# Release Notes for Cisco 5760 Controller, Cisco IOS XE Release 3.2.xSE

**First Published: January 29, 2013**
**Last Modified: September 3, 2014**
**OL-28115-04**

This release note describes the features and caveats for the Cisco IOS XE 3.2.xSE software on the Cisco 5760 controller.

## Contents



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

# Introduction

The Cisco 5760 controller 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 wireless network. The controller works with other controllers and access points to provide network managers with a robust wireless LAN solution. The Cisco 5760 controller provides:

- Network traffic visibility through Flexible NetFlow Version 9
- 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 in Cisco IOS XE Release 3.2.3SE

## Cisco Prime Infrastructure (PI) 2.0

Cisco PI 2.0 manages both wired and wireless LAN devices such as Catalyst 3850 switches, Cisco 5760 controllers, Cisco 5500 series wireless controllers, and access points. PI 2.0 provides unified management for the features that are common to both switches and wireless controllers. After your devices are added to Prime Infrastructure, you can use the Initial Device Setup workflow to configure the wired and wireless features on switches and controllers.

For more details on PI 2.0, see the documents at this URL:

http://www.cisco.com/en/US/products/ps12239/tsd_products_support_series_home.html

## Captive Portal Bypassing for Local Web Authentication

In Cisco IOS XE Release 3.2.2SE, Apple devices that need to resolve Wireless Internet Service Provider roaming (WISPr) and have support for captive portal bypass could not get local web authentication. This issue is resolved in Cisco IOS XE Release 3.2.3SE.

If you have configured virtual IP resulting in a successful web authentication, but when you log out, you receive a popup window prompting you to click a link to log out, you can disable this popup by following these steps:

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal**<br>**Example:**<br>`Controller# configure terminal` | Enters global configuration mode. |
| Step 2 | **parameter-map type webauth** *map-name*<br>**Example:**<br>`Controller(config)# parameter-map type webauth named` | Configures a name for the parameter map and enters the parameter map configuration mode. |
| Step 3 | **type consent**<br>**Example:**<br>`Controller(config-params-parameter-map)# type consent` | Configures the parameter type as consent.<br>**Note** You can disable the popup window only if the parameter map type is configured as consent. |
| Step 4 | **logout-window-disabled**<br>**Example:**<br>`Controller(config-params-parameter-map)# logout-window-disabled` | Disables the web authentication logout popup window. |
| Step 5 | **end**<br>**Example:**<br>`Controller(config-params-parameter-map)# end` | Returns to privileged EXEC mode. |

For more information about captive portal bypassing, see http://www.cisco.com/en/US/docs/wireless/controller/7.5/config_guide/b_cg75_chapter_01010001.html

# What's New in Cisco IOS XE Release 3.2.2SE

## New and Enhanced GUI Features

In the earlier releases, the controller web user interface is accessed by entering http://*ipaddress* (the *ipaddress* is the controller IP address) in the browser. Now, you can enter http://*ipaddress*/wireless in the browser, which will also allow you to access the web user interface.

The controller web user interface is enhanced to support the following:

The Configuration Wizard—After initial configuration of the IP address and the local username/password or auth via the authentication server (privilege 15 needed), the wizard provides a method to complete the initial wireless configuration. Start the wizard through Configuration -> Wizard and follow the nine-step process to configure the following:

- Admin Users
- NMP System Summary
- Management Port
- Wireless Management
- RF Mobility and Country code

- Mobility configuration
- WLANs
- 802.11 Configuration
- Set Time

The Monitor tab:

- Displays summary details of controller, clients, and access points.
- Displays all radio and AP join statistics.
- Displays air quality on access points.
- Displays list of all Cisco Discovery Protocol (CDP) neighbors on all interfaces and the CDP traffic information.
- Displays all rogue access points based on their classification—friendly, malicious, ad hoc, classified, and unclassified.

The Configuration tab:

- Enables you to configure the controller for all initial operation using the web Configuration Wizard. The wizard allows you to configure user details, management interface, and so on.
- Enables you to configure the system, internal DHCP server, management, and mobility management parameters.
- Enables you to configure the controller, WLAN, and radios.
- Enables you to configure and set security policies on your controller.
- Enables you to access the controller operating system software management commands.

The Administration tab enables you to configure system logs.

# Enhanced Bring Your Own Device (BYOD) Support

When supporting personal devices on a corporate network, you must protect network services and enterprise data by authenticating and authorizing users and their devices. A Cisco Identity Services Engine (ISE) Advanced License provides the tools that you need to allow employees to securely use personal devices on a corporate network.

- Device Profiling—When a client device tries to associate with a WLAN, the controller collects information related to DHCP, RADIUS, HTTP, and so on and sends that information in the form of RADIUS packets to the Cisco Identity Services Engine (ISE). As a result, the client type can be determined.
- Single SSID and Dual SSID support—In the single SSID scenario, one SSID is used for certificate enrollment, provisioning, and network access. In the dual SSID scenario, one SSID provides certificate enrollment and provisioning and a second SSID provides secure network access. This certificate is used by the client to authenticate with the ISE EAPTLS protocols after it is provisioned in the first SSID (open). For more details, see the *Cisco Identity Services Engine User Guide* at this URL:

http://www.cisco.com/en/US/docs/security/ise/1.1.1/user_guide/ise_user_guide.html

## Fast SSID Changing

Fast SSID changing allows wireless clients to move from one SSID to another without delay. For more information, see Configuring Fast SSID Changing, page 33.

