Release Notes for Cisco 5700 Series Wireless LAN Controller, Cisco IOS XE Release 3.7.xE

This document gives an overview of the features for the Cisco IOS XE 3.7.xE software on the Cisco 5700 Series Wireless LAN Controller.

Introduction

The Cisco 5700 Series Wireless LAN Controller (Cisco 5700 Series WLC) 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

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

Revision History

Table 1 Revision History

Modification Date	Modification Details
April 27, 2017	• Resolved Caveats in Cisco IOS XE Release 3.7.5E, page 29 Added: CSCus83638

What's New in Cisco IOS XE Release 3.7.5E

There are no features or enhancements in this release. For more information about updates in this release, see the "Caveats" section on page 28

What's New in Cisco IOS XE Release 3.7.4E

Support for –B Domain

The FCC (USA) rule making on 5 GHz released on April 1, 2014 (FCC 14-30 Report and Order) goes into effect for products that are sold or shipped on or after June 2, 2016. Cisco APs and Cisco WLCs will comply with the new rules by supporting the new regulatory domain (–B) for the US and will create new AP SKUs that are certified under the new rules. Examples of new rules include new 5-GHz band channels permitted for outdoor use, and transmission (Tx) power level increased to 1W for indoor, outdoor, and point-to-point transmissions.

Note Cisco APs and Cisco WLCs that are in the –A domain category can continue to operate and even coexist with –B domain devices without any issues.

We recommend that you upgrade Cisco APs and Cisco WLCs to the appropriate software release that supports –B domain.

–B Domain Compliant Cisco APs in this Release

- AP700
- AP702
- AP1532
- AP1570 (V02)
- AP1600
- AP1700
- AP1800
- AP2600
- AP2700

- AP3600
- AP3700

What's New in Cisco IOS XE Release 3.7.3E

- Support is added for the following access points:
  - Cisco Aironet 1850 Series Access Points
  - Cisco Aironet 1830 Series Access Points
- Support for HTTP Request—You can customize the HTML pages to send credentials through an HTTP GET Request.

Note We recommend password encryption while using an HTTP GET Request.

- Different Attributes in Long URL—The webauth parameter map supports external URLs with a maximum length of 256 characters. While configuring a login URL for web authentication, ensure that complete length of the redirected URL does not exceed 550 characters. Use the following commands to configure external webauth parameter map with long URL:

```
parameter-map type webauth external
type webauth
redirect for-login http://<login_url>/login.html
redirect on-failure http://failurepage.html
redirect on-success http://successpage.html
redirect portal ipv4 <external-webserver-ip-address>
```

- Multiple VLAN support for Wired Guest Access with both Anchor and Foreign as Cisco 5760 WLC—Wired guest anchor can now support multiple VLANs and multiple guest LANs. Separate VLANs can be assigned for each security profile like openauth, webauth and web consent. For more information about the Wired Guest Anchor feature, see "Multiple VLAN Support for Wired Guest Access with Cisco 5760 WLC as Both Anchor and Foreign Controller" section on page 3.

Multiple VLAN Support for Wired Guest Access with Cisco 5760 WLC as Both Anchor and Foreign Controller

Restrictions

- Wired guest VLAN on the access switch should not have any switch virtual interfaces (SVIs) present on any of the local switches. It should terminate directly on the foreign controller, so that the traffic is exported to the anchor.
- The anchor VLAN should not be allowed on the foreign controller's uplink. Doing so may result in unexpected behavior.
- The foreign and anchor guest LANs should not be on the same VLAN.
- Wired guest configuration should only be performed during scheduled network downtime period.

Overview

In enterprise networks, there is typically a need for providing network access to a network's guests on the campus. Guest access requirements include providing connectivity to the Internet or other selective enterprise resources to both wired and wireless guests in a consistent and manageable manner. The same wireless LAN controller can be used to provide access to both types of guests on the campus. For security reasons, a large number of enterprise network administrators segregate guest access to a demilitarized zone (DMZ) controller via tunneling. The guest access solution is also used as a fallback method for guest clients that fail dot1x and MAB authentication methods.

This document covers deployment of Wired Guest Access feature on Cisco 5760 WLC acting as Foreign Anchor and Cisco 5760 WLC acting as Guest Anchor in the DMZ. The feature works in a similar fashion on Cisco Catalyst 3650 switch acting as foreign controller.

