Release Notes for the Cisco 5700 Series Wireless LAN Controller, Cisco IOS XE Release 3.3.xSE

First Published: October 7, 2013
Last Updated: January 30, 2015

OL-30703-05

This release note describes the features and caveats for the Cisco IOS XE 3.3.xSE software on the Cisco WLC 5700 Series.

Contents

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

Introduction

The Cisco 5700 Series Wireless LAN Controller (Cisco WLC 5700 Series) is designed for 802.11ac performance with maximum services, scalability, and high resiliency for mission-critical wireless networks. With an enhanced software programmable ASIC, the controller delivers wire-speed performance with services such as Advanced QoS, Flexible NetFlow Version 9, and downloadable ACLs enabled in a wireless network. The controller works with other controllers and access points to provide network managers with a robust wireless LAN solution. The Cisco WLC 5700 provides:

- Network traffic visibility through Flexible NetFlow Version 9
- Radio frequency (RF) visibility and protection
- Support for features such as CleanAir, ClientLink 2.0, and VideoStream

The Cisco IOS XE software represents the continuing evolution of the preeminent Cisco IOS operating system. The Cisco IOS XE architecture and well-defined set of APIs extend the Cisco IOS software to improve portability across platforms and extensibility outside the Cisco IOS environment. The Cisco IOS XE software retains the same look and feel of the Cisco IOS software, while providing enhanced future-proofing and improved functionality.

For more information about the Cisco IOS XE software, see
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps9442/ps11192/ps11194/QA_C67-622903.html

What's New

What's New in Cisco IOS XE Release 3.3.5SE

- Behavior change—When using PAP authentication, the MAC address of the client is presented in upper case characters as credential information to the AAA server. In previous releases, the MAC address was presented in lower case characters.

No features were added or enhanced for this release. For more information about updates in this release, see the "Caveats" section on page 21.

What's New in Cisco IOS XE Release 3.3.4SE

No features were added or enhanced for this release. For more information about updates in this release, see the "Caveats" section on page 21.

What's New in Cisco IOS XE Release 3.3.3SE

New Hardware Support

- Support for DWDM SFP+ and 10G ZR SFP+ modules. For a list of all supported SFP+ modules, see http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_6974.html.

CPP-Related Commands

- cpp [all | disable | system-default | traffic-type]
- show platform qos queue stats internal cpu policer

cpp [all | disable | system-default | traffic-type]

The **cpp** [**all | disable | system-default | traffic-type**] global configuration command for configuring Control Plane Policing (CPP) has been updated to include keywords for modifying CPP policer settings on CPU queues and for controlling the policer rate based on traffic types.

cpp [**all | disable | system-default | traffic-type** [*traffic-type* {**disable**}]]

all	(Optional) Enable policing on all CPU bound traffic.
disable	(Optional) Disable all CPU policing.

system-default	(Optional) Reset all CPU queues to system default policer rate values. Use the **show platform qos queue stats internal cpu** policer privileged EXEC command to display the system default values.
traffic-type [*traffic-type* {**disable**}]	(Optional) Set the CPU traffic type to police. • **disable**—Disable policing on the specified traffic type. Traffic types: • **broadcast**—Police broadcast traffic. • **dot1x**—Police IEEE 802.1x traffic. • **forus-packet**—Police forus packet traffic. Forus (or for-us) packets are packets destined to the router. • **icmp-redirect**—Police Internet Control Message Protocol (ICMP) redirect traffic. • **layer2-control**—Police Layer-2 control traffic. • **multicast-control**—Police multicast control traffic. • **multicast-data**—Police multicast data traffic. • **routing-control**—Police routing control traffic. • **snooping**—Police snooping traffic. • **software-forward**—Police software forward traffic. • **system-data**—Police system data traffic such as learning cache, RPF failure, GOLD, NFL sample. • **topology-control**—Police STP and STP topology control traffic. • **webauth** {*pps*}—Police web authentication traffic. – *pps*: The range is 100 pps to 13000 pps. • **wireless-iapp**—Police Cisco Inter Access Point Protocol (IAPP) traffic. • **wireless-mgmt**—Police wireless RFID, radio resource management (RRM), and probe management. • **wireless-mobility**—Police Control And Provisioning of Wireless Access Points (CAPWAP) mobility data and control traffic.

This example shows how to enable CPU queue policing on web authentication traffic at 1400 pps:

```
Switch(config)# cpp traffic-type webauth 1400
```

You can verify your setting by entering the **show platform qos queue stats internal cpu policer** privileged EXEC command. For information about this show command, see the "show platform qos queue stats internal cpu policer" section on page 5.

show platform qos queue stats internal cpu policer

The **show platform qos queue stats internal cpu policer** privileged EXEC command is a new command to display the configured Control Plane Policing (CPP) CPU queue and corresponding traffic TYPES.

Table 1 CPP CPU Queue Mapping in FED with Corresponding Traffic Types

CPU Queue	Traffic Type
WK_CPU_Q_L2_CONTROL	layer2-control
WK_CPU_Q_ROUTING_CONTROL	routing-control
WK_CPU_Q_MCAST_DATA	multicast-data
WK_CPU_Q_PROTO_SNOOPING	snooping
WK_CPU_Q_PUNT_WEBAUTH	webauth
WK_CPU_Q_SW_FORWARDING_Q	sw-fwd
WK_CPU_Q_WIRELESS_PRIO_1	capwap-control
WK_CPU_Q_WIRELESS_PRIO_3	wireless-iapp
WK_CPU_Q_WIRELESS_PRIO_4, WK_CPU_Q_WIRELESS_PRIO_5	wireless-misc
WK_CPU_Q_TOPOLOGY_CONTROL	topology-control
WK_CPU_Q_MCAST_END_STATION_SERVICE	multicast-snooping
WK_CPU_Q_LEARNING_CACHE_OVFL, WK_CPU_Q_EXCEPTION, WK_CPU_Q_CRYPTO_CONTROL, WK_CPU_Q_EGR_EXCEPTION, WK_CPU_Q_NFL_SAMPLED_DATA, WK_CPU_Q_SGT_CACHE_FULL, WK_CPU_Q_GOLD_PKT, WK_CPU_Q_RPF_FAILED	system-data
WK_CPU_Q_ICMP_REDIRECT	icmp-redirect
WK_CPU_Q_DOT1X_AUTH	dot1x
WK_CPU_Q_BROADCAST	broadcast
WK_CPU_Q_FORUS_TRAFFIC	forus

The **show platform qos queue stats internal cpu policer** command output shows the CPP policer settings (such as traffic types and CPP rates) on the CPU queues.

```
Switch# sh platform qos queue stats internal cpu policer

For Asic 0
 Queue                       Enabled   Rate(default)  Rate(set)       Drop
-------------------------------------------------------------------------
DOT1X Auth                    No       1000           1000             0
L2 Control                    No       500            500              0
Forus traffic                 No       1000           1000             0
ICMP GEN                      Yes      200            200              0
Routing Control               No       500            500              0
Forus Address resolution      No       1000           1000             0
ICMP Redirect                 No       500            500              0
WLESS PRI-5                   No       1000           1000             0
WLESS PRI-1                   No       1000           1000             0
```