# Supported Hardware

## Catalyst 3850 Switch Models

*Table 1 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 350WAC 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 350WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately) |
| WS-C3850-24P-L | LAN Base | Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715WAC 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 715WAC 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 1100WAC 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 350WAC 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 350WAC 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 715WAC 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 715WAC power supply 1 RU, IP Base feature set |

*Table 1 Catalyst 3850 Switch Models (continued)*

| Switch Model | Cisco IOS Image | Description |
|---|---|---|
| WS-C3850-48F-S | IP Base | Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100WAC 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 350WAC power supply 1 RU, IP Services feature set |
| WS-C3850-48T-E | IP Services | Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350WAC 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 715WAC power supply 1 RU, IP Services feature set |
| WS-C3850-48P-E | IP Services | Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715WAC 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 1100WAC 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 |

# Network Modules

Table 2 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 2 Supported Network Modules*

| Network Module | Description |
|---|---|
| C3850-NM-4-1G | Four 1-Gigabit SFP module slots. Any combination of standard SFP modules are supported. SFP+ modules are not supported. |
| C3850-NM-2-10G | Four SFP module slots:<br>• 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.<br>Supported combinations of SFP and SFP+ modules:<br>• Slots 1, 2, 3, and 4 populated with 1-Gigabit SFP modules.<br>• Slots 1 and 2 populated with 1-Gigabit SFP modules and Slot 3 and 4 populated with 10-Gigabit SFP+ module. |

*Table 2 Supported Network Modules (continued)*

| Network Module | Description |
|---|---|
| C3850-NM-4-10G | Four 10-Gigabit slots or four 1-Gigabit slots.<br>**Note** This is only supported on the 48-port models. |
| C3850-NM-BLANK | No uplink ports. |

# Optics Modules

The Catalyst 3850 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 3 Cisco 5760 Controller 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 |

Table 4 lists the supported products of the 5760 controller.

*Table 4 Cisco 5760 Controller Supported Products*

| Product | Platform Supported |
|---|---|
| Access Point | Cisco Aironet 1040, 1140, 1260, 1600[1], 2600, 3500, 3600 |
| Mobility Services Engine | 3310, 3350, 3355, Virtual Appliance |
| Identity Services Engines (ISE) | ISE 1.1.1 on 3315, 3355, 3395 and Virtual Instance |
| Cisco Prime Infrastructure | Cisco Prime Infrastructure 2.0 |

1. AP 1600 will not work with 5508/WiSM2 as MC in converged access mode.

# Supported Access Points

Table 5 lists the specific supported Cisco access points.

*Table 5 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 |
| 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 |

# Compatibility Matrix

Table 6 lists the software compatibility matrix.

*Table 6 Software Compatibility Matrix*

| 5760 | Catalyst 3850 | 5508 or WiSM2 | MSE | ISE | ACS | Cisco PI |
|---|---|---|---|---|---|---|
| 3.2.0SE | 3.2.0SE | 7.3.112.0[1] | — | 1.1.1MR | 5.2 | NA |
| 3.2.1SE | 3.2.1SE | 7.3.112.0 | — | 1.1.3, 1.1.2 | 5.2, 5.3 | NA |
| 3.2.2SE | 3.2.2SE | 7.3.112.0 and the 7.5 Release | — | 1.1.3, 1.1.2 | 5.2, 5.3 | NA |
| 3.2.3SE | 3.2.3SE | 7.3.112.0 and the 7.5 Release | — | 1.1.3, 1.1.2 | 5.2, 5.3 | 2.0 |

1. IRCM Feature: Seamless roam between 5760 / 3850 and 5508 / WiSM2 with 7.3 MR1 running new mobility.

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

# Web UI System Requirements

## Software Requirements

- Supported Browsers
  - Google Chrome—Version 26.x
  - Microsoft Internet Explorer—Versions 8.x, 9.x and 10.x
  - Mozilla—Version 20.x

# Software Version

Table 7 shows the mapping of Cisco IOS XE version number and the Cisco IOS version number.

*Table 7 Cisco IOS XE to Cisco IOS Version Number Mapping*

| Cisco IOS XE Version | Cisco IOSd Version | Cisco Wireless Control Module Version | Access Point Version |
|---|---|---|---|
| 03.02.00SE | 15.0(1)EX | 10.0.100.0 | 152-2.JN |
| 03.02.01SE | 15.0(1)EX1 | 10.0.101.0 | 152-2.JN |
| 03.02.02SE | 15.0(1)EX2 | 10.0.111.0 | 152-2.JN |
| 03.02.03SE | 15.0(1)EX3 | 10.0.120.0 | 152-2.JN |

# Upgrading the Controller Software

For information about how to upgrade the controller software, see the *Cisco IOS File System, Configuration Files, and Bundle Files Appendix* at the following URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/system_management/appendix/swiosfs.html#wp1311040

# Features

The Cisco 5760 controller is the first Cisco IOS-based controller built with smart ASIC for next generation unified wireless architectures. The 5760 controller can be deployed both as a Mobility Controller (MC) in Converged Access solutions and as a Centralized Controller.

The device has these features:



## Scalability

- Supports up to 1000 access points and 12,000 wireless clients for business-critical wireless services.
- Multiple controllers can support up to 72,000 access points, and 864,000 wireless clients in a mobility group.

## High-Performance

- Optimized for 802.11ac standard
- 6 x 10-G SFP + ports
- Hardware-assisted processing to provide up to 60 Gbps throughput with services such as downloadable ACL, granular QoS queues, fairness algorithm, and NetFlow Version 9 processing

## High Resiliency

- Cisco 5760 controller supports primary/secondary/tertiary N+1 redundancy, multiple EtherChannels and FlexLinks.

## Cisco IOS-Based Controller

- Proven and security-hardened Cisco IOS operating system.
- Well-known Cisco IOS CLI allows users to leverage existing management tools for operations.
- The Cisco NetFlow eco-system allows users to leverage reporting, monitoring, traffic analysis, and troubleshooting tools for the wireless network.

## ClientLink 2.0

Cisco ClientLink 2.0 technology improves downlink performance to all mobile devices including one, two, and three-spatial-stream devices on 802.11n while improving battery life on mobile devices such as smartphones and tablets.

## CleanAir

Cisco CleanAir technology provides proactive, high-speed spectrum intelligence to combat performance problems due to wireless interference.