A guest user connects to the designated wired port on an access layer switch for access. Optionally, it may be made to go through Web Consent or Web Authentication modes, depending upon the security requirements. After guest authentication succeeds, access is provided to the network resources and the guest controller manages the client traffic. Foreign controller is the primary switch where a client connects for network access; it also initiates tunnel requests. Guest anchor is the switch where a client gets anchored.

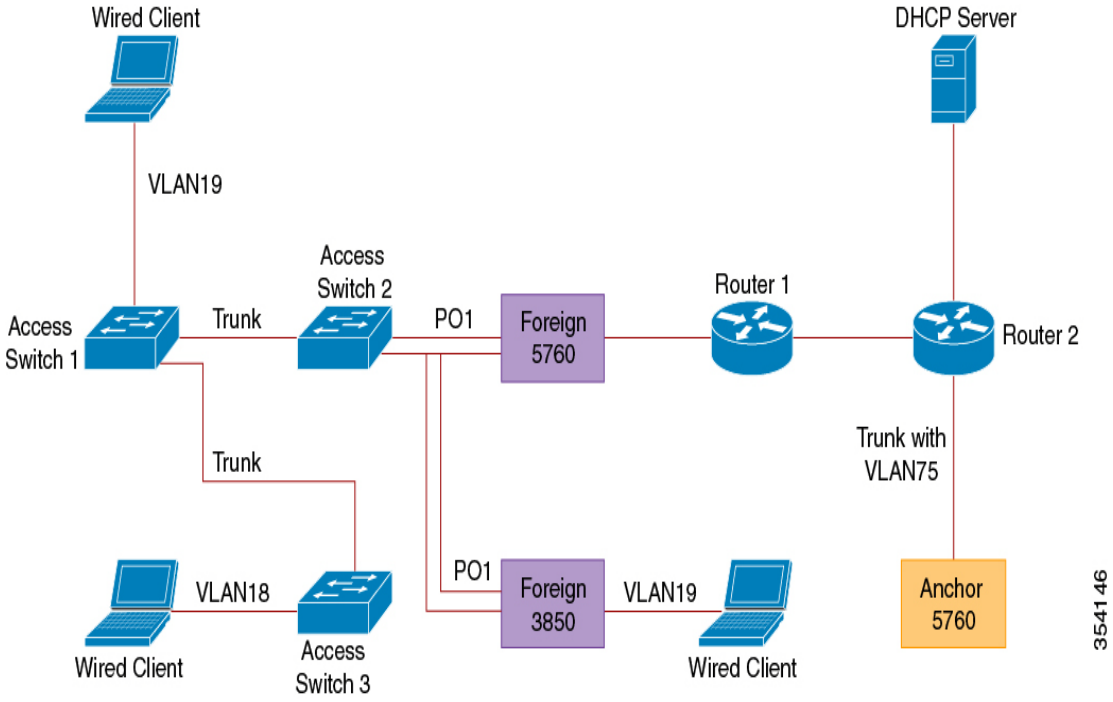
Before the guest access feature can be deployed, a mobility tunnel is established between the foreign anchor and guest anchor switches. The guest access feature works for both MC (Foreign Controller) to MC (Guest Anchor) and MA (Foreign Controller) to MC (Guest Anchor) models. The foreign anchor switch trunks wired guest traffic to the guest anchor controller. Multiple guest anchors can be configured for load balancing. The client is anchored to a DMZ anchor controller. It is also responsible for handling DHCP IP address assignment and authentication of a client. After the authentication is completed, the client is able to access the network.

Deployment Scenarios

The following sections describe common scenarios where the wired clients connect to access switches for network access. Two modes of access are explained with different examples. In both the methods, the wired guest access feature can act as a fallback method for authentication. This is typically a scenario where a guest user brings an end device that is unknown to the network. Since the end device is missing endpoint supplicant, it will fail the dot1x mode of authentication. Similarly, MAC authentication bypass (MAB) will also fail, as the MAC address of the end device is unknown to the authenticating server. It is worth noting that in such implementations, corporate end devices successfully get access to network as they would either have a dot1x supplicant or MAC addresses in the authenticating server for validation. This enables flexibility in deployment, because the administrator does not have to restrict and tie up ports specifically for guest access.

