



# Software Versions

**Revised: August 28, 2014**

**What’s New:** Updated Cisco ISE software version and the software versions for the Cisco 5508 and Flex 7500 Series WLCs.

The following tables highlight the hardware and software components used for validation testing in this design guide. While other software versions provide the required BYOD functionality, the Validated Software Version column indicates the software version used during the validation.

For specific feature support, consult the Cisco Feature Navigator: <http://www.cisco.com/go/fn>.

**Table C-1 Security**

Component	Role	Validated Software Version
Microsoft Active Directory	Server	Windows 2008 Server R2
Microsoft Certificate Authority	Server	Windows 2008 Server R2
Cisco Identity Services Engine	Authentication/Policy Server	ISE SW 1.2.0.899 patch 8
Cisco Prime Infrastructure	Management	1.4.1

**Table C-2 Wireless Access**

Component	Role	Validated Software Version
Cisco AP3702	Access Point	N/A
Cisco AP2702	Access Point	N/A
Cisco AP3602	Access Point	N/A
Cisco AP2602	Access Point	N/A
Cisco 5508 Wireless Controller	Wireless LAN Controller	AireOS 7.6.122.21
Cisco Flex 7500 Wireless Controller	Wireless LAN Controller	AireOS 7.6.122.21
Cisco Mobility Services Engine	Mobility Services Engine	MSE 7.6
Cisco 5760	Wireless LAN Controller	IOS XE 3.3.1SE

**Table C-2 Wireless Access**

Component	Role	Validated Software Version
Cisco Catalyst 3850	Campus and Branch Wireless Access	IOS XE 3.3.1SE
Apple iPad	Wireless Device	iOS 7.0.2
Apple iPhone	Wireless Device	iOS 6.1.4
Samsung Galaxy SIV	Wireless Device	Android 4.3
Samsung Galaxy Tab2	Wireless Device	Android 4.1.1

The document Cisco Identity Services Engine Network Component Compatibility, Release 1.2 provides a detailed description of which end user devices are supported ([http://www.cisco.com/en/US/docs/security/ise/1.2/compatibility/ise\\_sdt.html](http://www.cisco.com/en/US/docs/security/ise/1.2/compatibility/ise_sdt.html)).

**Table C-3 TrustSec**

Component	Role	Validated Software Version
CT5760	Centralized Wireless Lan Controller with support for inline tagging	IOS-XE 3.3.1SE
CT5508	Centralized Wireless Lan Controller with only SXP support	7.6.122.21
Catalyst 6500	6500 VSS Distributed Switch and Policy Enforcement point for Scenario #2	SUP2-T; 15.1.1.-SYI WS-X6904 Linecard with 10GE Modules (FourX Adapter)
C3850	Converged Access Switch with support for in line tagging	IOS-XE 3.3.1SE
Nexus 7000	Data Center Switches and policy enforcement point for Scenario #1	SUP2; 6.2(6) M1 Linecards; N7K-M108X2-12L F2e Linecard; N7K-F248XP-25E (only last 8 ports supporting MACsec)
Nexus 5548	Data Center Switch	5.2(1)N1(3)
Cisco Identity Services Engine	Authentication and Authorization RADIUS Server	1.2.0.899 patch 8
ASA Firewall	Policy enforcement for Deployment Scenario 2	9.0.2

**Table C-4 Cisco UC and Expressway Components**

Component	Role	Validated Software Version
Cisco Expressway	Expressway Core	X8.1.1
Cisco Expressway	Expressway Edge	X8.1.1
Unified CM	Call Processing	10.0.1

**Table C-4 Cisco UC and Expressway Components**

Component	Role	Validated Software Version
Unified IM and Presence	Instant Messaging, presence	10.0.1
Cisco ASA 5585X	VPN Concentrator	9.2(1)
Cisco Network Registrar	DHCP	8.1.3
Microsoft Active Directory/DNS	Directory and Domain Name Services	Windows 2008 R2
Jabber for Windows	Jabber Client	9.7
Jabber for iPhone and iPad	Jabber Client	9.6.2
Jabber for Mac	Jabber Client	9.6
Jabber for Android	Jabber Client	9.6.1
TelePresence EM/MX Series	Video Endpoint	TC 7.1.4

**Table C-5 Wired Access**

Component	Role	Validated Software Version
Catalyst 3560	Wired Access	IOS 15.2(1)E
Catalyst 3850	Campus/Branch	IOS XE 3.3.1SE
Catalyst 3750-X	Wired Access	IOS 15.2(1)E
Catalyst 4500E Sup7-E	Wired Access/Distribution	IOS XE 15.2(1)E
Catalyst 6500 VSS 1400 Catalyst 6500-E VSS4T	Campus Distribution/Core	IOS 15.1(1)SY1
Cisco Nexus® 7000 Sup1	Campus Core/Data Center	NX-OS 6.2.6
Apple MacBook Pro	Wired/Wireless Device	OSX 10.9.1 and 10.8.5
Windows Laptop	Wired/Wireless Device	Microsoft Windows 7 (64 bit)

**Table C-6 Remote Access**

Component	Role	Software Version
ASA 5520	VPN Concentrator	8.4(2)
AnyConnect	VPN Client Software	3.0

The three feature sets available with Cisco Catalyst 3850 Series Switches are:

- LAN Base—The LAN Base feature set offers enhanced intelligent services that include comprehensive Layer 2 features with up to 255 VLANs. It does not support either the wireless Mobility Agent (MA) or the Mobility Controller (MC) function.
- IP Base—Enterprise access Layer 3 switching features. The IP Base feature set provides entry-level enterprise services in addition to all LAN Base features with 1000 VLANs. IP Base also includes the support for wireless controller functionality (Mobility Agent (MA) and Mobility Controller (MC) role; additional access point license required for Mobility Controller role), routed access, smart operations, FNF, etc.

- IP Services—The IP Services feature set provides full enterprise services that include advanced Layer 3 features such as EIGRP, OSPF, BGP, PIM, and IPv6 routing such as OSPFv3 and EIGRPv6. Also supports the wireless controller functionality.

All software feature sets support advanced security and MQC-based QoS.

Customers can transparently upgrade the software feature set in the Cisco Catalyst 3850 Series Switches through Cisco IOS Software CLI using the right to use (RTU)-based software upgrade process. Software activation enables the Cisco IOS Software feature sets. Based on the license's type, Cisco IOS Software activates the appropriate feature set. License types can be changed, or upgraded, to activate a different feature set.

An access point license is required for Cisco Catalyst 3850 operating in Mobility Controller (MC) mode. No access point license is required for 3850 operating in Mobility Agent (MA) mode. This functionality is included in the IP Base feature set. Access point licenses can be transferred only between two Catalyst 3850 switches or between Catalyst 3850 switches and CT5760 wireless controllers and vice versa.

The Catalyst 3850 and CT 5760 running IOS XE 3.2.2 and higher software is compatible with CUWN software version 7.3.112 or 7.5 and higher—in order to support mobility interoperability.