## RF Management

Provides both real-time and historical information about RF interference impacting network performance across controllers, via system-wide Cisco CleanAir technology integration.

## Comprehensive End-to-End Security

Offers control and provisioning of wireless access points (CAPWAP)-compliant DTLS encryption to ensure encryption between access points and controllers or between controllers.

## High Performance Video

- Optimized video delivery via a single stream for wireless clients.
- Supports Cisco VideoStream technology to optimize the delivery of business-critical multicast video applications across the WLAN.

## End-to-End Voice

- Supports Unified Communications for improved collaboration through messaging, presence, and conferencing.
- Supports all Cisco Unified Communications Wireless IP Phones for cost-effective, real-time voice services.

## Advanced QoS

- Consistent configuration CLI for wireless QoS through Modular QoS CLI (MQC).
- Granular QoS policies per AP, SSID, radio, and client.
- Fair bandwidth allocation across wireless clients on an AP.
- Leverages the Cisco IOS software and proprietary ASIC technology to provide line rate performance.

## Advanced ACL

- Supports both distributed and centralized Cisco IOS-based ACL policies.
- Simplifies and centralizes security policies through downloadable ACLs.
- ACLs are processed in hardware to provide line-rate performance.

## Flexible NetFlow v9

- Network-wide visibility with Flexible NetFlow for wireless clients.

## Mobility and Security

- Secure, reliable wireless connectivity and consistent end-user experience.
- Increased network availability through proactive blocking of known threats.

# IPv6

- Supports IPv6 addressing on interfaces with appropriate **show** commands for monitoring and troubleshooting.
- IPv6 ACLs are processed in hardware to provide line-rate performance.
- Supports IPv6 clients. The configuration for IPv6 mobility is the same as IPv4 mobility and requires no separate software on the client side to achieve seamless roaming.

# Wireless Features

Table 8 is a detailed list of wireless features supported on the device.

*Table 8 Wireless Features*

| Feature | Description |
|---|---|
| Layer 3 Mobility | Layer 3 roaming occurs when a station roams to a controller where the same VLAN or subnet is not available. |
| RRM | The Radio Resource Management (RRM) software embedded in the controller acts as a built-in RF engineer to consistently provide real-time RF management of your wireless network. |
| Port bundling | Port bundling is achieved through Cisco IOSd EtherChannel features including support for PAgP Port Aggregation Protocol (PAgP) and LACP (Link Aggregation Control Protocol). |
| Videostream | The VideoStream feature makes the IP multicast stream delivery reliable over the air, by converting the broadcast frame over the air to a unicast frame. |
| WMM call admission control (CAC) | CAC enables an access point to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi multimedia (WMM) protocol deployed in CCXv3 ensures sufficient QoS as long as the wireless LAN is not congested. However, to maintain QoS under differing network loads, CAC in CCXv4 is required. |
| Guest Services Internal Webauth | When a WLAN is configured to use the web policy, either for authentication or pass-through, the internal web server is invoked by default. |
| Guest Services External Webauth Centrally Switched | If an enterprise wants to use an external web server, the controller can be configured to redirect to it in place of using the internal server. The user database for the guest users can either be stored on the Wireless LAN Controller's local database, or might be stored external of the controller. |

*Table 8 Wireless Features (continued)*

| Feature | Description |
|---|---|
| Guest Anchor | The guest anchor controller is a controller dedicated to guest traffic.<br><br>The guest anchor controller is usually located in an unsecured network area, often called the demilitarized zone (DMZ). Other internal WLAN controllers from where the traffic originates are located in the enterprise LAN.<br><br>**Note** The Cisco 5760 controller can be a Guest Anchor; the Catalyst 3850 switch cannot be a guest anchor but it can be a foreign controller. You can use the Cisco 5508 Wireless Controller or the WiSM2 as a GA. |
| ACLs—dynamic on controller | ACLs on the WLC are meant to restrict or permit wireless clients to services on its WLAN. |
| ACLs—downloadable | You can create ACLs on the controller that can be assigned to groups and individual users based on the RADIUS authorization. Use ACLs to prevent unwanted traffic from entering the network. ACLs can filter source and destination IP addresses, transport protocols and more. |
| Data DTLS | Datagram Transport Layer Security (DTLS) is required to encrypt the data plane traffic. |
| Adaptive wIPS | The Cisco Adaptive Wireless Intrusion Prevention System (wIPS) is an advanced approach to wireless threat detection and performance management. It combines network traffic analysis, network device and topology information, signature-based techniques, and anomaly detection to deliver highly accurate and complete wireless threat prevention. |
| Enhanced Local Mode (ELM) | Local mode access points with a subset of wIPS capabilities is referred to as Enhanced Local Mode (ELM) access point or just ELM AP. |
| Rich RF (Clean Air, Client Link) | Cisco CleanAir technology, which provides proactive, high-speed spectrum intelligence to combat performance problems due to wireless interference. Cisco ClientLink 2.0 technology to improve downlink performance to all mobile devices including one, two, and three-spatial-stream devices on 802.11n while improving battery life on mobile devices such as smartphones and tablets. |
| Open/Static WEP | Controllers can control static WEP keys across access points. |