The figure below shows the topology used in this deployment scenario:

Figure 1-1 Wired Guest Access with Cisco 5760 WLC as Both Guest Anchor and Foreign Controller



Open Authentication

Guest Anchor Configuration

Step 1 Enable IP Device Tracking (IPDT) and Dynamic Host Configuration Protocol (DHCP) snooping on client VLANs (VLAN75). The client VLAN should be created in the guest anchor:

```
ip device tracking
ip dhcp relay information trust-all
ip dhcp snooping vlan 75
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
```

Step 2 Create VLAN 75 and a L3 VLAN interface:

```
vlan 75
interface Vlan75
ip address <layer-3-interface-ip-address>
ip helper-address <dhcp-server-ip-address>
ip dhcp pool DHCP_75
network <client-subnet>
default-router 75.1.1.1
lease 0 0 10
update arp
```

Step 3 Create a guest LAN specifying the client VLAN, with Cisco 5760 WLC acting as the mobility-anchor. (For openmode, use the **no security web-auth** command.)

```
guest-lan GUEST_LAN_OPENAUTH 3
client vlan 75
```

```
mobility anchor
no security web-auth
no shutdown
```

Foreign Configuration

Step 1 Enable DHCP and create a VLAN. The client VLAN need not be on the foreign controller.

```
ip dhcp relay information trust-all
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
ip device tracking
```

Step 2 The switch detects MAC address of the incoming client on the port channel configured with the **access-session port-control auto** command and applies the OPENAUTH subscriber policy. The OPENAUTH policy should be created first, as described below:

```
policy-map type control subscriber OPENAUTH
event session-started match-all
class always do-until-failure
activate service-template SERV-TEMP3-OPENAUTH
authorize
interface Po1
switchport trunk allowed vlan 19,137
switchport mode trunk
ip arp inspection trust
access-session port-control auto
service-policy type control subscriber OPENAUTH
ip dhcp snooping trust
end
```

Note The policy can be applied on the port where the end device is connected while the 3850/3650 is acting as the Foreign.

Step 3 Configure MAC learning on the foreign controller for the VLAN:

```
mac address-table learning vlan 19
```

Step 4 The OPENAUTH policy is referred to sequentially, which in this example points to a service template named SERV-TEMP3-OPENAUTH as defined below:

```
service-template SERV-TEMP3-OPENAUTH
tunnel type capwap name GUEST_LAN_OPENAUTH
```

Step 5 The service template contains a reference to the tunnel type and name. The VLAN 75 client should exist only on the guest anchor because it is responsible for handling client traffic:

```
guest-lan GUEST_LAN_OPENAUTH 3
client vlan 75
mobility anchor <anchor-ip-address>
no security web-auth
no shutdown
```

Step 6 A tunnel request is initiated from the foreign controller to the guest anchor for the wired client and a 'tunneladdsuccess' message is displayed to indicate that the tunnel build up process is completed.

On the access switch 1, a wired client connects to the Ethernet port that is set to access mode by the network administrator. It is portGigabitEthernet 1/0/11 in this example.

```
interface GigabitEthernet1/0/11
switchport access vlan 19
switchport mode access
```

Configuring WEBAUTH

Guest Anchor Configuration

Step 1 Enable IPDT and DHCP snooping on a client VLAN, in this example VLAN75 is created on the guest anchor.

```
ip device tracking
ip dhcp relay information trust-all
ip dhcp snooping vlan 75
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
```

Step 2 Create VLAN 75 and the L3 VLAN interface:

```
vlan 75
interface Vlan75
ip address <layer-3-interface-ip-address>
ip helper-address <dhcp-server-ip-address>
ip dhcp pool DHCP_75
network <client-subnet>
default-router <router-ip>
lease 0 0 10
update arp
```

Step 3 Configure the RADIUS server and the parameter map.

```
aaa new-model
aaa group server radius rad-grp
server Radius1
dot1x system-auth-control
aaa authentication dot1x default group rad-grp
radius server Radius1
address ipv4 172.19.45.194 auth-port 1812 acct-port 1813
timeout 60
retransmit 3
key radius
parameter-map type webauth <named-parameter-map>
type webauth
timeout init-state sec 5000
```

Step 4 Create a guest LAN specifying the client VLAN, with Cisco 5760 WLC acting as the mobility anchor:

```
guest-lan GUEST_LAN_WEBAUTH 3
client vlan VLAN0075
mobility anchor
security web-auth authentication-list default
security web-auth parameter-map <named-parameter-map>
no shutdown
```

Foreign Configuration

Step 1 Enable DHCP and create a VLAN. The client VLAN does not have to be set up on the foreign controller.

```
ip dhcp relay information trust-all
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
ip device tracking
```

