✓	✓	✗	!	✗	✗	✗	✗
Third Party Access Switches									
Avaya ERS 2526T	4.4	✓	!	✗	✗	✗	✗	✗	✗
	4.4	✓	!	✗	✗	✗	✗	✗	✗
Brocade ICX 6610	7.3	✓	!	✗	✗	✗	✗	✗	✗
	7.3	✓	!	✗	✗	✗	✗	✗	✗
Juniper EX3200	12.3R6.6	✓	!	✗	✗	✗	✗	✗	✗
	12.3R6.6	✓	!	✗	✗	✗	✗	✗	✗
Cisco Wireless LAN Controllers [5]									
WLC 2100	AireOS 7.0.116.0	!	✓	✗	!	✗	!	✗	✗
	AireOS 7.0.116.0	!	✓	✗	!	✗	!	✗	✗
WLC 4400	AireOS 7.0.116.0	!	✓	✗	!	✗	!	✗	✗
	AireOS 7.0.116.0	!	✓	✗	!	✗	!	✗	✗
WLC 2500	AireOS 8.0.121.0	✓	✓	✓	✓	✗	✓	✓	✓
	AireOS 7.2.103.0	!	✓	✓	✓	✗	✓	✓	✓
WLC 5508	AireOS 8.0.121.0	✓	✓	✓	✓	✗	✓	✓	✓
	AireOS 7.0.116.0	!	✓	✗	!	✗	!	✗	✓
WLC 5520	AireOS 8.1.122.0	✓	✓	✓	✓	✗	✓	✓	✓
	AireOS 8.1.122.0	✓	✓	✓	✓	✗	✓	✓	✓

Table 1 Supported Network Access Devices (continued)

Device	Recommended OS[1] / Minimum OS [4]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture [2]	MDM	TrustSec [3]
WLC 7500	AireOS 8.0.121.0	✓	✓	✓	✓	✗	✓	✓	✗
	AireOS 7.2.103.0	!	✓	✗	✗	✗	!	✗	✗
WLC 8510	AireOS 8.0.120.0	✓	✓	✓	✓	✗	✓	✓	✗
	AireOS 7.4.121.0	✓	✓	✗	✗	✗	!	✓	✗
WLC 8540	AireOS 8.1.122.0	✓	✓	✓	✓	✗	✓	✓	✗
	AireOS 8.1.122.0	✓	✓	✓	✓	✗	✓	✓	✗
vWLC	AireOS 8.0.120.0	✓	✓	✓	✓	✗	✓	✓	✗
	AireOS 7.4.121.0	✓	✓	✓	✓	✗	✓	✓	✗
WiSM1 6500	AireOS 7.0.116.0	!	✓	✗	!	✗	!	✗	✗
	AireOS 7.0.116.0	!	✓	✗	!	✗	!	✗	✗
WiSM2 6500	AireOS 8.0.120.0	✓	✓	✓	✓	✗	✓	✓	✓
	AireOS 7.2.103.0	!	✓	✓	✓	✗	✓	✓	✓
WLC 5760	IOS XE 3.6	✓	✓	✓	✓	✓	✓	✓	✓
	IOS XE 3.3	✓	✓	✓	✓	✗	✓	✓	✓
WLC for ISR (ISR2 ISM, SRE700, and SRE900)	AireOS 7.0.116.0	!	✓	✗	!	✗	!	✗	✗
	AireOS 7.0.116.0	!	✓	✗	!	✗	!	✗	✗
Meraki MR Platforms	Public Beta	✓	✓	✓	✓	✗	✓	✓	✗
	General Availability	✓	!	✗	!	✗	✗	✗	✗
Third Party Wireless LAN Controllers									
Aruba 3200XM Aruba 650	6.3	✓	✓	✗	!	✗	!	✗	✗
	6.3	✓	✓	✗	!	✗	!	✗	✗
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	✓	✓	✓	✓	✗	✓	✓	✓
Cisco Remote Access									
ASA 5500, ASA 5500-X (Remote Access Only)	ASA 9.2.1	NA	NA	✓	NA	✗	✓	✗	✓
	ASA 9.1.5	NA	NA	✗	NA	✗	!	✗	✗

Table 1 Supported Network Access Devices (continued)

Device	Recommended OS[1] / Minimum OS [4]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture [2]	MDM	TrustSec [3]
Meraki MX Platforms	Latest Version	✓	!	✗	!	✗	✗	✗	✗
	Latest Version	✓	!	✗	!	✗	✗	✗	✗