*Table 8 Wireless Features (continued)*

| Feature | Description |
|---|---|
| WPA-PSK | Wi-Fi Protected Access - Pre-Shared Key (WPA-PSK) is a data encryption specification for a WLAN that does not require an authentication server. Each wireless network device authenticates with the access point using the same 256-bit key generated from a password or passphrase. You can configure WPA parameters on the controller and specify the ASCII or HEX format of the preshared key. This key is used as the Pairwise Master Key (PMK) between the clients and the authentication server. |
| 802.1x (WPA/WPA2) | Wi-Fi Protected Access (WPA or WPA1) and WPA2 are standards-based security solutions from the Wi-Fi Alliance that provide data protection and access control for wireless LAN systems. WPA1 is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification; WPA2 is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard. By default, WPA1 uses Temporal Key Integrity Protocol (TKIP) and message integrity check (MIC) for data protection while WPA2 uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). Both WPA1 and WPA2 use 802.1X for authenticated key management by default. |
| MAC Authentication | You can configure the controller to start 802.1X authentication when MAC authentication with static WEP for the client fails. If MAC authentication is successful and the client requests for an 802.1X authentication, the client must pass the 802.1X authentication to be allowed to send data traffic. |
| CCKM Fast Roaming | Cisco Centralized Key Management (CCKM) uses a fast rekeying technique that enables clients to roam from one access point to another without going through the controller, typically in under 150 milliseconds (ms). CCKM reduces the time required by the client to mutually authenticate with the new access point and derive a new session key during reassociation. CCKM fast secure roaming ensures that there is no perceptible delay in time-sensitive applications such as wireless Voice over IP (VoIP), enterprise resource planning (ERP), or Citrix-based solutions. CCKM is a CCXv4-compliant feature. |

*Table 8 Wireless Features (continued)*

| Feature | Description |
|---|---|
| PMK Fast Roaming/OKC | In OKC (Opportunistic Active Key caching), the client and controller store one Pairwise Master Key Security Association (PMKSA). When the client roams, it calculates a new PMKID based on the PMKSA and sends the PMKID with the association request to the AP. The controller calculates the new PMKID based on PMKSA stored for the client. If both PMKIDs match, fast roaming is performed. |
| MIC | Manufactured-installed certificate is a type of certificate installed on the access points. |
| TACACS Accounting | The process of recording user actions and changes. |
| LDAP | An LDAP backend database allows the controller to query an LDAP server for the credentials (username and password) of a particular user. These credentials are then used to authenticate the user. For example, local EAP may use an LDAP server as its backend database to retrieve user credentials. |
| Rogue Detection/Classification | The controller software enables you to create rules that can organize and display access points as Friendly, Malicious, or Unclassified. |
| MFP (Client, Infrastructure) | Management frame protection (MFP) provides security for the otherwise unprotected and unencrypted 802.11 management messages passed between access points and clients. MFP provides both infrastructure and client support. |
| RLDP | The controller continuously monitors all 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. |
| QoS Markings | Quality of Service (QoS) Marking gives critical traffic preferential treatment to make sure it is delivered quickly and reliably. |

*Table 8 Wireless Features (continued)*

| Feature | Description |
|---|---|
| QoS TCLAS, SIP | The controller can perform traffic classification (TCLAS) to ensure that voice streams are properly classified. As LWAPP/CAPWAP data packets always use the same ports, 16666 and 5247 respectively, and the AP uses the outside QoS marking to determine which queue the packets should be placed in, using port-based QoS policies is inadequate. With TCLAS, even if the LWAPP/CAPWAP AVVID IP DSCP markings are incorrect, the traffic is tagged correctly. |
| Dot1p markings | You can configure 802.1p tagging for wired packets. Wireless packets are impacted only by the maximum priority level set for QoS. The tagged packets include CAPWAP data packets (between access points and the controller) and packets sent toward the core network. If a QoS profile has 802.1p tagging configured and if this QoS profile is assigned to a WLAN that uses an untagged interface on the controller, the client traffic will be blocked. |
| U-APSD | Unscheduled automatic power save delivery (U-APSD) is a QoS facility defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending battery life, this feature reduces the latency of traffic flow delivered over the wireless media. |
| TSPEC /CAC | Call Admission Control (CAC) enables an access point to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion. |
| Voice Diagnostics | The controller allows you to perform voice diagnostics and view debug messages between a maximum of two 802.11 clients. You can view details like TSPEC, RSSI, QoS/DSCP mapping and packet statistics information sent from the clients. |
| Voice metrics | You can generate reports on Traffic Stream Metrics (TSM) using the controller. The report displays TSM metrics such as time QoS, packet loss ratio (uplink and downlink), average queuing delay (uplink and downlink), roaming delay, roaming count, and percentage of queuing delay packets. |
| Multicast-Unicast | Unicast option configures the controller to use the unicast method to send multicast packets. |

*Table 8 Wireless Features (continued)*

| Feature | Description |
|---|---|
| Multicast-Multicast | Multicast option configures the controller to use the multicast method to send multicast packets to a CAPWAP multicast group. |
| DFS/802.11h | The Cisco UWN solution complies with regulations that require radio devices to use dynamic frequency selection (DFS) to detect radar signals and avoid interfering with them. |
| IPv6 (client mobility) | Internet Protocol version 6 (IPv6) is the next-generation network layer Internet protocol intended to replace version 4 (IPv4) in the TCP/IP suite of protocols. To support IPv6 clients across controllers, ICMPv6 messages must be dealt with specially to ensure the IPv6 client remains on the same Layer 3 network. |
| IPv6 RA guard | IPv6 clients configure IPv6 addresses and populate their router tables based on IPv6 Router Advertisement (RA) packets. The RA Guard feature is similar to the RA guard feature of wired networks. RA Guard increases the security of the IPv6 network by dropping the unwanted or rogue RA packets that come from wireless clients. |
| IPv6 DHCP guard | The IPv6 DHCP server guard feature prevents wireless clients from handing out IPv6 addresses to other wireless clients upstream. In order to prevent DHCPv6 addresses from being handed out, any DHCPv6 advertise packets from wireless clients are dropped. |
| RA throttling/Rate limit | RA throttling allows the controller to enforce limits to RA packets headed toward the wireless network. By enabling RA throttling, routers that send many RA packets can be trimmed to a minimum frequency that will still maintain an IPv6 client connectivity. |
| IPv6 ACL | IPv6 ACLs support the same options as IPv4 ACLs including source, destination, source and destination ports. |
| IPv6 Client Visbility | The addition of IPv6 client support to the Cisco Next Generation Wiring Closet (NGWC) feature maintains feature parity between IPv4 and IPv6 clients including mobility, security, guest access, quality of service, and endpoint visibility. |
| IPv6 Neighbor Discovery | IPv6 Neighbor Discovery is a set of messages and processes that determine relationships between neighboring nodes. Neighbor Discovery replaces ARP, ICMP Router Discovery, and ICMP Redirect used in IPv4. |