Step 2 The switch detects MAC address of the incoming client on the port channel configured with **access-session port-control auto** command and applies the WEBAUTH subscriber policy. The WEBAUTH policy should be created first, as described below:

```
policy-map type control subscriber WEBAUTH
event session-started match-all
class always do-until-failure
activate service-template SERV-TEMP3-WEBAUTH
authorize
interface po1
switchport trunk allowed vlan 19,137
switchport mode trunk
ip arp inspection trust
access-session port-control auto
service-policy type control subscriber WEBAUTH
ip dhcp snooping trust
end
```

Step 3 MAC learning should be configured on the foreign controller for the VLAN:

```
mac address-table learning vlan 19
```

Step 4 The WEBAUTH policy is referred to sequentially, which in this example points to a service template named SERV-TEMP3-WEBAUTH, as defined below:

```
service-template SERV-TEMP3-WEBAUTH
tunnel type capwap name GUEST_LAN_WEBAUTH
```

Step 5 The service template contains a reference to the tunnel type and name. The client VLAN75 should exist only on the guest anchor as it is responsible for handling client traffic:

```
guest-lan GUEST_LAN_WEBAUTH 3
client vlan 75
mobility anchor 9.7.104.62
security web-auth authentication-list default
security web-auth parameter-map <named-parameter-map>
no shutdown
```

Step 6 A tunnel request is initiated from the foreign controller to the guest anchor for the wired client. A 'tunneladdsuccess' message is displayed to indicate that the tunnel build-up process is completed.

On access switch 1, a wired client connects to the Ethernet port that is set to access mode by the network administrator. It is portGigabitEthernet 1/0/11 in this example.

```
interface GigabitEthernet1/0/11
switchport access vlan 19
switchport mode access
```

Configuring OPENAUTH and WEBAUTH in Parallel

If you have two guest LANs and wants to assign them to different clients, base them on the VLANs on which the clients are learned.

Guest Anchor Configuration

Step 1 Enable IPDT and DHCP snooping on a client VLAN, in this case VLAN75. The client VLAN should be created on the guest anchor.

```
ip device tracking
ip dhcp relay information trust-all
ip dhcp snooping vlan 75
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
```

Step 2 Create VLAN 75 and the L3 VLAN interface:

```
vlan 75
interface Vlan75
ip address 75.1.1.1 255.255.255.0
ip helper-address 192.168.1.1
ip dhcp pool DHCP_75
network 75.1.1.0 255.255.255.0
default-router 75.1.1.1
lease 0 0 10
update arp
```

Step 3 Create a guest LAN specifying the client VLAN, with Cisco 5760 WLC acting as the mobility anchor. (For openmode, use the **no security web-auth** command.)

```
guest-lan GUEST_LAN_OPENAUTH 3
client vlan 75
mobility anchor
no security web-auth
no shutdown


guest-lan GUEST_LAN_WEBAUTH 4
client vlan VLAN0075
mobility anchor
security web-auth authentication-list method-list
security web-auth parameter-map <named-parameter-map>
no shutdown
```

Foreign Configuration

Step 1 Enable DHCP and create a VLAN. Note that the client VLAN need not have to be setup on the foreign controller.

```
ip dhcp relay information trust-all
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
ip device tracking
```

Step 2 The switch detects MAC address of the incoming client on the port channel configured with **access-session port-control auto** command and applies the DOUBLEAUTH subscriber policy. The vlan18, vlan19 class maps are explained in "Step4". Everything else is WEBAUTH. Using the second "always" class-map with "match-first" event, create the DOUBLEAUTH policy, as described below:

```
policy-map type control subscriber DOUBLEAUTH
event session-started match-first
class vlan19 do-until-failure
activate service-template SERV-TEMP3-OPENAUTH
authorize
class vlan18 do-until-failure
activate service-template SERV-TEMP4-WEBAUTH
authorize


interface po1
switchport trunk allowed vlan 19,137
switchport mode trunk
ip arp inspection trust
access-session port-control auto
service-policy type control subscriber DOUBLEAUTH
ip dhcp snooping trust
end
```

Step 3 Configure MAC learning on the foreign controller for VLAN 18 and VLAN 19.

```
mac address-table learning vlan 18 19
```

Step 4 The 'VLAN 18 and VLAN 19 class maps contain the VLAN match criteria based on which the guest LAN, under which the client falls in is differentiated.

```
class-map type control subscriber match-any vlan18
 match vlan 18

class-map type control subscriber match-any vlan19
 match vlan 19
```