WLESS PRI-2	No	1000	1000	0
WLESS PRI-3	No	1000	1000	0
WLESS PRI-4	No	1000	1000	0
BROADCAST	Yes	200	200	0
Learning cache ovfl	Yes	100	100	0
Sw forwarding	Yes	1000	1000	0
Topology Control	No	13000	13000	0
Proto Snooping	No	500	500	0
BFD Low Latency	No	500	500	0
Transit Traffic	Yes	500	500	0
RPF Failed	Yes	100	100	0
MCAST END STATION	Yes	2000	2000	0
LOGGING	Yes	1000	1000	0
Punt Webauth	No	1000	1000	0
Crypto Control	Yes	100	100	0
Exception	Yes	100	100	0
General Punt	No	500	500	0
NFL SAMPLED DATA	Yes	100	100	0
SGT Cache Full	Yes	100	100	0
EGR Exception	Yes	100	100	0
Show frwd	No	1000	1000	0
MCAST Data	Yes	500	500	0
Gold Pkt	Yes	100	100	0

What's New in Cisco IOS XE Release 3.3.2SE

No features were added or enhanced for this release.

What's New in Cisco IOS XE Release 3.3.1SE

- Support added for Cisco Aironet 3700 Series Access Points—The Cisco Aironet 3700 Series Access Points with the 802.11ac module is supported in this release. For more information about the AP, see http://www.cisco.com/en/US/products/ps13367/index.html.
- Wired Guest Access—Uses Ethernet in IP (RFC3378) within the centralized architecture to create a tunnel across a Layer 3 topology between two WLC endpoints. No additional protocols or segmentation techniques are needed to isolate guest traffic from the enterprise.

  Note For more information about Wired Guest Access, see http://www.cisco.com/en/US/docs/ios-xml/ios/ibns/configuration/xe-3se/3850/ibns-wired-guest-access.html.

- For information about open and resolved caveats, see "Caveats" section on page 21.

What's New in Cisco IOS XE Release 3.3.0SE

- Wireshark—A packet analyzer program that supports multiple protocols and presents information in a text-based user interface. Wireshark analyzes wired traffic and wireless traffic.
- Wired Guest Access—Uses Ethernet in IP (RFC3378) within the centralized architecture to create a tunnel across a Layer 3 topology between two WLC endpoints. No additional protocols or segmentation techniques are needed to isolate guest traffic from the enterprise.
- Service Discovery Gateway feature—Enables multicast Domain Name System (mDNS) to operate across Layer 3 boundaries by filtering, caching, and redistributing services from one Layer 3 domain to another. This feature enhances Bring Your Own Device (BYOD).
- Captive Portal Bypassing for Local Web Authentication—Support for Apple devices that need to resolve Wireless Internet Service Provider roaming (WISPr) and have support for captive portal bypass.
- Multicast Fast Convergence with Flex Links Failover feature—Reduces the convergence time of multicast traffic after a Flex Links failure.
- High Availability (HA)
  - Controller Stack—This release supports a stack of two controllers connected using the stack cable, working together using the Cisco StackWise-480 technology. The HA feature is enabled by default when the controllers are connected using the stack cable and the Cisco StackWise-480 technology is enabled.
  - Access Point Stateful Switchover—Controller supports 1000 access points and 12000 clients. When a switchover from the active controller to standby controller occurs, the access points continue to remain connected during the active-to-standby switchover. However, all the clients are deauthenticated and need to be reassociated with the new active controller.
- Client Count per WLAN—You can configure client limits per WLAN, per AP per WLAN, and per AP per Radio. The number of clients that you can configure for each WLAN depends on the platform that you are using.
- 802.11w support—Support for the 802.11w standard as defined by the Management Frame Protection (MFP) service. Disassociation, Deauthentication, and Robust Action frames increase Wi-Fi network security by protecting the management frames from being spoofed.
- 802.11r support in local mode—Support for IEEE Standard for fast roaming allows the handshake with the new access point before the client roams to the target access point. Allows clients to move between access points without breaking a session.
- Wi-Fi Direct Client Policy—Devices that are Wi-Fi Direct capable can connect directly to each other quickly and conveniently to do tasks such as printing, synchronization, and sharing of data. Wi-Fi Direct devices may associate with multiple peer-to-peer (P2P) devices and with infrastructure wireless LANs (WLANs) concurrently. You can use the controller to configure the Wi-Fi Direct Client Policy, on a per WLAN basis, where you can allow or disallow association of Wi-Fi devices with infrastructure WLANs, or disable Wi-Fi Direct Client Policy altogether for WLANs.
- Assisted Roaming—The 802.11k standard allows clients to request neighbor reports containing information about known neighbor access points that are candidates for a service set transition. The use of the 802.11k neighbor list can limit the need for active and passive scanning. The assisted roaming feature is based on an intelligent and client-optimized neighbor list.
- Support for IPv6 wireless clients—Client policies can have IPv4 and IPv6 filters.
- Support for 802.11ac module—The 802.11ac radio module, which is based on the IEEE 802.11ac Wave 1 standard, is available on the Cisco lightweight access points.

  The 802.11ac module provides enterprise-class reliability and wired-network-like performance. The 802.11ac module supports three spatial streams and 80 MHz-wide channels for a maximum data rate of 1.3 Gbps. The 802.11ac standard is a 5-GHz-only technology, which is faster and a more scalable version of the 802.11n standard.

- Application Visibility and Control—Classifies applications using deep packet inspection techniques with the Network-Based Application Recognition (NBAR2) engine and provides application-level visibility into Wi-Fi networks.

  Note The capability of dropping or marking the data traffic (control part) is not supported in the Cisco IOS XE 3.3.0SE.

- Security Enhancements
  - Manage Rogue devices—The controller continuously monitors all the nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) to determine if the rogue is attached to your network. For more information about managing rogue devices, see the "Managing Rogue Devices" section in the *System Management Configuration Guide*.
  - Classify rogue access points—The controller software enables you to create rules that can organize and display rogue access points as Friendly, Malicious, or Unclassified. For more information about classifying rogue access points, see the "Classifying Rogue Access Points" section in the *System Management Configuration Guide*.
  - wIPS—The Cisco Adaptive wireless intrusion prevention system (wIPS) continually monitors wireless traffic on both the wired and wireless networks and uses network intelligence to analyze attacks and more accurately pinpoint and proactively prevent attacks in the future. You can configure an access point to work in wIPS mode if the access point is in the Monitor or Local mode.
  - Radio Frequency Grouping—A radio frequency (RF) group is a logical collection of controllers that coordinate to perform radio resource management (RRM) in a globally optimized manner to perform network calculations on a per-radio basis. An RF group exists for each 802.11 network type. Clustering controllers into a single RF group enables the RRM algorithms to scale beyond the capabilities of a single controller.
- Lightweight Directory Access Protocol Server mode—Operates as the backend database for web authentication to retrieve user credentials and authenticate the user.
- Wireless Flexible NetFlow—Enables flow monitoring and control of wireless traffic.
- Enhanced QoS support for wireless IPv6 clients—Support for IPv6 ACLs and DSCP-matching of IPv6 packets.