*Table 8 Wireless Features (continued)*

| Feature | Description |
|---|---|
| Syslog | A syslog server can be configured to allow:<br>• Receiving syslog messages through either TCP or UDP<br>• Full reliability because messages can be sent through TCP |
| CDP | The Cisco Discovery Protocol (CDP) is a device discovery protocol that runs on all Cisco-manufactured equipment. A device enabled with CDP sends out periodic interface updates to a multicast address in order to make itself known to neighboring devices. |
| WGB Support | A workgroup bridge (WGB) is a mode that can be configured on an autonomous Cisco IOS access point to provide wireless connectivity to a lightweight access point on behalf of clients that are connected by Ethernet to the WGB access point. |
| VLAN pooling per group | With VLAN select and VLAN pooling, there is a possibility that you might increase duplicate packets. |
| Passive Clients | Passive clients are wireless devices, such as scales and printers that are configured with a static IP address. These clients do not transmit any IP information such as IP address, subnet mask, and gateway information when they associate with an access point. As a result, when passive clients are used, the controller never knows the IP address unless they use the DHCP. |
| Band Select | Band Select addresses client distribution between the 2.4-GHz and 5-GHz bands by first understanding the client capabilities to verify whether a client can associate on both 2.4-GHz and 5-GHz spectrum. Enabling band select on a WLAN forces the AP to do probe suppression on the 2.4-GHz band that ultimately moves dual band clients to 5-GHz spectrum. |
| Peer-to-Peer blocking | Peer-to-peer blocking is applied to individual WLANs, and each client inherits the peer-to-peer blocking setting of the WLAN to which it is associated. You also have more control over how traffic is directed. |
| Client load balancing (Aggressive load balancing) | Enabling aggressive load balancing on the controller allows the controller to load balance wireless clients across access points. |

*Table 8 Wireless Features (continued)*

| Feature | Description |
|---|---|
| Client and RFID tag location (see Context aware) | The controller enables you to configure radio-frequency identification (RFID) tag tracking. RFID tags are small wireless devices that are affixed to assets for real-time location tracking. They operate by advertising their location using special 802.11 packets, which are processed by access points, the controller, and the mobility services engine. |
| Efficient AP upgrade | When upgrading the image of an AP, you can use the pre-image download feature to reduce the amount of time the AP is unavailable to serve clients. |
| HA SKU and licensing | A high availability SKU AIR-CT5760-HA-K9 is available to deploy as a redundant N+1 controller in case the primary controller goes down.<br>You do not need to purchase duplicate AP scale licensing on the redundant controller. |
| AAA override (VLAN and ACL) | When AAA Override option is set, the controller allows the RADIUS server to set VLAN or ACL on a per-MAC address basis and override the global values for the VLAN and ACL as configured on the WLAN. |
| Basic AAA functions | Authentication is used to ensure that the person attempting to use the device or service is authorized to use it according to the credentials configured. Authorization is used to configure the specific actions a user (or group of users) is allowed to perform on a device. Accounting is used for billing purposes to log the amount of packets or traffic forwarded through a device. |
| Posturing | A service that Cisco ISE provides is to scan endpoint compliancy; for example, AV/AS software installation and its definition file validity (known as Posture). |
| Extensible Authentication Protocol (EAP) Authentication | EAP is an authentication framework frequently used in wireless networks for providing transport and usage of keying material and parameters generated by EAP methods which include PEAP, EAP-FAST, TLS, and so on. |
| Accounting | Enables you to track the services that are accessed and the amount of network resources that are consumed. |

*Table 8 Wireless Features (continued)*

| Feature | Description |
|---|---|
| Device Profiling | Provides the functionality in discovering and determining the capabilities of all the attached endpoints on your network, regardless of their device types, to ensure and maintain appropriate access to your network. It primarily collects an attribute or a set of attributes of all the endpoints on network and classifies them according to their profiles. |
| Central Guest access | Allows a guest user to connect to a designated WLAN and access the guest network as configured by the administrator after completing the configured authentication. |
| Local Auth | Local auth is an authentication method that allows users and wireless clients to be authenticated locally on the switch/controller. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down. |
| Internal DHCP Server | The controllers contain an internal DHCP server. This server is typically used in branch offices that do not already have a DHCP server. The internal server provides DHCP addresses to wireless clients. |
| New Hierarchical Mobility | Allows a client to roam seamlessly between AireOS controllers running the maintenance Release 7.3.112.0 or Release 7.5 and Cisco controllers running Cisco IOS Release 3.2.xSE. |
| Web GUI | A web browser, or graphical user interface (GUI), is built into each controller. It allows multiple users to simultaneously browse into the controller HTTP or HTTPS (HTTP over SSL) management pages to configure parameters and monitor the operational status for the controller and its associated access points. |
| Fast Heart beat | Allows you to enable the fast heartbeat timer and reduce the amount of time it takes to detect a controller failure for all access points. |
| AP Fall back | Unlike Hot Standby Router Protocol (HSRP) standby, AP fallback disrupts wireless service while the AP failsover and then falls back to the configured (primary/secondary/tertiary) controller. |

*Table 8 Wireless Features (continued)*

| Feature | Description |
|---|---|
| AP Priority | During installation, we recommend that you connect all lightweight access points to a dedicated controller, and configure each lightweight access point for final operation. This step configures each lightweight access point for a primary, secondary, and tertiary controller. When sufficient controllers are deployed, if one controller fails, active access point client sessions are momentarily dropped while the dropped access point associates with another controller, which allows the client device to immediately reassociate and reauthenticate. |
| AP Priming | If the access point was previously associated to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point's nonvolatile memory. This process of storing controller IP addresses on an access point for later deployment is called priming the access point. |

# Interoperability with Other Client Devices

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

Table 9 lists the client types on which the tests were conducted. The clients included laptops, handheld devices, phones, and printers.