Step 5 The OPENAUTH policy is referred to sequentially, which in this example points to a service template named SERV-TEMP3-OPENAUTH, as defined below:

```
service-template SERV-TEMP3-OPENAUTH
tunnel type capwap name GUEST_LAN_OPENAUTH
service-template SERV-TEMP4-WEBAUTH
tunnel type capwap name GUEST_LAN_WEBAUTH
```

Step 6 The service template contains a reference to the tunnel type and name. The VLAN 75 client should exist only on the guest anchor because it is responsible for handling client traffic:

```
guest-lan GUEST_LAN_OPENAUTH 3
client vlan 75
mobility anchor 9.7.104.62
no security web-auth
no shutdown


guest-lan GUEST_LAN_WEBAUTH 4
client vlan VLAN0075
mobility anchor 9.7.104.62
security web-auth authentication-list method-list
security web-auth parameter-map <named-parameter-map>
no shutdown
```

Step 7 A tunnel request is initiated from the foreign controller to the guest anchor for the wired client. A 'tunneladdsuccess' message is displayed to indicate that the tunnel build-up process is complete.

On the access swicth, there are multiple wired clients connecting to either VLAN 18 or VLAN 19, which can be then be assigned guest LANs accordingly.

```
interface GigabitEthernet1/0/11
switchport access vlan 19
switchport mode access
```

WEBAUTH Command Output Examples

- FOREIGN# **show wireless client summary**

```
Number of Local Clients : 2
MAC Address    AP Name                              WLAN State              Protocol
-------------------------------------------------------------------------------------
0021.ccbc.44f9 N/A                                   3    UP                 Ethernet
0021.ccbb.ac7d N/A                                  4   UP               Ethernet
```

- ANCHOR# **show mac address-table**

```
          Mac Address Table
-------------------------------------------

Vlan   Mac Address       Type       Ports
----   -----------       --------   -----
19   0021.ccbc.44f9   DYNAMIC     Po1
19   0021.ccbb.ac7d   DYNAMIC     Po1
```

- FOREIGN# **show access-session mac 0021.ccbc.44f9 details**

```
            Interface: Port-channel1
                IIF-ID: 0x83D880000003D4
          MAC Address: 0021.ccbc.44f9

          IPv6 Address: Unknown
          IPv4 Address: Unknown
            User-Name: 0021.ccbc.44f9
          Device-type: Un-Classified Device
                Status: Unauthorized
                Domain: DATA
        Oper host mode: multi-auth
      Oper control dir: both
      Session timeout: N/A
    Common Session ID: 090C895F000012A70412D338
      Acct Session ID: Unknown
                Handle: 0x1A00023F
        Current Policy: OPENAUTH
        Session Flags: Session Pushed

Local Policies:
        Service Template: SERV-TEMP3-OPENAUTH (priority 150)
Tunnel Profile Name: GUEST_LAN_OPENAUTH
          Tunnel State: 2
Method status list:
        Method           State
```

```
       webauth         Authc Success
```

- ANCHOR# **show wireless client summary**

```
Number of Local Clients : 1

MAC Address    AP Name                             WLAN State              Protocol
-------------------------------------------------------------------------------
0021.ccbc.44f9 N/A                                  3    WEBAUTH_PEND       Ethernet
0021.ccbb.ac7d N/A                                 4   WEBAUTH_PEND       Ethernet
```

- ANCHOR# **show wireless client summary**

```
Number of Local Clients : 2

MAC Address    AP Name                             WLAN State              Protocol
-------------------------------------------------------------------------------
0021.ccbc.44f9 N/A                                  3    UP                 Ethernet
0021.ccbb.ac7d N/A                                  4   UP                 Ethernet
```

- ANCHOR# **show mac address-table**

```
          Mac Address Table
-------------------------------------------

Vlan   Mac Address       Type       Ports
----   -----------       --------   -----
19   0021.ccbc.44f9   DYNAMIC     Po1
18   0021.ccbb.ac7d   DYNAMIC     Po1
```

- ANCHOR# **show wireless client summary**

```
Number of Local Clients : 1

MAC Address   AP Name                            WLAN State              Protocol
-------------------------------------------------------------------------------
0021.ccbc.44f9 N/A                                  3   UP                 Ethernet
0021.ccbb.ac7d N/A                                  4   UP                 Ethernet
```

- ANCHOR# **show access-session mac 0021.ccbc.44f9**

```
Interface   MAC Address   Method Domain Status Fg Session ID
-----------------------------------------------------------------------
Ca1         0021.ccbc.44f9 webauth DATA   Auth     090C895F000012A70412D338
```