1. Recommended OS is the version tested for compatibility and stability.
2. Cisco routers such as ISR 88x, 89x Series do not support CWA, therefore, an IPN has to be deployed for posture.
3. For a complete list of Cisco TrustSec feature support, see http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns1051/product_bulletin_c25-712066.html.
4. Minimum OS is the version in which the features got introduced.
5. 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 the requirements for Inline Posture Node as they do not send Framed-IP-Address. 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 AAA Attributes for Third-Party VPN Concentrators

For third-party VPN concentrators to integrate with Cisco ISE and Inline Posture nodes, the following authentication, authorization, and accounting (AAA) attributes must be included in RADIUS communication:

- Calling-Station-Id (for MAC_ADDRESS)
- USER_NAME
- NAS_PORT_TYPE

Also, for VPN devices, the RADIUS accounting message must have the framed-ip-address attribute set to the VPN client's IP address pool.

Supported External Identity Sources

Refer to *Release Notes for the Cisco Identity Services Engine, Release 1.4* for more information.

Table 2 Supported External Identity Sources

External Identity Source	OS/Version
Active Directory[1, 2, 3]	
Microsoft Windows Active Directory 2003	—
Microsoft Windows Active Directory 2003 R2	—
Microsoft Windows Active Directory 2008	—
Microsoft Windows Active Directory 2008 R2	—
Microsoft Windows Active Directory 2012	—

Table 2 Supported External Identity Sources (continued)

External Identity Source	OS/Version
Microsoft Windows Active Directory 2012 R2[4]	—
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)	
Oracle Access Manager (OAM)	Version 11.1.2.2.0
Oracle Identity Federation (OIF)	Version 11.1.1.2.0

1. Cisco ISE OCSP functionality is available only on Microsoft Windows Active Directory 2008, 2008 R2, 2012, and 2012 R2.
2. Cisco ISE SCEP functionality is available only on Microsoft Windows Active Directory 2008 R2, 2012, and 2012 R2.
3. Microsoft Windows Active Directory version 2000 or its functional level are not supported by Cisco ISE.
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.

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*

Supported Browsers for the Admin Portal

- Mozilla Firefox version 31.*x* ESR, 36.*x*, and 37.*x*
- Microsoft Internet Explorer 10.*x* and 11.*x*

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

Adobe Flash Player 11.1.0.0 or above must be installed on the system running your client browser.

The minimum required screen resolution to view the Cisco ISE Admin portal and for a better user experience is 1280 x 800 pixels.

Supported Virtual Environments

Cisco ISE supports the following VMware servers and clients:

- VMware version 8 (default) for ESXi 5.*x*
- VMware version 11 (default) for ESXi 6.0 (requires Cisco ISE 1.4 Patch 3)

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

Client Machine Operating Systems and Agent Support in Cisco ISE, page 8 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 1.4 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 1.4*). 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 4.9.4.3 and later can be used on both Cisco NAC Appliance Releases 4.9(1), 4.9(3), 4.9(4) and Cisco ISE Releases 1 1.1.3-patch 11, 1.1.4-patch 11, 1.2.x, 1.3. 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, Release 1.4, 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. Refer to the *Cisco Identity Services Engine Administrator Guide, Release 1.4* for more information.

Client Machine Operating Systems and Agent Support in Cisco ISE

- Others

Table 3 Google Android [1]

Client Machine Operating System	Web Browser	Supplicants (802.1X)
Google Android 7.x[2]	• Native browser • Mozilla Firefox	Google Android Supplicant 7.x
Google Android 6.x[3]	• Native browser • Mozilla Firefox	Google Android Supplicant 6.x
Google Android 5.x	• Native browser • Mozilla Firefox	Google Android Supplicant 5.x
Google Android 4.4.x	• Native browser • Mozilla Firefox	Google Android Supplicant 4.4.x
Google Android 4.2.x	• Native browser • Mozilla Firefox	Google Android Supplicant 4.2.x
Google Android 4.1.2	• Native browser • Mozilla Firefox	Google Android Supplicant 4.1.2
Google Android 4.0.4	• Native browser • Mozilla Firefox	Google Android Supplicant 4.0.4
Google Android 4.0.3	• Native browser • Mozilla Firefox	Google Android Supplicant 4.0.3
Google Android 4.0	• Native browser	Google Android Supplicant 4.0
Google Android 3.2.1	• Native browser • Mozilla Firefox	Google Android Supplicant 3.2.1
Google Android 3.2	• Native browser	Google Android Supplicant 3.2
Google Android 2.3.6	• Native browser • Mozilla Firefox	Google Android Supplicant 2.3.6
Google Android 2.3.3	• Native browser • Mozilla Firefox	Google Android Supplicant 2.3.3
Google Android 2.2.1	• Native browser	Google Android Supplicant 2.2.1
Google Android 2.2	• Native browser • Mozilla Firefox	Google Android Supplicant 2.2

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.
2. Tested with Cisco ISE, Release 1.4 patch 8.
3. Cisco ISE 1.4 patch 4 supports Android 6.x. Requires SPW 1.2.47.