*Table 9 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 |

*Table 9 Client Types (continued)*

| Client Type and Name | Version |
|---|---|
| **Handheld Devices** | |
| Apple iPad | iOS 5.0.1 |
| Apple iPad2 | iOS 6.0.1 |
| Apple iPad3 | iOS 6.0.1 |
| 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 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 |

# Important Notes

- The following features are not supported in Cisco IOS XE Release 3.2.xSE:
  - Outdoor Access Points
  - Mesh, FlexConnect, and OEAP deployment
  - AP stateful switchover (SSO)
  - Wired Guest Access
  - Secure Group Access (SXP, SGT)

# Limitations and Restrictions

- For wired QoS policy modifications, detach input and output service policies under the interfaces, modify the policies, and re-attach to the interface.
- Although visible in the CLI, the **show platform qos** commands are not supported. (CSCug09112)

# Caveats

If you need information about a specific caveat that does not appear in these release notes, you can use the Cisco Bug Toolkit to find caveats of any severity. Click this URL to browse to the Bug Toolkit:

http://tools.cisco.com/Support/BugToolKit/

(If you request a defect that cannot be displayed, the defect number might not exist, the defect might not yet have a customer-visible description, or the defect might be marked Cisco Confidential.)

The following sections lists Open Caveats and Resolved Caveats for the Cisco 5760 controller, Cisco IOS XE Release 3.2.xSE.

## Open Caveats

- CSCua75283

  The following tracebacks are noticed on normal setup:

  ```
  DATACORRUPTION-1-DATAINCONSISTENCY: strstr_s: dmax exceeds max,  -PC= 0x240BE60Cz
  -Traceback= 190BA74z 182D4C8z 5E68CD5z 5E68B63z 55817EBz 55815D7z 558154Dz 5580E60z
  5580444z 55802CAz
  ```

  There is no workaround. There is no functional impact.

- CSCuc12774

  When the Ethernet management port receives a frame whose destination MAC address is not FA1, it does not drop the traffic. Instead, the port uses the vrf mgmtVrf routing table to route the traffic back.

  There is no workaround.

- CSCuc95293

  In very rare cases, all traffic to and from the controller ceases; all access points and LAG links disconnect as the controller fails to transmit the LACP PDUs; however, the management interfaces function.

  Run the **sh platform punt statistics port-asic 0 cpuq -1 direction tx** command to verify whether the suspend/unsuspend count is stuck for any of the transmission queues. Run the command several times to make sure that the suspend/unsuspend counters are no longer incrementing, and the TX suspend count = TX unsuspend count + 1. If you see this problem on any of the transmission queues, open a case with the TAC, or contact your Cisco technical support representative.

  There is no workaround. Reboot the controller.

- CSCud11467

  When the same PV HQOS policies are applied to both directions of an interface, the output policy stops working when the input policy is removed.

  The workaround is to detach the output policy and reapply it to the interface.

- CSCud11552

  After a HQOS policy is attached to interface and the interface speed or bandwidth is changed while the policy is attached, the HQOS policy gets detached from the interface.

  The workaround is to detach the policy, change the bandwidth or speed of the interface, and reattach the policy.

- CSCud37375

  No output is displayed on the USB console when the USB console cable is inserted after the image starts booting from the RJ-45 port.

  The workaround is to insert the USB console cable before booting the image from the RJ-45 port.

- CSCud40163

  Rogue Location Discovery Protocol (RLDP) does not work when the AP is in local mode. This problem occurs when there is no WLAN configured in controller or monitor mode AP.

  The workaround is to ensure that you configure one SSID on the controller when AP is in local mode. RLDP does not work when the AP is in monitor mode and there is no workaround.

- CSCud54501

  The class video counters for the AP port policy appear as zero when you use the **show policy-map interface wireless ap** command.

  There is no workaround.

- CSCud54725

  When a class is removed from a queuing policy map that is attached to a wired port, the queue programming in the hardware is removed.

  The workaround is to remove the policy from the port before making modifications.

- CSCud55333

  When the incoming rate is far beyond the rate configured in a policy map through policing, the traffic is not properly shaped.

  The workaround is to configure the policy map with priority level 1 percent and priority level 2 percent instead of configuring the policy with priority level x and policing.

- CSCud56426

  When you modify the webauth virtual IP while there are active webauth sessions, the session stays in the pending-delete state and you cannot create a new session.

  The workaround is to not make CLI changes when authorized webauth sessions are in use.

- CSCud60008

  When a policy with priority and a policer is attached to a range of interfaces on an uplink, in some scenarios, any change made to the policer rate causes the policy to be unprogrammed on one or more ports.

  The workaround is to remove the policy from the affected ports and reattach it.

- CSCud60070

  When configuring policy maps using absolute values, the maximum rate is limited to 2G/second.

  The workaround is to configure policy maps using the **priority level 1 percent *x*** command instead of configuring absolute values with the **priority level 1 *x*** command.

- CSCud62982

  When policers are attached to uplink interfaces using the **range** command, the policers do not always work.

  The workaround is to attach the policy to each port, one by one.

- CSCud63110

  In a hierarchical queueing policy, a table map under the child policy continues to mark traffic after the policy is detached from an interface.

  The workaround is to attach a default policy, for example:

```
policy-map trust-cos
     class class-default
     set cos cos table default
```

  You then detach it.

- CSCud63823

  After a queuing policy is deleted from one uplink port (10 G), the queueing policy on the other 1-G uplink stops working.

  The workaround is to detach the policy and reattach it.

- CSCud65034

  When using hierarchical policies, the child classification does not work properly when its matching value is a subset of the parent class's matching values for COS, DSCP, UP, and PREC classes.