- ANCHOR# **show access-session mac 0021.ccbc.44f9 details**

```
           Interface: Capwap1
               IIF-ID: 0x6DAE4000000248
         MAC Address: 0021.ccbc.44f9
         IPv6 Address: Unknown
         IPv4 Address: 75.1.1.11
           User-Name: 0021.ccbc.44f9
               Status: Authorized
               Domain: DATA
```

```
        Oper host mode: multi-auth
      Oper control dir: both
      Session timeout: N/A
    Common Session ID: 090C895F000012A70412D338
      Acct Session ID: Unknown
                Handle: 0x4000023A
        Current Policy: (No Policy)

Method status list:
       Method           State
       webauth         Authc Success
```

For additional details on this feature, see the following document:

https://techzone.cisco.com/t5/Converged-Access-NGWC/Wired-Guest-Access-with-Both-Anchor-and-Foreign-as-5760-WLC/ta-p/778400

What's New in Cisco IOS XE Release 3.7.2E

New parameter **call-station-id** added to the **wireless security dot1x radius mac-authentication** command. The **call-station-id** parameter configures Call Station ID type for MAC authentication.

There are no other features or enhancements in this release. For more information about updates in this release, see the "Caveats" section on page 28.

What's New in Cisco IOS XE Release 3.7.1E

There are no other features or enhancements in this release. For more information about updates in this release, see the "Caveats" section on page 28.

What's New in Cisco IOS XE Release 3.7.0E

- Wireless capability is added to Catalyst 4500E Series Switch Supervisor Engine 8-E.
- Support is added for the following access points:
  - Cisco Aironet 1700 Series Access Point
  - Cisco Aironet 1570 Series Access Point (supported only in Local mode)
- VLAN tagging is supported on Cisco Aironet 700W Series Access Points
- mDNS Service Discovery Gateway—The Service Discovery Gateway feature enables multicast Domain Name System (mDNS) to operate across Layer 3 (L3) boundaries. In this phase, features such as de-congestion of incoming mDNS traffic, redistribution of service withdrawal messages, a filter criterion for learning services available on a specific interface, and the periodic browsing of services on specific interfaces are introduced.
- AVC top 'N' users per application—This feature enables you to know network usage information on a per user basis within an application. This feature is enabled by default and is available if AVC is enabled.
- AN Infra—Autonomic networking makes network devices intelligent by introducing self-management concepts that simplify network management for the network operator.

- WebAuth sleeping client—Allows successfully authenticated devices to stay logged in for a configured period without reauthentication.

  The following CLI is added under the webauth parameter map:

  sleeping-client timeout *timeout-in-minutes*

  Restrictions:

  - There is one-to-one mapping between device MAC and username/password. Once an entry is added to sleeping-client cache, the device/user gets policies for the user stored in the cache. Therefore, any other user using the device also gets the same policies as the user stored in the sleeping-client cache. The user can force normal authentication by logging out. To do that, the user must explicitly enter the following URL:

    ```
    http[s]://<Virtual IP/Virtual Host>/logout.html
    ```

  - Mobility is not supported. If the client roams from one controller to another, the client undergoes normal authentication on the foreign controller.
- Regulatory domains for India (–D), Indonesia (–F), Brazil (–Z), Honk Kong (–S) are supported.
- New Flexible NetFlow Collect parameters:
  - **collect wireless afd drop bytes**—Collects the fields for wireless approximate fair drop (AFD) drop bytes
  - **collect wireless afd accept bytes**—Collects the fields for AFD accept bytes
- New CLI is added to view AFD statistics information:

  Controller# **show platform qos wireless stats ssid** {*ssid-value* | **all**} **client all**

  This CLI lists client MAC address, WLAN ID, BSSID, accept byte, and drop byte details.
- New CLI is added to check whether an access point model is supported or not:

  Controller# **show ap is-supported** *ap-model-part-number*
- Wireless AutoQoS is supported.
- CWDM SFP+ 10-Gigabit optics are supported.

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 3650-24TD-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 3650-48FQ-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

Table 4 Catalyst 3650 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
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 3650-24TD-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
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

Table 4 Catalyst 3650 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
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 3650-24TD-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
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 3650-48FQ-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

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.

Note On platforms that run Cisco IOS XE releases, the WSSI/3G modules on access points are not supported.