Supported Hardware

Catalyst 3850 Switch Models

Table 2 Catalyst 3850 Switch Models

Switch Model	Cisco IOS Image	Description
WS-C3850-24T-L	LAN Base	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately)
WS-C3850-48T-L	LAN Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately)

Table 2 Catalyst 3850 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
WS-C3850-24P-L	LAN Base	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately)
WS-C3850-48P-L	LAN Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately)
WS-C3850-48F-L	LAN Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately)
WS-C3850-24T-S	IP Base	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Base feature set
WS-C3850-48T-S	IP Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Base feature set
WS-C3850-24P-S	IP Base	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Base feature set
WS-C3850-48P-S	IP Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Base feature set
WS-C3850-48F-S	IP Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, IP Base feature set
WS-C3850-24T-E	IP Services	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Services feature set
WS-C3850-24PW-S	IP Base	Cisco Catalyst 3850 24-port PoE IP Base with 5-access point license
WS-C3850-48PW-S	IP Base	Cisco Catalyst 3850 48-port PoE IP Base with 5-access point license
Catalyst 3850-12S-S	IP Base	12 SFP+ module slots, 1 network module slot, 350-W power supply
Catalyst 3850-24S-S	IP Base	24 SFP+ module slots, 1 network module slot, 350-W power supply
WS-C3850-48T-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Services feature set
WS-C3850-24P-E	IP Services	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Services feature set

Table 2 Catalyst 3850 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
WS-C3850-48P-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Services feature set
WS-C3850-48F-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, IP Services feature set
WS-3850-24U-E	IP Services	Cisco Catalyst 3850 Stackable 24 10/100/1000 Cisco UPOE ports,1 network module slot, 1100-W power supply
WS-3850-48U-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Cisco UPOE ports,1 network module slot, 1100-W power supply
Catalyst 3850-12S-E	IP Services	12 SFP+ module slots, 1 network module slot, 350-W power supply
Catalyst 3850-24S-E	IP Services	24 SFP+ module slots, 1 network module slot, 350-W power supply

Network Modules

Table 3 lists the three optional uplink network modules with 1-Gigabit and 10-Gigabit slots. You should only operate the switch with either a network module or a blank module installed.

Table 3 Supported Network Modules

Network Module	Description
C3850-NM-4-1G	Four 1-Gigabit small form-factor pleadable (SFP) module slots. Any combination of standard SFP modules are supported. SFP+ modules are not supported.
C3850-NM-2-10G	Four SFP module slots: • Two slots (left side) support only 1-Gigabit SFP modules and two slots (right side) support either 1-Gigabit SFP or 10-Gigabit SFP+ modules. Supported combinations of SFP and SFP+ modules: • Slots 1, 2, 3, and 4 populated with 1-Gigabit SFP modules. • Slots 1 and 2 populated with 1-Gigabit SFP modules and Slot 3 and 4 populated with 10-Gigabit SFP+ module.
C3850-NM-4-10G	Four 10-Gigabit slots or four 1-Gigabit slots. **Note** The module is supported only on the 48-port models.
C3850-NM-BLANK	No uplink ports.

Catalyst 3650 Switch Models

Table 4 Catalyst 3650 Switch Models

Switch Model	Cisco IOS Image	Description
Catalyst 3650-24TS-L	LAN Base	Stackable 24 10/100/1000 Ethernet downlink ports, four 1-Gigabit SFP (small form-factor pluggable) uplink ports, 250-W power supply
Catalyst 3650-48TS-L	LAN Base	Stackable 48 10/100/1000 Ethernet downlink ports, four 1-Gigabit SFP uplink ports, 250-W power supply
Catalyst 3650-24PS-L	LAN Base	Stackable 24 10/100/1000 PoE+[1] downlink ports, four 1-Gigabit SFP uplink ports, 640-W power supply
Catalyst 3650-48PS-L	LAN Base	Stackable 48 10/100/1000 PoE+ downlink ports, four 1-Gigabit SFP uplink ports, 640-W power supply
Catalyst 3650-48FS-L	LAN Base	Stackable 48 10/100/1000 Full PoE downlink ports, four 1-Gigabit SFP uplink ports, 1025-W power supply
Catalyst 3650-24US-L	LAN Base	Stackable 24 10/100/1000 Cisco UPOE downlink ports and four 1-Gigabit uplink ports
Catalyst 3650-48US-L	LAN Base	Stackable 48 10/100/1000 Cisco UPOE downlink ports and four 1-Gigabit uplink ports
Catalyst 3650-24TD-L	LAN Base	Stackable 24 10/100/1000 Ethernet downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 250-W power supply
Catalyst 3650-48TD-L	LAN Base	Stackable 48 10/100/1000 Ethernet downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 250-W power supply
Catalyst 3650-24PD-L	LAN Base	Stackable 24 10/100/1000 PoE+ downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 640-W power supply
Catalyst 3650-48PD-L	LAN Base	Stackable 48 10/100/1000 PoE+ downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 640-W power supply
Catalyst 3650-48FD-L	LAN Base	Stackable 48 10/100/1000 Full PoE downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 1025-W power supply
Catalyst 3650-24UD-L	LAN Base	Stackable 24 10/100/1000 Cisco UPOE downlink ports, and two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports
Catalyst 3650-48UD-L	LAN Base	Stackable 48 10/100/1000 Cisco UPOE downlink ports, and two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports

Table 4 Catalyst 3650 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
Catalyst 3650-48FQ-L	LAN Base	Stackable 48 10/100/1000 Full PoE downlink ports, four 10-Gigabit SFP+ uplink ports, 1025-W power supply
Catalyst 3650-48PQ-L	LAN Base	Stackable 48 10/100/1000 PoE+ downlink ports, four 10-Gigabit SFP+ uplink ports, 640-W power supply
Catalyst 3650-48TQ-L	LAN Base	Stackable 48 10/100/1000 Ethernet downlink ports, four 10-Gigabit SFP+ uplink ports, 250-W power supply
Catalyst 3650-24TS-S	IP Base	Stackable 24 10/100/1000 Ethernet downlink ports, four 1-Gigabit SFP uplink ports, 250-W power supply
Catalyst 3650-48TS-S	IP Base	Stackable 48 10/100/1000 Ethernet downlink ports, four 1-Gigabit SFP uplink ports, 250-W power supply
Catalyst 3650-24PS-S	IP Base	Stackable 24 10/100/1000 PoE+ downlink ports, four 1-Gigabit SFP uplink ports, 640-W power supply
Catalyst 3650-48PS-S	IP Base	Stackable 48 10/100/1000 PoE+ downlink ports, four 1-Gigabit SFP uplink ports, 640-W power supply
Catalyst 3650-48FS-S	IP Base	Stackable 48 10/100/1000 Full PoE downlink ports, four 1-Gigabit SFP uplink ports, 1025-W power supply
Catalyst 3650-24US-S	IP Base	Stackable 24 10/100/1000 Cisco UPOE downlink ports and four 1-Gigabit uplink ports
Catalyst 3650-48US-S	IP Base	Stackable 48 10/100/1000 Cisco UPOE downlink ports and four 1-Gigabit uplink ports
Catalyst 3650-24TD-S	IP Base	Stackable 24 10/100/1000 Ethernet downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 250-W power supply
Catalyst 3650-48TD-S	IP Base	Stackable 48 10/100/1000 Ethernet downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 250-W power supply
Catalyst 3650-24PD-S	IP Base	Stackable 24 10/100/1000 PoE+ downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 640-W power supply
Catalyst 3650-48PD-S	IP Base	Stackable 48 10/100/1000 PoE+ downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 640-W power supply
Catalyst 3650-48FD-S	IP Base	Stackable 48 10/100/1000 Full PoE downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 1025-W power supply

Table 4 Catalyst 3650 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
Catalyst 3650-24UD-S	IP Base	Stackable 24 10/100/1000 Cisco UPOE downlink ports, and two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports
Catalyst 3650-48UD-S	IP Base	Stackable 48 10/100/1000 Cisco UPOE downlink ports, and two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports
Catalyst 3650-48FQ-S	IP Base	Stackable 48 10/100/1000 Full PoE downlink ports, four 10-Gigabit SFP+ uplink ports, 1025-W power supply
Catalyst 3650-48PQ-S	IP Base	Stackable 48 10/100/1000 PoE+ downlink ports, four 10-Gigabit SFP+ uplink ports, 640-W power supply
Catalyst 3650-48TQ-S	IP Base	Stackable 48 10/100/1000 Ethernet downlink ports, four 10-Gigabit SFP+ uplink ports, 250-W power supply
Catalyst 3650-24TS-E	IP Services	Stackable 24 10/100/1000 Ethernet downlink ports, four 1-Gigabit SFP uplink ports, 250-W power supply
Catalyst 3650-48TS-E	IP Services	Stackable 48 10/100/1000 Ethernet downlink ports, four 1-Gigabit SFP uplink ports, 250-W power supply
Catalyst 3650-24PS-E	IP Services	Stackable 24 10/100/1000 PoE+ downlink ports, four 1-Gigabit SFP uplink ports, 640-W power supply
Catalyst 3650-48PS-E	IP Services	Stackable 48 10/100/1000 PoE+ downlink ports, four 1-Gigabit SFP uplink ports, 640-W power supply
Catalyst 3650-48FS-E	IP Services	Stackable 48 10/100/1000 Full PoE downlink ports, four 1-Gigabit SFP uplink ports, 1025-W power supply
Catalyst 3650-24US-E	IP Services	Stackable 24 10/100/1000 Cisco UPOE downlink ports and four 1-Gigabit uplink ports
Catalyst 3650-48US-E	IP Services	Stackable 48 10/100/1000 Cisco UPOE downlink ports and four 1-Gigabit uplink ports
Catalyst 3650-24TD-E	IP Services	Stackable 24 10/100/1000 Ethernet downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 250-W power supply
Catalyst 3650-48TD-E	IP Services	Stackable 48 10/100/1000 Ethernet downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 250-W power supply
Catalyst 3650-24PD-E	IP Services	Stackable 24 10/100/1000 PoE+ downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 640-W power supply

Table 4 Catalyst 3650 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
Catalyst 3650-48PD-E	IP Services	Stackable 48 10/100/1000 PoE+ downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 640-W power supply
Catalyst 3650-48FD-E	IP Services	Stackable 48 10/100/1000 Full PoE downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 1025-W power supply
Catalyst 3650-24UD-E	IP Services	Stackable 24 10/100/1000 Cisco UPOE downlink ports, and two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports
Catalyst 3650-48UD-E	IP Services	Stackable 48 10/100/1000 Cisco UPOE downlink ports, and two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports
Catalyst 3650-48FQ-E	IP Services	Stackable 48 10/100/1000 Full PoE downlink ports, four 10-Gigabit SFP+ uplink ports, 1025-W power supply
Catalyst 3650-48PQ-E	IP Services	Stackable 48 10/100/1000 PoE+ downlink ports, four 10-Gigabit SFP+ uplink ports, 640-W power supply
Catalyst 3650-48TQ-E	IP Services	Stackable 48 10/100/1000 Ethernet downlink ports, four 10-Gigabit SFP+ uplink ports, 250-W power supply
Catalyst 3850-24U-E	IP Services	Stackable 24 10/100/1000 Cisco UPOE ports, one network module slot, 1100-W power supply
Catalyst 3850-48U-E	IP Services	Stackable 48 10/100/1000 Cisco UPOE ports, one network module slot, 1100-W power supply

1. PoE+ = Power over Ethernet plus (provides up to 30 W per port).

Optics Modules

Catalyst switches support a wide range of optics. Because the list of supported optics is updated on a regular basis, consult the tables at this URL for the latest (SFP) compatibility information:

http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Cisco Wireless LAN Controller Models

Table 5 Cisco WLC 5700 Models

Part Number	Description
AIR-CT5760-25-K9	Cisco 5760 Wireless Controller for up to 25 Cisco access points
AIR-CT5760-50-K9	Cisco 5760 Wireless Controller for up to 50 Cisco access points
AIR-CT5760-100-K9	Cisco 5760 Wireless Controller for up to 100 Cisco access points
AIR-CT5760-250-K9	Cisco 5760 Wireless Controller for up to 250 Cisco access points
AIR-CT5760-500-K9	Cisco 5760 Wireless Controller for up to 500 Cisco access points
AIR-CT5760-1K-K9	Cisco 5760 Wireless Controller for up to 1000 Cisco access points
AIR-CT5760-HA-K9	Cisco 5760 Series Wireless Controller for High Availability

Access Points and Mobility Services Engine

Table 6 lists the supported products of the Cisco 5700 Series WLC.

Table 6 Cisco 5700 Series WLC Supported Products

Product	Platform Supported
Access Point	Cisco Aironet 1040, 1140, 1260, 1600, 2600, 3500, 3600, 3700
Mobility Services Engine	3355, Virtual Appliance

Table 7 lists the specific supported Cisco access points.