  The workaround is to configure hierarchical policies to achieve one of these results:

  – The parent class has only class-default and the child class has user-defined classes.

  – The parent class has user-defined classes and the child has only class-default.

- CSCud69035

  The management port on the device may stop working when it is connected to a Fast Ethernet port.

  The workaround is to use the **shutdown** and **no shutdown** commands to clear and restart the management port.

- CSCud71747

  The **snmp get** command on cLMobilityExtMoMcLinkStatus for a given mobility controller (MC) and on cLMobilityExtMcAssocTime for a given mobility controller's client returns incorrect values.

  The workaround is to use the following commands:

  – **show wireless mobility oracle summary** to display the link status between the mobility oracle and the mobility controller

  – **show wireless mobility controller client summary** to display the client association time.

- CSCud72626

  After a per-VLAN policy is removed from a port, the policer stays active. The VLAN has an SVI with a policy attached that is performing a set.

  The workaround is to remove the policy from the SVI before removing it from the port.

- CSCud86642

  The Cisco 5760 controller console may stop responding on AIR-CT5760-6 with 5000 clients and high CPU usage after entering WLAN **shutdown** and **no shutdown** commands.

  The workaround is to SSH to the AIR-CT5760-6 instead of using direct Telnet to the console connection. You can also press **Ctrl**, **Shift-6**.

- CSCuf86171

  The DHCP snooping database agent fails to start while changing the DNS entry that the URL pointed to or when restarting the DHCP server. To avoid this issue, use another file transport mechanism like SCP or TFTP.

  The workaround is to reload the controller.

- CSCuf93185

  When a 1-G port on a Catalyst 3850 switch is connected to a 10-G port on a 5760 controller with a 1-G SFP module, the 10-G controller port stays up even when the switch port is shut down.

  There is no workaround.

- CSCug38523

  In WebUI, it takes up to 10 to 15 seconds for the home page to load.

  There is no workaround.

- CSCug41165

  If you copy and paste several wireless configuration lines into the configuration, the system drops the first few characters from every other line. The number of characters dropped appears to be related to how long the command takes to execute. The issue does not occur on non-wireless configuration lines.

  The workaround is to copy and paste line by line.

- CSCug58178

  Multicast traffic travels on the WLAN-mapped VLAN rather than on the AP-group mapped VLAN when an AP is placed in an AP group where VLAN is overridden for the SSID and a client associates with the AP that is broadcasting this SSID.

  There is no workaround.

- CSCuh20848

  The console displays %IPC-5-WATERMARK log messages repeatedly.

  There is no workaround. There is no functional impact.

- CSCuh25601

  ARP traffic is occasionally dropped. The ARP loss corresponds with buffer counter under “failures” incrementing in the output of **show platform punt client**.

  If IP device tracking is not required and neither dot1x or DAI is used, then the workaround is to add the **nmsp attachment suppress** command at the interface level of all switchports. This stops ARP snooping from being enabled on the ports.

- CSCui57827

  When a fiber interface is configured with the default configuration, the following error message is displayed:

  ```
  ETHCNTR-3-LOOP_BACK_DETECTED
  ```

  and the interface is placed in the error-disabled state.

  The workaround is to configure the interface with the **no keepalive** command.

- CSCui59004

  When the Network Time Protocol (NTP) configuration is removed from the controller, the Cisco IOS software unexpectedly halts.

  There is no workaround.

# Resolved Caveats



## Caveats Resolved in Cisco IOS XE Release 3.2.3SE

- CSCud06451

  During many simultaneous dot1x authentication operations, sessions may time out and fail to correctly authenticate. The console will continuously report authorization and authentication messages.

  There is no workaround.

- CSCuf77489

  The switch can crash when there are concurrent sessions and you try remove an existing password from the console or VTY. Various inconsistencies can be seen in the running configuration that can result in a crash.

  The workaround is to minimize configuration changes to the password, and to use a standalone switch when making such changes.

- CSCug75799

  All wireless clients become stuck in idle state. Once idle, the clients cannot reconnect to the wireless network. New clients can connect, but will become idle on disconnect.

  The workaround is to reload the affected device or stack and upgrade to release 3.3.0(SE) or greater.

- CSCug80708

  A port channel is in the “not connect” status when BPDU packets are received.

  There is no workaround.

- CSCug87540

  Layer 3 traffic routed on one switch or stack member fails for newly added devices.

  There is no direct workaround. Reload the impacted switch to recover.

- CSCug90789

  When the internal process takes more than 3 seconds to process the mobility state change request, the client can be stuck in local state on the foreign switch. As a result, traffic is not forwarded through the anchor; instead, traffic is forwarded through the foreign switch.

  There is no workaround.

- CSCuh09405

  When multiple activities such as the following are running in parallel, the controller may unexpectedly reboot.

  - multiple SSH sessions
  - multiple Telnet sessions
  - several invalid logins
  - multiple show-tech CLI commands executed

  There is no workaround.

- CSCuh09941

  There is an QoS ACL matching issue when multiple classes match in the ACL range.

  The workaround is to remove auto qos voip cisco-softphone from all attaching interfaces and then reattach the policy.

- CSCuh68137

  Katana-3.11.22-3500TSIM Clients for WLAN in client excluded state when with ACL.

  Workaround: Do not use an ACL.

- CSCuh90283

  Access Points cannot register to the 5760 controller when the wireless management VLAN is 1 and the SVI IP address is 172.16.140.230/231.

  The workaround is to use a different IP address in this subnet.

- CSCuh93075

  BW of the **show interfaces port-channel** privileged EXEC command does not display correctly.

  There is no workaround.

- CSCui23050

  The external webauth page redirect stops working after some time.

  The workaround is to reboot the system.

- CSCui40588

  After a TACACS authentication, the wireless GUI is not available on the switch.

  The workaround is to use CLI interface (Telnet, Console, SSH) and configure the device.

- CSCui43534

  The WLC5760 controller crashes during CWA client association when ISE is unreachable.