Table 6 Cisco 5700 Series WLC Supported Products

Product	Platform Supported
Access Point	Cisco Aironet 700, 700W, 1040, 1140, 1260, 1530, 1570, 1600, 1700, 2600, 2700, 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 700 Series	AIR-CAP702W-x-K9
	AIR-CAP702I-x-K9
	AIR-CAP702I-xK910
Cisco Aironet 700W Series	AIR-CAP702Wx-K9
	AIR-CAP702W-xK910

Table 7 Supported Access Points (continued)

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 1530 Series	AIR-CAP1532I-x-K9
	AIR-CAP1532E-x-K9
Cisco Aironet 1570 Series	AIR-AP1572EAC-A-K9
	AIR-AP1572ECx-A-K9
	AIR-AP1572ICx-A-K9
Cisco Aironet 1600 Series	AIR-CAP1602E
	AIR-CAP1602I
Cisco Aironet 1700 Series	AIR-CAP1702I-x-K9
	AIR-CAP1702I-xK910
Cisco Aironet 1850 Series	AIR-AP1852I-UXK9
	AIR-AP1852I-UXK910
	AIR-AP1852I-x-K9
	AIR-AP1852E-UXK9
	AIR-AP1852E-UXK910
	AIR-AP1852E-x-K9
Cisco Aironet 2600 Series	AIR-CAP2602E
	AIR-CAP2602I
Cisco Aironet 2700 Series	AIR-CAP2702I-x-K9
	AIR-CAP2702E-x-K9

Table 7 Supported Access Points (continued)

Access Points	
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

Compatibility Matrix

Table 8 lists the software compatibility matrix.

Table 8 Software Compatibility Matrix

Cisco 5700 WLC	Catalyst 3850	Catalyst 3650	Cisco 5508 WLC or WiSM2	MSE	ISE	ACS	Cisco PI
03.07.01E 03.07.00E	03.07.01E 03.07.00E	03.07.01E 03.07.00E	8.0 7.6	8.0[1]	1.3	5.2 5.3	2.2
03.06.02E 03.06.01E 03.06.00E	03.06.02aE 03.06.01E 03.06.00E	03.06.02aE 03.06.01E 03.06.00E	8.0 7.6	8.0[2]	1.2	5.2 5.3	2.1.2 or 2.1.1 if MSE is also deployed[3] 2.1.0 if MSE is not deployed
03.03.03SE 03.03.02SE 03.03.01SE 03.03.00SE	03.03.03SE 03.03.02SE 03.03.01SE 03.03.00SE	03.03.03SE 03.03.02SE 03.03.01SE 03.03.00SE	7.6[4] 7.5[5]	7.5	1.2	5.2 5.3	2.0

1. Because of SHA-2 certificate implementation, MSE 7.6 is not compatible with Cisco IOS XE Release 3.6E and later. Therefore, we recommend that you upgrade to MSE 8.0.
2. Because of SHA-2 certificate implementation, MSE 7.6 is not compatible with Cisco IOS XE Release 3.6E and later. Therefore, we recommend that you upgrade to MSE 8.0.
3. If MSE is deployed on your network, we recommend that you upgrade to Cisco Prime Infrastructure 2.1.2.
4. Cisco WLC Release 7.6 is not compatible with Cisco Prime Infrastructure 2.0.

5. 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.

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

Wireless Web UI Software Requirements

- Operating Systems
  - Windows 7
  - Windows 8
  - Mac OS X 10.8
- Browsers
  - Google Chrome—Version 35
  - Microsoft Internet Explorer—Versions 10 or 11
  - Mozilla Firefox—Version 30
  - Safari—Version 6.1

Software Version

Table 9 shows the mapping of the Cisco IOS XE version number and the Cisco IOS version number.

Table 9 Cisco IOS XE to Cisco IOS Version Number Mapping

Cisco IOS XE Version	Cisco IOSd Version	Cisco Wireless Control Module Version	Access Point Version
03.07.03E	15.2(3)E3	10.3.130.0	15.3(3)JNB3
03.07.02E	15.2(3)E2	10.3.100.0	15.3(3)JNB2
03.07.01E	15.2(3)E1	10.3.100.0	15.3(3)JNB1
03.07.00E	15.2(3)E	10.3.100.0	15.3(3)JNB
03.06.01E	15.2(2)E1	10.2.111.0	15.3(3)JN3
03.06.00E	15.2(2)E	10.2.102.0	15.3(3)JN
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

