Cisco Identity Services Engine Network Component Compatibility, Release 1.1.x

Revised: December 10, 2013, OL-26141-01

This document describes Cisco Identity Services Engine (ISE) compatibility with switches, wireless LAN controllers, and other policy enforcement devices, as well as client machine operating systems with which Cisco ISE interoperates in the network. This document covers the following topics:

Supported Network Access Devices

Cisco ISE supports interoperability with any (Cisco or non-Cisco) RADIUS client 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 "Configuring Authentication Policies" chapter of the *Cisco Identity Services Engine User Guide, Release 1.1.x*.

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

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

advanced functions like central web authentication (CWA), Change of Authorization (CoA), Security Group Access, and downloadable 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 that do not support RADIUS Change of Authorization (CoA) must use inline posture.

For information on enabling specific functions of Cisco ISE in your network switches, see the Switch Configuration Required to Support Cisco ISE Functions appendix of the *Cisco Identity Services Engine User Guide, Release 1.1.x*.

Note Some switch models and IOS versions may have reached their Cisco end-of-maintenance milestones, hence interoperability may not be fully supported for these switch types.

Caution To support the Cisco ISE Profiling service, Cisco recommends using the latest version of NetFlow (version 9), which has additional functionality that is needed to operate the Profiler. If you use NetFlow version 5 in your network, then you can use version 5 only on the primary NAD at the access layer, as it will not work anywhere else.

Table 1 Supported Network Access Devices

Device	Minimum OS Version	MAB	802.1X	Web Auth		Session CoA	VLAN	DACL	SGA	IOS Sensor
				CWA	LWA					
Access Switches										
Catalyst 2940	IOS v12.1(22)EA1	Yes	Yes	No	No	No	Yes	No	No	No
Catalyst 2950	IOS v12.1(22)EA1	No	Yes	No	No	No	Yes	No	No	No
Catalyst 2955	IOS v12.1(22)EA1	No	Yes	No	No	No	Yes	No	No	No
Catalyst 2960[1] ISR EtherSwitch ES2	IOS v 15.0.2-SE3 LAN Base	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Catalyst 2960[1], Catalyst 2960-S[1], Catalyst 2960-C	IOS v12.2(52)SE LAN Lite[2]	Yes	Yes	No	No	No	Yes	No	No	No
Catalyst 2970	IOS v12.2(25)SE	Yes	Yes	No	No	No	Yes	No	No	No
Catalyst 2975	IOS v12.2(52)SE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Catalyst 3550	IOS v12.2(44)SE	Yes	Yes	No	No	No	Yes	Yes	No	No
Catalyst 3560[1], Catalyst 3560-C[1]	IOS v12.2(52)SE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes 15.0 (1) SE
Catalyst 3560-E[1], ISR EtherSwitch ES3	IOS v12.2(52)SE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes 15.0 (1) SE
Catalyst 3560-X[1]	IOS v12.2(52)SE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes 15.0 (1) SE
Catalyst 3750[1]	IOS v12.2(52)SE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes 15.0 (1) SE

Table 1 Supported Network Access Devices (continued)

Device	Minimum OS Version	MAB	802.1X	Web Auth		Session CoA	VLAN	DACL	SGA	IOS Sensor
				CWA	LWA					
Catalyst 3750-E[1]	IOS v12.2(52)SE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes 15.0 (1) SE
Catalyst 3750 Metro[1]	IOS v12.2(52)SE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes 15.0 (1) SE
Catalyst 3750-X[1]	IOS v12.2(52)SE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes 15.0 (1) SE
Catalyst 3850[3]	3.2.2 SE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Catalyst 4500	IOS v12.2(54)SG1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Catalyst 6500	IOS v12.2(33)SXI6	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Data Center Switches										
Catalyst 4900	IOS v12.2(54)SG1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—
Nexus 7000[4]	—	—	—		—	—	Yes	—	Yes	—
Wireless (An ISE Inline Posture node is required if the WLC does not support CoA as discussed in Footnote #4. WLCs with the code specified in this table do support CoA without an ISE Inline Posture node) [5] [6]										
Wireless LAN Controller (WLC) 2100, 4400	7.0.116.0	No[7]	Yes	No	Yes	Yes	Yes	Yes	No	No
Wireless LAN Controller (WLC) 2500, 5500	7.2.103.0	No[6]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
WLC 7500 Series	7.2.103.0 (basic RADIUS auth supported in 7.0.116.0)	Yes[6]	Yes	No	Yes (local only)	No	Yes	No	No	No
WiSM1 Blade for 6500	7.0.116.0	No[6]	Yes	No	Yes	Yes	Yes	Yes	No	No
WiSM2 Blade for 6500	7.2.103.0	No[6]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
WLC for ISR (ISR2 ISM, SRE700, and SRE900)	7.0.116.0	No[6]	Yes	No	Yes	Yes	Yes	Yes	No	No
WLC for 3750	7.0.116.0	No[6]	Yes	No	Yes	Yes	Yes	Yes	No	No
ISR 88x, 89x Series	15.2(2)T	Yes	Yes	No	LWA (L3)	Yes	Yes	No	Yes (IPsec)	No
ISR 19x, 29x, 39x Series	15.2(2)T	Yes	Yes	No	LWA (L3)	Yes	Yes	Yes	Yes (IPsec)	No