  Workaround:

  1. Configure backup radius.
  2. Remove mac filter.

- CSCui47662

  Segmentation fault crash in process cpf_msg_rcvq_process.

  There is no workaround.

- CSCuj25927

  fFED crash on a WLC5760 controller running 3.2.2 SE.

  There is no workaround.

- CSCuj31006

  Egress SSID policy does not install in FED.

  The workaround is to use default QoS.

- CSCuj51372

  In rare cases, Mac Learning does not occur for either ports 1-24 or ports 25-48 on one stack member in a switch stack. The other stack members are not affected.

  The workaround is to reload the affected stack member.

## Caveats Resolved in Cisco IOS XE Release 3.2.2SE

- CSCud25890

  The results of the **snmp get** command on the following MIBs in the cLWlanConfigTable are inconsistent:

  - cLWlanNACSupport
  - cLWlanScanDeferPriority
  - cLWlanNACPostureSupport
  - cLWlanWepKeyChange

  The **snmp set** command on the cLWlanNACSupport MIB does not work.

  The workaround is to use the **show wlan name** *profile name* command.

- CSCud36670

  The ranges for cLQd11aRadioMaxStreams/cLQd11bRadioMaxStreams and cLQd11aClientMaxStreams/cLQd11aClientMaxStreams do not start at 0. This situation occurs when you perform an **snmp set** on cLQd11aRadioMaxStreams or cLQd11bRadioMaxStreams under cLQd11aCACConfig. The same situation exists for a Radio type.

  There is no workaround.

- CSCud53860

  The **snmp get** command returns an incorrect value on bsnMobileStationWepState from bsnMobileStationTable.

  The workaround is to use the **show wlan name** *profile-name* command.

- CSCud57372

  After a roam operation, when you enter the **show policy** command, the police-conformed rate state under a child policy is displayed incorrectly.

  There is no workaround.

- CSCud68770

  When you perform a continuous SNMPWALK on the table's attributes, the output is inconsistent.

  When you perform a **set** on the cLD11ClientCalibTable, SNMPWALK gives the correct data for the first few minutes and then it does not return any data.

  There is no workaround.

- CSCud88714

  When a nonhierarchical policy is installed on SSID output and when you try to overwrite it with a new policy which is in a hierarchical format, the policy change fails. This problem occurs only when a nonhierarchical policy is overwritten with a hierarchical policy.

  The workaround is to unconfigure the existing policy and apply the new policy.

- CSCud94109

  If a client is roaming from Mobility Agent (MA) to Mobility Controller (MC) and joins another MA in a different peer group before complete authentication to MC, and then tries to rejoin to MC, the client entry cannot be deleted from the database. The client will not be able to join on the AP connected to MC but can join anywhere else in the network.

  The workaround is to use the **test platform llm clear-database** *client_mac_address* **true** command to remove the client entry on MC.

- CSCue44402

  The controller displays the following message:

  ```
  FRU Power Supply is not responding
  ```

  There is no workaround.

- CSCug23120

  The **show environment power all** command randomly displays a power supply failure message and displays the wattage is displayed incorrectly as 235 W.

  There is no workaround.

- CSCug52183

  When significant traffic (~ 4 billion packets) has traversed the CPU, the controller reloads unexpectedly. Depending on the control traffic pattern, it can take days or weeks for CPU-bound traffic to reach 4 billion. To check for this condition use the **show platform punt stat port-asic 0 cpuq -1 direction rx** command.

  There is no workaround.

- CSCug65693

  A Macbook client bug causes connectivity problems with a recent OS X update. This problem is triggered by the client sending an out of sequence packet.

  The workaround is to disable A-MPDU.

- CSCug85580

  When the **auto qos voip cisco-phone** command is applied to a port, data traffic over 10 (or 20) Mb/s is dropped at ingress ports.

  The workaround is to remove the policer from the following class-map policy:

  ```
  Service-policy input: AutoQos-4.0-CiscoPhone-Input-Policy
  Class AutoQos-4.0-Default-Class
        set dscp default
  ```

```
police cir 10000000 bc 8000 be 8000
  conform-action transmit
  exceed-action set-dscp-transmit dscp table policed-dscp
  violate-action drop
```

- CSCuh21506

  When the switch is in VTP client mode, all broadcast traffic is blocked for a given VLAN when a vtp prune event is immediately followed by a re-join event. ARP does not complete and consequently MAC addresses on upstream devices are not learned.

  The workaround is to set the VTP mode to transparent.

### Caveats Resolved in Cisco IOS XE Release 3.2.1SE

- CSCue76684

  In certain boot sequences, the BOOT variable is removed from the switch. At the next reboot attempt, the reboot fails, and the switch remains in the bootloader prompt.

  The workaround is to:

  – Boot the switch with **boot flash:***file_name* command.

    or

  – Set the BOOT variable explicitly in the bootloader using **BOOT=flash:***file_name* and, then boot the switch using boot command.

# Documentation Updates

## System Management Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)

### Configuring Fast SSID Changing

When the client sends a new association for a different SSID and fast SSID changing is disabled, the client entry in the controller connection table is cleared before the client is added to the new SSID. This means that the controller enforces a delay before clients are allowed to move to a new SSID. When fast SSID changing is enabled, there is no delay, and clients move more quickly from one SSID to another.

Beginning in privileged EXEC mode, follow these steps to configure fast SSID changing:

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal**<br>**Example:**<br>`Controller# configure terminal` | Enters global configuration mode. |

| | Command | Purpose |
|---|---|---|
| Step 2 | **wireless client fast-ssid-change**<br><br>**Example:**<br>`Controller(config)# wireless client fast-ssid-change` | Enables fast SSID change for wireless clients. |
| Step 3 | **end**<br><br>**Example:**<br>`Controller(config)# end` | Returns to privileged EXEC mode. |

# 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

For additional information about the Cisco controllers, see the documents at this URL:

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

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *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 reader application. The RSS feeds are a free service.

---

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