Table 7 Supported Access Points

Access Points	
Cisco Aironet 1040 Series	AIR-AP1041N
	AIR-AP1042N
	AIR-LAP1041N
	AIR-LAP1042N
Cisco Aironet 1140 Series	AIR-AP1141N
	AIR-AP1142N
	AIR-LAP1141N
	AIR-LAP1142N

Table 7 Supported Access Points (continued)

Access Points	
Cisco Aironet 1260 Series	AIR-LAP1261N
	AIR-LAP1262N
	AIR-AP1261N
	AIR-AP1262N
Cisco Aironet 1600 Series	AIR-CAP1602E
	AIR-CAP1602I
Cisco Aironet 2600 Series	AIR-CAP2602E
	AIR-CAP2602I
Cisco Aironet 3500 Series	AIR-CAP3501E
	AIR-CAP3501I
	AIR-CAP3501P
	AIR-CAP3502E
	AIR-CAP3502I
	AIR-CAP3502P
Cisco Aironet 3600 Series	AIR-CAP3602E
	AIR-CAP3602I
Cisco Aironet 3700 Series	AIR-CAP3702I
	AIR-CAP3702E
	AIR-CAP3702P

Wireless Web UI Software Requirements

- Operating Systems
  - Windows XP
  - Windows 7
  - Mac OS X
- Browsers
  - Google Chrome
  - Microsoft Internet Explorer
  - Mozilla Firefox

Software Mapping

Table 8 shows the mapping of the Cisco IOS XE version number and the Cisco IOS version number.

Table 8 Cisco IOS XE to Cisco IOS Version Number Mapping

Cisco IOS XE Version	Cisco IOSd Version	Cisco Wireless Control Module Version	Access Point Version
03.03.05SE	15.1(0)EZ5	10.1.150.0	15.2(4)JB7
03.03.04SE	15.0(1)EZ4	10.1.140.0	15.2(4)JB6
03.03.03SE	15.0(1)EZ3	10.1.130.0	15.2(4)JB5h
03.03.02SE	15.0(1)EZ2	10.1.121.0	15.2(4)JB3h
03.03.01SE	15.0(1)EZ1	10.1.110.0	15.2(4)JB2
03.03.00SE	15.0(1)EZ	10.1.100.0	15.2(4)JN

Software Compatibility Matrix

Table 9 lists the software compatibility matrix.

Table 9 Software Compatibility Matrix

Cisco 5700 WLC	Catalyst 3850	Catalyst 3650	Cisco 5508 WLC or WiSM2	MSE	ISE	ACS	Cisco PI
03.03.05SE	03.03.05SE	03.03.05SE	7.6	7.6	1.2	5.2, 5.3	2.1.2
03.03.04SE	03.03.04SE	03.03.04SE	7.6	7.6	1.2	5.2, 5.3	2.1.2
03.03.03SE	03.03.03SE	03.03.03SE	7.5	7.5			
03.03.02SE	03.03.02SE	03.03.02SE	7.6[1]	7.6	1.2	5.2, 5.3	2.1.1[3]
03.03.01SE	03.03.01SE	03.03.01SE	7.5[2]	7.5			2.0
03.03.00SE	03.03.00SE	03.03.00SE					

1. Cisco WLC Release 7.6 is not compatible with Cisco Prime Infrastructure 2.0.
2. Prime Infrastructure 2.0 enables you to manage Cisco WLC 7.5.102.0 with the features of Cisco WLC 7.4.110.0 and earlier releases. Prime Infrastructure 2.0 does not support any features of Cisco WLC 7.5.102.0 including the new AP platforms.
3. Prime Infrastructure 2.1.1 allows you to manage Cisco WLC Releases 7.5.102.0 and 7.6.x with the features of Cisco WLC 7.4.121.0 and earlier releases. Prime Infrastructure 2.1.1 does not support any features that are introduced in Cisco WLC Releases 7.5.102.0 and 7.6.x except the new access point platforms and the new mobility feature.

For more information on the compatibility of wireless software components across releases, see the *Cisco Wireless Solutions Software Compatibility Matrix*.

Interoperability with Other Client Devices

This section describes the interoperability of this version of the controller software release with other client devices.

Table 10 lists the client types on which the tests were conducted. The clients included laptops, handheld devices, phones, and printers.

Table 10 Client Types

Client Type and Name	Version
Laptop	
Intel 4965	11.5.1.15 or 12.4.4.5, v13.4
Intel 5100/6300	v14.3.0.6
Intel 6205	v14.3.0.6
Dell 1395/1397	XP/Vista: 5.60.18.8 Win7: 5.30.21.0
Dell 1505/1510/Broadcom 4321MCAG/4322HM	5.60.18.8
Dell 1515 (Atheros)	8.0.0.239
Dell 1520/Broadcom 43224HMS	5.60.48.18
Dell 1530 (Broadcom BCM4359)	v5.100.235.12
Cisco CB21	v1.3.0.532
Atheros HB95	7.7.0.358
MacBook Pro (Broadcom)	5.10.91.26
Handheld Devices	
Apple iPad	iOS 5.0.1
Apple iPad2	iOS 6.0.1
Apple iPad3	iOS 7.1.1(11D201)
Apple iPad Mini	iOS 7.1.1(11D201)
Samsung Galaxy Tab	Android 3.2
Intermec CK70	Windows Mobile 6.5 / 2.01.06.0355
Intermec CN50	Windows Mobile 6.1 / 2.01.06.0333
Symbol MC5590	Windows Mobile 6.5 / 3.00.0.0.051R
Symbol MC75	Windows Mobile 6.5 / 3.00.2.0.006R
Phones and Printers	
Cisco 7921G	1.4.2.LOADS
Cisco 7925G	1.4.2.LOADS
Ascom i75	1.8.0
Spectralink 8030	119.081/131.030/132.030
Vocera B1000A	4.1.0.2817
Vocera B2000	4.0.0.345
Apple iPhone 5	iOS 7.1.1(11D201)
Apple iPhone 5s	iOS 7.1.1(11D201)

Table 10 Client Types (continued)

Client Type and Name	Version
Apple iPhone 5c	iOS 7.1.1(11D201)
Apple iPhone 4	iOS 6.0.1
Apple iPhone 4S	iOS 6.0.1
Apple iPhone 5	iOS 6.0.1
Ascom i62	2.5.7
HTC Sensation	Android 2.3.3
Samsung Galaxy S II	Android 2.3.3
SpectraLink 8450	3.0.2.6098/5.0.0.8774
Samsung Galaxy Nexus	Android 4.0.2

Upgrading the Controller Software

To upgrade the Cisco IOS XE software, use the **software install** privileged EXEC command to install the packages from a new software bundle file. You can install the software bundle from the local storage media or it can be installed over the network using TFTP or FTP.