[1] For 802.1X authentications, you need IOS version 12.2(55)SE3.

[2] Does not support posture and profiling services.

[3] For LWA, use the local pages of the switch or customize redirect pages on Cisco ISE with an external RADIUS server. For wireless LWA, edit the default authorization condition, WLC_Web_Authentication to check for Radius:Service-Type = Outbound & Radius:NAS-Port = Wireless IEEE 802.11.

[4] SGA only

5. Wireless LAN Controllers (WLCs) do not support downloadable ACLs (dACLs), but support named ACLs. WLCs prior to release 7.0.116.0 do not support CoA and require deployment of an ISE Inline Posture Node to support posture services. Use of Inline Posture Node requires WLC version 7.0.98 or later. Autonomous AP deployments (no WLC) also require deployment of an Inline Posture Node for posture support. Profiling services are currently supported for 802.1X-authenticated WLANs only on the WLC with CoA support. HREAP is not supported. WLCs do not currently support MAC Authentication Bypass (MAB).
6. An issue has been observed during wireless login scenarios where the WLC is running firmware version 7.0.116.0. Unless you require features available only in version 7.0.116.0, Cisco recommends returning your WLC firmware version to 7.0.98.218 or upgrade your WLC firmware version to 7.0.220.0. For more information, see the *Release Notes for Cisco Identity Services Engine, Release 1.1.x*.
7. Wireless Controllers support MAC filtering with RADIUS lookup. For WLCs that support version 7.2.103.0, there is support for session ID and COA with MAC filtering so it is more MAB-like.

AAA Attributes Required for Third-Party VPN Concentrators

For third-party VPN concentrators to integrate with Cisco ISE and Inline Posture nodes, the following 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

Table 2 lists the external identity sources supported with Cisco ISE.

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	—
LDAP Servers	
SunONE LDAP Directory Server	Version 5.2
Linux LDAP Directory Server	Version 2.4.23
Cisco NAC Profiler	Version 2.18 or later
Token Servers	
RSA ACE/Server	6.x series
RSA Authentication Manager	7.x series
Any RADIUS RFC 2865-compliant token server	—

[1] Cisco ISE OCSP functionality is available only on Microsoft Windows Active Directory 2008 and 2008 R2.

[2] Cisco ISE SCEP functionality is available only on Microsoft Windows Active Directory 2008 R2.

3. Microsoft Windows Active Directory version 2000 or its functional level are not supported by Cisco ISE.

RADIUS

Cisco ISE fully interoperates 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 Request For Comments (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 for Tunnel Protocol Support

Supported Administrative User Interface Browsers

You can access the Cisco ISE administrative user interface using the following browsers:

- Mozilla Firefox 3.6 (applicable for Windows, Mac OS X, and Linux-based operating systems)
- Mozilla FireFox 9 (applicable for Windows, Mac OS X, and Linux-based operating systems)
- Windows Internet Explorer 8
- Windows Internet Explorer 9 (in Internet Explorer 8 compatibility mode)

Note Cisco ISE GUI is not supported on Internet Explorer version 8 running in Internet Explorer 7 compatibility mode. For a collection of known issues regarding Windows Internet Explorer 8, see the "Known Issues" section of the *Release Notes for Cisco Identity Services Engine, Release 1.1.x*.

Note The minimum required screen resolution to view the Cisco ISE GUI and for a better user experience is 1280*800 pixels.

Supported Virtual Environments

Cisco ISE supports the following virtual environment platforms:

- VMware ESX 4.x
- VMware ESXi 4.x
- VMware ESXi 5.x

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

This section 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 your web browser.