Table 4 Apple iOS [1]

Client Machine Operating System	Web Browser	Supplicants (802.1X)
Apple iOS 10[2]	• Safari	Apple iOS Supplicant 10
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 5.1	• Safari	Apple iOS Supplicant 5.1
Apple iOS 5.0.1	• Safari	Apple iOS Supplicant 5.0.1

1. 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.
2. Tested with Cisco ISE, Release 1.4 patch 8.

Table 5 Apple Mac OS X

Client Machine Operating System	Web Browser[1, 2]	Supplicants (802.1X)	Cisco ISE	Mac OS X Agent	AnyConnect
Apple Mac OS X 10.11	• Apple Safari • Mozilla Firefox • Google Chrome	Apple Mac OS X Supplicant 10.11	1.4 patch 6	4.9.5.3	4.1.00028
Apple Mac OS X 10.10	• Apple Safari • Mozilla Firefox • Google Chrome	Apple Mac OS X Supplicant 10.10	1.4	4.9.5.3	4.1.00028
Apple Mac OS X 10.9	• Apple Safari • Mozilla Firefox • Google Chrome	Apple Mac OS X Supplicant 10.9	1.4	4.9.5.3	4.1.00028
Apple Mac OS X 10.8	• Apple Safari • Mozilla Firefox • Google Chrome	Apple Mac OS X Supplicant 10.8	1.4	4.9.5.3	4.1.00028

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 6 Microsoft Windows [1]

Client Machine Operating System	Web Browser	Supplicants (802.1X)	Cisco ISE	Cisco NAC Agent[2]	Cisco NAC Web Agent[15]	AnyConnect
Microsoft Windows 10						
Windows 10	• Microsoft Edge[3] • Microsoft IE 11.*x* • Mozilla Firefox • Google Chrome	Microsoft Windows 10 802.1X Client	1.4 Patch 3	4.9.5.8	4.9.5.4 4.9.5.8[4]	4.1.04011
Microsoft Windows 8 [5,6,7]						
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.*x*, 10.*x* • Mozilla Firefox • Google Chrome	Microsoft Windows 8 802.1X Client	1.4	4.9.5.7	4.9.5.3 4.9.5.8[8]	4.1.00028
Microsoft Windows 7[9]						
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.*x*, 10.*x* [10] • Mozilla Firefox • Google Chrome	• Microsoft Windows 7 802.1X Client • AnyConnect Network Access Manager	1.4	4.9.5.7	4.9.5.3 4.9.5.8[11]	4.1.00028
Microsoft Windows Vista[19]						

Table 6 Microsoft Windows [1]

Client Machine Operating System	Web Browser	Supplicants (802.1X)	Cisco ISE	Cisco NAC Agent[2]	Cisco NAC Web Agent[15]	AnyConnect
Windows Vista SP1, SP2 Windows Vista x64 SP1, SP2	• Microsoft IE 11.*x*, 10.*x* • Mozilla Firefox • Google Chrome	• Microsoft Windows Vista 802.1X Client • Cisco Secure Services Client (SSC) 5.*x*	1.4	4.9.5.7	4.9.5.3	4.1.00028

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 such as Internet Explorer 7.0, 8.0, or 9.0 or Mozilla Firefox 3.5.7, 3.6, or 20.x.
3. Microsoft Edge browser does not support NAC Agent provisioning.
4. Cisco NAC Web Agent 4.9.5.8 is supported for Cisco ISE 1.4 Patch 10.
5. 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.")
6. When you create a Cisco ISE client provisioning policy to accommodate Windows 8, you must specify the "Windows All" operating system option.
7. Windows 8 RT is not supported.
8. Cisco NAC Web Agent 4.9.5.8 is supported for Cisco ISE 1.4 Patch 10 on Windows 8.1 and Windows 8 operating systems only.
9. Cisco ISE does not support the Windows Embedded operating systems available from Microsoft.
10. When Internet Explorer 10 is installed on Windows 7, to get full network access, you need to update to March 2013 Hotfix ruleset.
11. Cisco NAC Web Agent 4.9.5.8 is supported for Cisco ISE 1.4 Patch 10 and Microsoft IE browser is not supported on Windows 7 operating system with Cisco NAC Web Agent 4.9.5.8.