The **software install all**command expands the package files from the specified source bundle file and copies them to the local flash: storage device. When the source bundle is specified as a tftp: or ftp: URL, the bundle file is first downloaded into the switch's memory (RAM); the bundle file is not copied to local storage media.

After the package files are expanded and copied to flash: the running provisioning file (flash:packages.conf) is updated to reflect the newly installed packages, and the controller displays a reload prompt.

```
MC#software install file tftp://10.10.10.2/system1/ct5760-ipservicesk9.SPA.03.03.00.SE.150-1.EZ.bin
Preparing install operation ...
[1]: Downloading file tftp://10.10.10.2/system1/ct5760-ipservicesk9.SPA.03.03.00.SE.150-1.EZ.bin to active
switch 1
[1]: Finished downloading file tftp://172.19.26.230/kart/ct5760-ipservicesk9.SPA.03.03.00.SE.150-1.EZ.bin to
active switch 1
[1]: Starting install operation
[1]: Expanding bundle ct5760-ipservicesk9.SPA.03.03.00.SE.150-1.EZ.bin
[1]: Copying package files
[1]: Package files copied
[1]: Finished expanding bundle ct5760-ipservicesk9.SPA.03.03.00.SE.150-1.EZ.bin
[1]: Verifying and copying expanded package files to flash:
[1]: Verified and copied expanded package files to flash:
[1]: Starting compatibility checks
[1]: Finished compatibility checks
[1]: Starting application pre-installation processing
[1]: Finished application pre-installation processing
[1]: Old files list:
    Removed ct5760-base.SPA.03.02.03.SE.pkg
    Removed ct5760-drivers.SPA.03.02.03.SE.pkg
    Removed ct5760-infra.SPA.03.02.03.SE.pkg
    Removed ct5760-iosd-ipservicesk9.SPA.150-1.EX3.pkg
    Removed ct5760-platform.SPA.03.02.03.SE.pkg
    Removed ct5760-wcm.SPA.10.0.120.0.pkg
[1]: New files list:
    Added ct5760-base.SPA.03.03.00SE.pkg
    Added ct5760-drivers.SPA.03.03.00SE.pkg
    Added ct5760-infra.SPA.03.03.00SE.pkg
    Added ct5760-iosd-ipservicesk9.SPA.150-1.EZ.pkg
```

```
    Added ct5760-platform.SPA.03.03.00SE.pkg
    Added ct5760-wcm.SPA.10.1.100.0.pkg
[1]: Creating pending provisioning file
[1]: Finished installing software. New software will load on reboot.
[1]: Committing provisioning file

[1]: Do you want to proceed with reload? [yes/no]:
```

Features

The Cisco 5700 Series WLC is the first Cisco IOS-based controller built with smart ASIC for next generation unified wireless architectures. The Cisco 5700 Series WLC can be deployed both as a Mobility Controller (MC) in Converged Access solutions and as a Centralized Controller.

For more information about the features, see the product data sheet at this URL:

http://www.cisco.com/en/US/products/ps12598/products_data_sheets_list.html

Important Notes

- A switch stack containing a mix of Catalyst 3850 and Catalyst 3650 switches is not supported.
- Although visible in the CLI, the following commands are not supported:
  - **switchport mode dot1qtunnel**
  - **collect flow username**
  - **authorize-lsc-ap** (CSCui93659)
  - **show platform qos *xxx*** (CSCug09112)
- The following features are not supported in Cisco IOS XE Release 3.3.0SE:
  - Outdoor Access Points
  - Wired Guest Access

  Note Wired Guest Access is supported is the Cisco IOS XE Release 3.3.1SE.

  - Mesh, FlexConnect, and Office Extend Access Point deployment

Limitations and Restrictions

- Flex Links are not supported. We recommend that you use spanning tree protocol (STP) as the alternative.
- Restrictions for Cisco TrustSec:
  - Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.
  - Cisco TrustSec for IPv6 is not supported.
  - Dynamic binding of IP-SGT is not supported for hosts on Layer 3 physical routed interfaces because the IP Device Tracking feature for Layer 3 physical interfaces is not supported.
  - Cisco TrustSec cannot be configured on a pure bridging domain with IPSG feature enabled. You must either enable IP routing or disable the IPSG feature in the bridging domain.

– Cisco TrustSec on the controller supports up to 255 security group destination tags for enforcing security group ACLs.

Caveats

Cisco Bug Search Tool

The Bug Search Tool (BST), which is the online successor to Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat listed in this document:

1. Access the BST (use your Cisco user ID and password) at https://tools.cisco.com/bugsearch/.
2. Enter the bug ID in the **Search For:** field.

Open Caveats

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the "Cisco Bug Search Tool" section on page 21.

Bug ID	Severity	Headline
CSCuj92028	2	WCCP Crash @edison_wccp_cam_write_event_handler
CSCup12631	2	WebGUI displays WSMA errors on some pages after TACACS authentication
CSCup50293	2	5760 HA standby console access command lost after reboot
CSCup65522	3	5760 Anchor generates error for " %MM-3-INVALID_PKT_RECVD
CSCuq48800	2	Low throughput due to UAPSD for Intel 7260 WiFi chipset

Resolved Caveats in Cisco IOS XE Release 3.3.5SE

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the "Cisco Bug Search Tool" section on page 21.

Bug ID	Severity	Headline
CSCul46957	3	9M stack:Traceback@%OSAPI-5-MUTEX_UNLOCK_FAILED during switchover
CSCuo66526	2	wcm restart observed on 5760 with 3600 AP module
CSCup39353	2	IOSd reboots at @ ios_syncmgr_lock_pop_errmsg
CSCup86496	2	unicast ARP replies not destined to 3850 are forwarded to ARP module
CSCuq22460	3	COMMON-1-WDOG_CPUHOG: 1 fed: CPU usage time exceeded
CSCuq79546	1	IOSd reboots on 5760 running 3.3.4 at be_epm_redirect_cache_entry_get
CSCuq91035	3	5760 MIB support AP3700P AP model

Resolved Caveats in Cisco IOS XE Release 3.3.4SE

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the "Cisco Bug Search Tool" section on page 21.