Note All standard 802.1X supplicants can be used with Cisco ISE 1.1.x 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 “Managing Authentication Policies” chapter of the *Cisco Identity Services Engine User Guide, Release 1.1.x*.) 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 NAC Appliance and Identity Services Engine (ISE)

Cisco supports different versions of the NAC Agent for integration with NAC Appliance and ISE. Current releases are developed to work in either environment, however, interoperability between deployments is not guaranteed. Therefore, there is no explicit interoperability support for a given NAC Agent version intended for one environment that will necessarily work in the other. If you require support for both NAC Appliance and ISE using a single NAC Agent, be sure to test NAC Agent in your specific environment to verify compatibility.

Unless there is a specific defect or feature required for your NAC Appliance deployment, Cisco recommends deploying the most current agent certified for your ISE deployment. If an issue arises, Cisco recommends restricting the NAC Agent’s use to its intended environment and contacting Cisco TAC for assistance. Cisco will be addressing this issue through the standard Cisco TAC support escalation process, but NAC Agent interoperability is not guaranteed.

Cisco is working on an approach to address NAC Agent interoperability testing and support in an upcoming release.

Client Machine Operating Systems and Agent Support in Cisco ISE

This section lists the details for the following Operating Systems:

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

Table 3 Google Android [1]

Client Machine Operating System	Web Browser	Supplicants (802.1X)	Agent	VPN
Google Android 4.1.2	• Native browser • Mozilla Firefox 16	Google Android Supplicant 4.1.2	—	—
Google Android 4.0.4	• Native browser • Mozilla Firefox 5	Google Android Supplicant 4.0.4	—	—
Google Android 4.0.3	• Native browser • Mozilla Firefox 5	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 5	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 5	Google Android Supplicant 2.3.6	—	—
Google Android 2.3.3	• Native browser • Mozilla Firefox 5	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 5	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.

Table 4 Apple iOS [1]

Client Machine Operating System	Web Browser	Supplicants (802.1X)	Agent	VPN
Apple iOS 6.1	• Safari 6	Apple iOS Supplicant 6.1	—	—
Apple iOS 6	• Safari 6	Apple iOS Supplicant 6	—	—
Apple iOS 5.1	• Safari 5 • Mozilla Firefox 5	Apple iOS Supplicant 5.1	—	—
Apple iOS 5.0.1	• Safari 5 • Mozilla Firefox 5	Apple iOS Supplicant 5.0.1	—	—
Apple iOS 5.0	• Safari 5 • Mozilla Firefox 5	Apple iOS Supplicant 5.0	—	—

[1] While Apple iOS devices use PEAP with Cisco ISE or 802.1x, the public certificate includes a CRL distribution point that the iOS device needs to verify but cannot do it without network access. Click "confirm/accept" on the iOS device to authenticate to the network.

Table 5 **Apple Mac OS X**

Client Machine Operating System	Web Browser	Supplicants (802.1X)	Cisco ISE	Mac OS X Agent	VPN
Apple Mac OS X 10.5	• Apple Safari 4, 5 • Google Chrome 11, 12, 13, 14, 15, 16 [3] • Mozilla Firefox 3.6, 4, 5, 9	Apple Mac OS X Supplicant 10.5	1.1.4 1.1.3	4.9.0.659	AnyConnect version 3.0.08057, 2.5.3041[1]
			1.1.2 1.1.1	4.9.0.657	
Apple Mac OS X 10.6	• Apple Safari 4, 5 • Google Chrome 11, 12, 13, 14, 15, 16 [3] • Mozilla Firefox 3.6, 4, 5, 9	Apple Mac OS X Supplicant 10.6	1.1.4 1.1.3	4.9.0.659	AnyConnect version 3.0.08057, 2.5.3041[1]
			1.1.2 1.1.1	4.9.0.657	
Apple Mac OS X 10.7	• Apple Safari 5.1, 6.0[2] • Google Chrome 11, 12, 13, 14, 15, 16 [3] • Mozilla Firefox 3.6, 4, 5, 9	Apple Mac OS X Supplicant 10.7	1.1.4 1.1.3	4.9.0.659	AnyConnect version 3.0.08057
			1.1.2 1.1.1	4.9.0.657	
Apple Mac OS X 10.8	• Apple Safari 6.0, • Mozilla Firefox 14	Apple Mac OS X Supplicant 10.8	1.1.4 1.1.3	4.9.0.659	—
			1.1.2 1.1.1	4.9.0.657	

[1] Anyconnect version 2.5.3041 is required to support “PowerPC” Macintosh systems.

[2] Apple Safari version 6.0 is only supported on Mac OS X 10.7.4 and later versions of the operating system.