Table 7 Others

Client Machine Operating System	Web Browser	Supplicants (802.1X)
Red Hat Enterprise Linux (RHEL) 5	• Google Chrome • Mozilla Firefox	Not tested extensively[1]
Ubuntu	Mozilla Firefox	Not tested extensively

1. 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.

Supported 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 8 Supported Operating Systems and Browsers

Supported Operating System[1]	Browser Versions
Google Android [2] 7.x[3], 6.x[4], 5.x, 4.4.x, 4.2.x, 4.1.2, 4.0.4, 4.0.3, 4.0, 3.2.1, 3.2, 2.3.6, 2.3.3, 2.2.1, 2.2	• Native browser • Mozilla Firefox
Apple iOS 10[5], 9.x, 8.x, 7.x, 6.1, 6, 5.1, 5.0.1	• Safari
Apple Mac OS X 10.11, 10.10, 10.9, 10.8, 10.7, 10.6	• Mozilla Firefox • Safari • Google Chrome
Microsoft Windows 10, 8, 8.1 [6], 7[7], Vista	• Microsoft Edge[8] • Microsoft IE 11.*x*, 10.*x*[9] • Mozilla Firefox • Google Chrome
Red Hat Enterprise Linux (RHEL) 5	• Mozilla Firefox • Google Chrome
Ubuntu	Mozilla Firefox

1. The latest two officially-released browser versions are supported for all operating systems except Microsoft Windows; refer to Table 8 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. Tested with Cisco ISE, Release 1.4 patch 8
4. Cisco ISE 1.4 patch 4 supports Android 6.x. Requires SPW 1.2.47.
5. Tested with Cisco ISE, Release 1.4 patch 8.
6. 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.”)
7. Cisco ISE does not support the Windows Embedded 7 versions available from Microsoft.
8. Cisco ISE, Release 1.4 Patch 3 supports Windows 10 operating system and Microsoft Edge browser.
9. When Internet Explorer 10 is installed on Windows 7, to get full network access, you need to update to March 2013 Hotfix ruleset.

Note When a guest user tries to log in using Google Chrome on Windows 7 OS, the login fails. It is recommended to upgrade the browser to Chrome 11 or later.

Supported 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 1.4* for any known issues or caveats.

Table 9 BYOD On-Boarding and Certificate Provisioning - Supported Devices and Operating Systems

Device	Operating System	Single SSID	Dual SSID (open > PEAP (no cert) or open > TLS)	Onboard Method
Apple iDevice	Apple iOS 10[1], 9.x, 8.x, 7.x, 6.1, 6, 5.1, 5.0.1	Yes	Yes[2]	Apple profile configurations (native)
Android	2.2 and above[3]	Yes	Yes	Cisco Network Setup Assistant
Barnes & Noble Nook (Android) HD/HD+ [4]	—	—	—	—
Windows	Windows 10, 8.1, 8, 7, Vista	Yes[5]	Yes	SPW from Cisco.com or Cisco ISE Client Provisioning feed
Windows	Mobile 8, Mobile RT, Surface 8, and Surface RT	No	No	—
MAC OS X[6]	Mac OS X 10.11, 10.10, 10.9, 10.8, 10.7, 10.6	Yes	Yes	SPW from Cisco.com or Cisco ISE client provisioning feed

1. Tested with Cisco ISE, Release 1.4 patch 8.
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. Barnes & Noble Nook (Android) works when it has Google Play Store 2.1.0 installed.
5. 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.
6. 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.

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 4.x 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.

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
- Supported Key Sizes: 1024, 2048, or 4096 bits
- Supported Secure Hash Algorithms (SHA): SHA-1 and SHA-2 (includes SHA-256)

Documentation Updates

Table 10 Cisco Identity Services Engine Network Component Compatibility Documentation Updates

Date	Update Description
05/15/2015	Cisco Identity Services Engine, Release 1.4

Related Documentation

This section covers information on release-specific documentation and platform-specific documentation.

Release-Specific Documents

Table 11 Product Documentation for Cisco Identity Services Engine

Document Title	Location
Release Notes for the Cisco Identity Services Engine, Release 1.4	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 1.4	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 1.4	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html
Cisco Identity Services Engine Hardware Installation Guide, Release 1.4	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html
Cisco Identity Services Engine Upgrade Guide, Release 1.4	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html
Cisco Identity Services Engine, Release 1.4 Migration Tool Guide	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html

Table 11 Product Documentation for Cisco Identity Services Engine (continued)

Document Title	Location
Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.4	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 1.4	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 1.4	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 3300 Series Appliance, Cisco Secure Access Control System 1121 Appliance, Cisco NAC Appliance, Cisco NAC Guest Server, and Cisco NAC Profiler	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.