Bug ID	Severity	Headline
CSCuc21859	2	Memory leak seen due to ESM (Embedded Syslog manager)
CSCuh88726	3	SNMP High CPU when polling lldpXMedLocMediaPolicy
CSCui65914	2	DATACORRUPTION-SP-1-DATAINCONSISTENCY copy error / 12.2(33)SRE6
CSCui69119	2	IPDT: rejected channel conf&Standby failed to boot up
CSCul43158	2	Random mobile disassociation with PEM unknown timeout
CSCum66082	2	IRCM:Client able to pass traffic in CWA_RE
CSCum66129	2	3850 not forwarding multicast traffic in layer 2 when PIM enabled on SVI
CSCum91301	1	IPDT: Standby crashes due to host table corruption
CSCun39810	2	Iosd Crash due to snmpProxy
CSCun92928	2	Must reboot controller for HotSpot WLAN to advertise IW IE; AP crashes
CSCuo14901	2	Crash/High CPU when enabling nbar for Flexible Netflow
CSCuo26294	2	WS-X45-SUP7-E crash with Process ffm: terminated abnormally
CSCuo38510	2	5760 WCM crash: Failed to send a msg to the msg queue object: SPAM-AP-Q
CSCuo43827	2	Guest portal does not load on foreign controller
CSCuo47903	1	No CWA redirect for client in case it roamed in webauth-reqd state
CSCuo48068	2	CSCuo48068 C5760 AP SSO 2nd controller keeps crashing
CSCuo63153	2	AP HA switchover Primary/secondary does not work on 3.3.3
CSCuo63950	2	WCM crash on customer production network
CSCuo81145	2	Client stuck in \"Idle\" on 5760 running 3.3.2SE
CSCuo86406	2	-D regulatory domain not supported with India (IN) country code in NGWC

Bug ID	Severity	Headline
CSCuo98816	2	Delete Payload not sent to previous AP when roaming to new AP
CSCup16325	2	5760 iosd stack crash
CSCup22590	2	Multiple Vulnerabilities in IOS/IOSd OpenSSL - June 2014
CSCup43034	2	WCM crash running 03.03.03
CSCup60078	2	7921/7925 phone not able to place call after failover
CSCup63909	2	Roaming fails when Anchored phone roams back from foreign.
CSCup73590	2	WCM crash in Mobility code.
CSCup76790	2	FNF flow doesn't age out after 50 days
CSCup91453	2	SNMP query cportQosStatsEntry with invalid ifindex prints hwidb is null
CSCup92808	2	No CWA redirect for client in case it roamed in webauth-reqd state
CSCuq09690	2	"no parameter-map" causes crash on 3.3.3 : auth_proxy_cache_redirect_url
CSCuq20970	2	Default multicast / broadcast forwarding mode cause latency
CSCuq25195	2	Adjust AFD for every client and BSSID add/del.
CSCuq29232	2	No CWA redirect for client if it roamed in webauth-reqd state
CSCuq32016	2	Incorrect AFD client ssid association
CSCuq38516	2	iosd crash at emweb_http_process

Resolved Caveats in Cisco IOS XE Release 3.3.3SE

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the "Cisco Bug Search Tool" section on page 21.

Bug ID	Severity	Headline
CSCtk68692	3	kron-initiated 'write mem' locks nvram indefinitely
CSCug75425	3	4500-Sup7E NTP synchronized but clock behind 5-8 seconds
CSCug92629	4	show tech-support | inc Sunil includes names
CSCuh56465	3	Span: Multiple SPAN source ports on the same switch not monitored
CSCuh59075	2	member switch crashed with tracebacks due to MEMBLK CORRUPTION
CSCui94876	3	Serviceability enhancement needed to identify the AVL tree getting full
CSCuj31712	3	certain Vendor Sfp force ports to err-disable upon OIR
CSCui94876	3	Serviceability enhancement needed to identify the AVL tree getting full
CSCuj31712	3	certain Vendor Sfp force ports to err-disable upon OIR
CSCuj51019	2	Alpha: FFM crash on member switch
CSCuj52086	3	SSID name does not get updated with fast ssid change in access-request.
CSCuj97492	3	Unable to easily swap AP primary/sec/Tertiary controller ip on wlc
CSCul44461	2	System failed to bootup due to initializationfailure + IOSd crash
CSCul47224	2	Traceback @ ngwc_dot1x_control_rcv when dot1x authentication starts
CSCul48578	3	Buffer sizing is different on odd and even physical interfaces on katana

Bug ID	Severity	Headline
CSCul66509	3	WLC 5760 GUI webpage error at first launch
CSCum07541	3	BYOD Guest client not joining the serving wlan sometimes.
CSCum09063	2	IOS system crash @ http_process
CSCum47451	2	3850 dACL is not applied on the stack member switch > 4
CSCum70737	2	3850 :: ACL definitions not consistent between stack master and members
CSCum81233	3	Config long vlan name cause tracback wcm_cs_debug_api + 780
CSCun10948	3	3850: Segfault with Process = ACL Logging Process
CSCun14712	3	5760 session timeout defaults and range are not shown properly in WebGUI
CSCun15859	2	Memory Leak ifm_send_ssid_update
CSCun22639	3	ip source guard with mac-check prevents DHCP
CSCun26520	3	HA Not able to Sync on 5760
CSCun29753	1	Acl crash seen in darya mr1
CSCun31450	2	IOSD-WATCHDOG: Process = IP SLAs XOS Event Processor IOSd crash
CSCun32266	2	ACL label leak with large scale webauth
CSCun36781	2	3850 - Service config configuration causes boot loop
CSCun40246	3	Dot1x along with WEP fails authentication only during re-auth
CSCun44526	1	Katana 12K wireless clients application tuning for WVU
CSCun46486	1	Darya MR2 crash on SNMP engine
CSCun48219	2	Crash on 3850 stack with DHCP snooping
CSCun48721	2	3850 responds to GARP not destined to it
CSCun55391	2	FED crash on 5760 3.3.1SE
CSCun62776	3	3850 crash with FED service at fnf_ffm_cache_stats_send
CSCun84970	3	3850 Every time diff wrap occurs, packet counter mismatch by 1
CSCun87876	2	multicast entries not synced completely to standby on IGMP leave
CSCun92474	3	EAPOL version should not always be V2
CSCun94333	3	5760 may send account stop after successful authentication with CWA
CSCun96020	2	5760 Client stuck in idle state
CSCun97822	3	Numeric VLAN name causing issues in wlan configuration with WebGUI.
CSCun98131	2	NG3K: Persistant snmp instance values for entity-mib
CSCuo01232	2	Clients not getting IP address at times when CPU utilization is high
CSCuo01236	2	CPU utilization is high with un-authenticated HTTPS redirected traffic
CSCuo14829	2	3850/03.03.02SE/Stuck Routing Control Q due to IPV6 MLD
CSCul31038	3	CSCul31038 NG3K: SNMP MAU-MIB support

Resolved Caveats in Cisco IOS XE Release 3.3.2SE

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the "Cisco Bug Search Tool" section on page 21.