[3] 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	Cisco NAC Web Agent	VPN
Microsoft Windows 8 [2,3,4]						

Table 6 **Microsoft Windows [1]**

Client Machine Operating System	Web Browser	Supplicants (802.1X)	Cisco ISE	Cisco NAC Agent	Cisco NAC Web Agent	VPN
Windows 8 Windows 8 x64 Windows 8 Professional Windows 8 Professional x64 Windows 8 Enterprise Windows 8 Enterprise x64	• Microsoft IE 10	• Microsoft Windows 8 802.1X Client	1.1.4 1.1.3	4.9.0.52	4.9.0.28	AnyConnect version 3.1.00495
			1.1.2 1.1.1	4.9.0.47	4.9.0.27	

Table 6 Microsoft Windows [1]

Client Machine Operating System	Web Browser	Supplicants (802.1X)	Cisco ISE	Cisco NAC Agent	Cisco NAC Web Agent	VPN
Microsoft Windows 7[5]						
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 9, 10 [6] • Google Chrome 11, 12, 13, 14, 15, 16 • Mozilla Firefox 3.6, 4, 5, 9	• Microsoft Windows 7 802.1X Client • AnyConnect Network Access Manager	1.1.4 1.1.3	4.9.0.52	4.9.0.28	AnyConnect version 3.1.00495
			1.1.2 1.1.1	4.9.0.42	4.9.0.23	
Microsoft Windows Vista[5]						
Windows Vista SP1, SP2 Windows Vista x64 SP1, SP2	• Microsoft IE 6, 7, 8, 9 • Google Chrome 8, 9, 11, 12, 13, 14, 15, 16 • Mozilla Firefox 3.6, 4, 5, 9	• Microsoft Windows Vista 802.1X Client • Cisco Secure Services Client (SSC) 5.x • AnyConnect Network Access Manager	1.1.4 1.1.3	4.9.0.52	4.9.0.28	AnyConnect version 3.1.00495
			1.1.2 1.1.1	4.9.0.42	4.9.0.23	

Table 6 **Microsoft Windows [1]**

Client Machine Operating System	Web Browser	Supplicants (802.1X)	Cisco ISE	Cisco NAC Agent	Cisco NAC Web Agent	VPN
Microsoft Windows XP[5]						
Windows XP Media Center Edition, SP2, SP3 Windows XP Tablet PC, SP2, SP3 Windows XP Home, SP2 Windows XP Professional SP2, SP3 Windows XP Professional x64, SP2	• Microsoft IE 6, 7, 8, 9 • Google Chrome 11, 12, 13, 14, 15, 16 • Mozilla Firefox 3.6, 9	• Microsoft Windows XP 802.1X Client • Cisco Secure Services Client (SSC) 5.x • AnyConnect Network Access Manager	1.1.4 1.1.3	4.9.0.52	4.9.0.28	AnyConnect version 3.1.00495
			1.1.2 1.1.1	4.9.0.42	4.9.0.23	

1. It is recommended to use the Cisco NAC/Web Agent versions along with the corresponding Cisco ISE version.
2. 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.”)
3. When you create a Cisco ISE client provisioning policy to accommodate Windows 8, you must specify the “Windows All” operating system option.
4. Windows 8 RT is not supported.
5. Cisco ISE does not support the Windows Embedded operating systems available from Microsoft.
6. When Internet Explorer 10 is installed on Windows 7, to get full network access, you need to update to March 2013 Hotfix ruleset.

Table 7 **Others**

Client Machine Operating System	Web Browser	Supplicants (802.1X)	Agent	VPN
Red Hat Enterprise Linux (RHEL) 5	• Google Chrome 11 • Mozilla Firefox 3.6, 4, 5	No official support [1]	—	—
Ubuntu	Mozilla Firefox 3.6	No official support	—	—

1. Although not supported by Cisco, the WPA_Supplicant and Open1X Supplicant are available for use with Linux.

Supported Operating Systems and Browsers for Cisco ISE 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	Browser Versions
Google Android [1] 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 5, 16
Apple iOS 6.1, 6, 5.1, 5.0.1, 5.0	• Safari 5, 6
Apple Mac OS X 10.5, 10.6, 10.7, 10.8	• Mozilla Firefox 3.6, 4, 5, 9, 14, 16 • Safari 4, 5, 6 • Google Chrome 11
Microsoft Windows 8[2]	• Microsoft IE 10
Microsoft Windows 7[3]	• Microsoft IE 9, 10 [4] • Mozilla Firefox 3.6, 5, 9, 16 • Google Chrome 11
Microsoft Windows Vista, Microsoft Windows XP	• Microsoft IE 6, 7, 8 • Mozilla Firefox 3.6, 9, 16 • Google Chrome 5
Red Hat Enterprise Linux (RHEL) 5	• Mozilla Firefox 3.6, 4, 5, 9, 16 • Google Chrome 11
Ubuntu	Mozilla Firefox 3.6, 9, 16

[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] 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.”)

[3] Cisco ISE does not support the Windows Embedded 7 versions available from Microsoft.

[4] 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 login using Google Chrome on Windows 7 OS, the login fails. It is recommended to upgrade the browser to Chrome 11.

Supported Devices for On-Boarding and Certificate Provisioning Functions

This section provides the Bring Your Own Device (BYOD) support chart. 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 1.1.x* for any known issues or caveats.

Table 9 My Devices Portal - Supported Devices and Operating Systems

Device	Operating System	Single SSID	Dual SSID (open > PEAP (no cert) or open > TLS)	Onboard Method
Apple iDevice	iOS 4	No	Yes[1]	Apple profile configurations (native)
Apple iDevice	iOS 5, 6, and 6.1	Yes		
Android	2.2 and above[2]	Yes	Yes	Cisco Network Setup Assistant
Android Nook HD/HD+ (Amazon)	—	—	—	—
Windows	XP, Vista, Win7	Yes[3]	Yes	SPW from Cisco.com or Cisco ISE Client Provisioning feed
Windows	Win8		Yes	
Windows	Mobile 8, Mobile RT, Surface 8, and Surface RT	No	No	—
Mac OS X [4]	10.6, 10.7, 10.8	Yes	Yes	SPW from Cisco.com or Cisco ISE Client Provisioning feed
RIM BlackBerry	—	—	—	—

[1] Connect to secure SSID after provisioning

[2] There are known EAP-TLS issues with Android 4.1.1 devices. Contact your device manufacturer for support.

[3] 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.

[4] 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.

Documentation Updates

Table 10 Cisco Identity Services Engine Network Component Compatibility Documentation Updates

Date	Update Description
04/25/13	Cisco Identity Services Engine, Release 1.1.4
04/08/13	Updated the Cisco NAC Agent version for ISE 1.1.3 and added support for Internet Explorer 10 on Windows 7
03/12/13	Updated Client Machine Operating Systems and Agent Support in Cisco ISE, page 6

Table 10 Cisco Identity Services Engine Network Component Compatibility Documentation Updates

Date	Update Description
03/05/13	Updated Windows 8 editions in Supported Client Machine and Personal Device Operating Systems, Supplicants, and Agents, page 6
2/28/13	Cisco Identity Services Engine, Release 1.1.3
2/1/13	Added support for Apple iOS 6.1
10/29/12	Added editions of Windows to Cisco NAC Agent Interoperability Between NAC Appliance and Identity Services Engine (ISE), page 6
10/26/12	Added support for Windows 8
9/21/12	Added support for Apple iOS 6
7/27/12	Added support for Apple Mac OS X 10.8
7/10/12	Cisco Identity Services Engine, Release 1.1.1

Related Documentation

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

Release-Specific Documents

Table 11 lists the product documentation available for the Cisco ISE Release. General product information for Cisco ISE is available at http://www.cisco.com/go/ise. End-user documentation is available on Cisco.com at http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html.

Table 11 Product Documentation for Cisco Identity Services Engine

Document Title	Location
Release Notes for Cisco Identity Services Engine, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_release_notes_list.html
Cisco Identity Services Engine Network Component Compatibility, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html
Cisco Identity Services Engine User Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine Upgrade Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

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

Document Title	Location
Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
Cisco Identity Services Engine API Reference Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
Cisco Identity Services Engine Troubleshooting Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_troubleshooting_guides_list.html
Regulatory Compliance and Safety Information for Cisco Identity Services Engine, Cisco 1121 Secure Access Control System, Cisco NAC Appliance, Cisco NAC Guest Server, and Cisco NAC Profiler	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine In-Box Documentation and China RoHS Pointer Card	http://www.cisco.com/en/US/products/ps11640/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/en/US/products/ps11640/prod_installation_guides_list.html
- Cisco Secure ACS
  http://www.cisco.com/en/US/products/ps9911/tsd_products_support_series_home.html
- Cisco NAC Appliance
  http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html
- Cisco NAC Profiler
  http://www.cisco.com/en/US/products/ps8464/tsd_products_support_series_home.html
- Cisco NAC Guest Server
  http://www.cisco.com/en/US/products/ps10160/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.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.