Bug ID	Severity	Headline
CSCtq21722	1	SNMP crash forced due to an invalid memory block
CSCud17778	2	memory leak in middle buffers due to snmp traps
CSCui40588	2	GUI is not accesible after aaa authentication for http/s
CSCui75983	3	ingress policy match to wrong class-map after reboot
CSCuj58616	2	Katana memory leak in IOSd - ppcp_to_ppm_policy
CSCuj61051	2	wcm crash in process_spi_job_incoming () at ios_services
CSCuj81941	2	Katana-HA:PI template for 802.11a radio config pushed but failed to sync
CSCuj98181	2	Amur: Katana WCM crash at "osapiSemaPrioSet"
CSCul19814	2	SCHED-3-tHRASHING at fnf-rpc_context_wait_for_completion
CSCul21515	2	Client policing behaviour is unexpected for TCP traffic
CSCul26646	2	Scheduler data structure cleanup issue "process_watch_watched_message"
CSCul30304	2	Failed to allocate hardware resource(REP RI)
CSCul30792	2	SNMP memory leak when heavy polling is done continuously
CSCul31225	2	QoS:svi set policy not work
CSCul32843	2	5760 fed crash 3.3SE
CSCul39085	2	Memory corruption in rrm commit replication entry
CSCul54414	2	Unable to configure anything after adding few SNMP communities/host
CSCul54484	2	Memory leak in eicored
CSCul66968	2	Crash after bringing up a port-channel configured with mode on
CSCul79858	2	Darya:SNMP pulling 3-4 days cause the switch crash
CSCul84467	2	C3850:Stack:Port-Channel:Active Mem Switch Power Shut cause Traffic Loss
CSCul87219	3	Clients Blacklisted permanently
CSCum04129	2	lock assert & crash on removing vlan from vlan pool
CSCum21662	2	Darya:SNMP pulling 3-4 days cause the switch crash
CSCum59496	2	5760 reboots in openssl_dtls_server_setup
CSCum66933	2	Iosd crash observed on customer setup
CSCum78391	2	Controller crashes in WCM @apfMsAddToBlackList

Resolved Caveats in Cisco IOS XE Release 3.3.1SE

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the "Cisco Bug Search Tool" section on page 21.

Bug ID	Severity	Headline
CSCsl45701	3	TACACS+ per VRF authen failing: Address already in use
CSCuc63146	2	Port-channel interface flap when changing vlan allowed list
CSCud08538	2	WNBU-ALPHA: WCM crash on 2M at pthread_mutex_lock
CSCue49527	2	WLC should delete the session ID from PMK cache when client is removed
CSCug18767	6	LWA Captive Portal Bypass + Consent logout popup blocker support
CSCui69999	2	3850 crashes when switches in the stack have different images
CSCuj21417	2	AID leak causing Stale Client entries on WLC
CSCuj34025	2	HCA: AUP PDF page does not display in PDF format
CSCuj48089	2	3850 Stuck Broadcast Queue
CSCuj48889	2	CT5760 Crash due to eicore_ipc used up CPU
CSCuj51372	2	MacLearning not occuring for a group of 24 ports on 3850
CSCuj57007	2	HCA: DHCPACK with no DHCPOPT_LEASE_TIME option field should trigger IPDT
CSCuj78610	2	High cpu issue dueto process Auth-proxy HTTP, Web Auth client issue
CSCuj81949	2	WCM crash observed on customer controller
CSCuj91918	2	Number of MA RF members getting restricted to eight (8) on MC (5760)
CSCul03186	2	HCA: HotSpot Error intermittently on iPad
CSCul06456	3	Bowdoin cust requirement: need snmp OID support to create local net user
CSCul06619	2	Stale IPDT entries causing client to be stuck in DHCP reqd state.
CSCul13504	3	web-auth logout pop-up window disable support
CSCul27659	3	DHCP NAK sent as broadcast is causing issues in Guest (F-A) scenarios
CSCul27717	2	APs disassociate in large scale setup when debug commands are executed
CSCul30051	2	Clients failing auth (psk/dot1x) due to uncreated dot1x interface for AP

Resolved Caveats in Cisco IOS XE Release 3.3.0SE

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the "Cisco Bug Search Tool" section on page 21.

Bug ID	Severity	Headline
CSCua75283	2	%DATACORRUPTION-1-DATAINCONSISTENCY and router hang with Codenomicon
CSCuc12774	3	FA1 routes unicast flood traffic back out FA1
CSCuc95293	1	All external communications cease
CSCud11467	3	Apply in and out PV HQOS policy/remove input policy/output policy fails
CSCud11552	3	Change int BW/speed when HQOS policy is attached causes policy to detach

Bug ID	Severity	Headline
CSCud54501	3	'show policy-map interface wireless ap' counters not updating
CSCud54725	3	policy stops working after remove class from policy-map attached to intf
CSCud55333	3	port-shape not reaching shape rate for 10gig port
CSCud56426	2	webauth does not unbind logout ACLs in use once virtual ip is removed
CSCud60008	3	with Priority+policer change on fly cause some policy to be uninstalle
CSCud60070	3	”increase range for “”prio+ abs rate”” from 2G to 10G”
CSCud62982	3	PV with same child policy don’t work properly on some uplink ports
CSCud63110	3	Table-map set still present after remove agg-policiing with table child
CSCud63823	3	Delete share policy on 4x10G uplink port share policy on 1G stop work
CSCud65034	3	classification not work under parent user-defined class
CSCud71747	3	SNMP Issues in MO MC client tables
CSCud72626	2	per vlan policy failed to be removed with certain sequence
CSCuf86171	2	DHCP snooping database agent fails to start
CSCuf93185	3	Newton Uplink 1-G only port up even force change state to admin down
CSCug38523	2	WebUI: home screen takes 10-15 sec to load
CSCug41165	3	Copy-paste of wireless config drops characters from beginning of line
CSCug58178	3	wireless multicast traffic not sent to vlan defined by AP group on 3850
CSCuh20848	3	3850 shows %IPC-5-WATERMARK log messages repeatedly
CSCui59004	2	iosd crash while configuring no ntp server

Security Configuration Guides

Refer to this document for Cisco TrustSec support on the controller:
http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec.html.

These documentation links provide incorrect information about Cisco TrustSec on the controller:

- http://www.cisco.com/c/en/us/td/docs/wireless/controller/5700/software/release/3se/consolidated_guide/configuration_guide/b_multi_3se_5700_cg/b_multi_3se_5700_cg_chapter_01011001.html
- http://www.cisco.com/c/en/us/td/docs/wireless/controller/5700/software/release/3se/security/configuration_guide/b_sec_3se_5700_cg/b_sec_3se_5700_cg_chapter_011000.html

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at this URL:

http://www.cisco.com/en/US/support/index.html

Choose **Product Support > Wireless**. Then choose your product and click **Troubleshoot and Alerts** to find information for the problem that you are experiencing.

Related Documentation

- Cisco 5700 controller documentation at this URL:

  http://www.cisco.com/en/US/products/ps12598/tsd_products_support_series_home.html
- Cisco Validated Designs documents at this URL:

  http://www.cisco.com/go/designzone
- Error Message Decoder at this URL:

  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

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/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation*, which lists all new and revised Cisco Technical documentation, as an RSS feed and deliver content directly to your desktop using a read application. The RSS feeds are a free service.