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 instal**l 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]:
```

Table 10 Software Images

Image	File Name
Cisco 5760 WIRELESS CONTROLLER SW Release 3.7	ct5760-ipservicesk9.SPA.03.07.01.E.152-3.E1.bin
Cisco 5760 WIRELESS CONTROLLER SW Release 3.7 without DTLS	ct5760-ipservicesk9ldpe.SPA.03.07.01.E.152-3.E1.bin

Important Upgrade Note

After you upgrade to Cisco IOS XE Release 3.7E, the WebAuth success page behavior is different from the behavior seen in Cisco IOS XE Release 3.3.X SE. After a successful authentication on the WebAuth login page, the original requested URL opens in a pop-up window and not on the parent page. Therefore, we recommend that you upgrade the Web Authentication bundle so that the bundle is in the format that is used by the AireOS Wireless LAN Controllers.

To download a sample Web Authentication bundle, follow these steps:

Step 1 Browse to http://software.cisco.com/download/navigator.html.

Step 2 Navigate to **Products > Wireless > Wireless LAN Controller > Standalone Controller > Cisco 5700 Series Wireless LAN Controllers > Cisco 5760 Wireless LAN Controller.**

Step 3 Click **Wireless Lan Controller Web Authentication Bundle**.

Step 4 Choose Release 3.7.0 and click **Download**.

Step 5 After the download, follow the instructions provided in the Read Me file that is attached in the bundle.

Note In a High Availability scenario, if you download the Web Authentication bundle to the active controller, the bundle cannot be synchronized with the standby controller. Therefore, we recommend that you also manually download the Web Authentication bundle to the standby controller.

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/c/en/us/products/wireless/5700-series-wireless-lan-controllers/datasheet-listing.html

Interoperability with Other Client Devices

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

Table 11 lists the client types on which the tests were conducted. The clients included laptops, handheld devices, phones, and printers.

Table 11 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	v15.10.5.1
Intel 6235	V15.10.5.1
Intel 6300	v15.10.4.2
Intel 7260(11AC)	17.0.0.34, Windows 8.1
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
Broadcom 4360(11AC)	6.30.163.2005
Macbook Air (11AC)	10.9.3
Macbook Air	10.9.3
Handheld Devices	
Apple iPad	iOS 5.0.1
Apple iPad2	iOS 6.0.1
Apple iPad3	8.0.2(12A405)
Apple iPad Air	8.0.2(12A405)
Apple iPad Mini	8.0.2(12A405)
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

Table 11 Client Types (continued)

Client Type and Name	Version
Vocera B1000A	4.1.0.2817
Vocera B2000	4.0.0.345
Apple iPhone 4	iOS 6.0.1
Apple iPhone 4S	8.0.2(12A405)
Apple iPhone 5s	8.0.2(12A405)
Apple iPhone 5c	8.0.2(12A405)
Apple iPhone 6	8.0.2(12A405)
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
Samsung Galaxy S4 (GT-I9500)	4.4.2
Samsung Galaxy Note (SM-900)	4.4.2

Important Notes

- With Cisco Prime Infrastructure 2.1.1, the refresh config and inventory collection tasks from the controller might take anywhere from 20 minutes to 40 minutes. For more information, see CSCum62747 on the Bug Search Tool.
- Although visible in the CLI, the following commands are not supported:
  - **collect flow username**
  - **authorize-lsc-ap** (CSCui93659)
- The following features are not supported in Cisco IOS XE Release 3.7E:
  - Mesh, FlexConnect, and OfficeExtend access point deployment

Limitations and Restrictions

- Flex Links are not supported. We recommend that you use spanning tree protocol (STP) as the alternative.
- Outdoor access points are supported only when they are in Local mode.
- 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.
  - Cisco TrustSec VLAN-to-SGT binding cannot be enabled in pure bridging domain. You have to either manually enable IP device tracking on the ports in the VLAN, or enable SVI interface for the VLAN.
  - For Cisco IOS Release 3.7E and later, Cisco TrustSec VLAN-to-SGT binding cannot be enabled in pure bridging domain. You have to either manually enable IP device tracking on the ports in the VLAN, or enable SVI interface for the VLAN.
- When configuring QoS queuing policy, the sum of the queuing buffer should not exceed 100%.
- For QoS policies, only Switched Virtual Interfaces (SVI) are supported for logical interfaces.
- QoS policies are not supported for port-channel interfaces, tunnel interfaces, and other logical interfaces.

Caveats

Cisco Bug Search Tool

Caveats describe unexpected behavior in a product. The Open Caveats section lists open caveats that apply to the current release and may apply to previous releases. A caveat that is open for a prior release and is still unresolved applies to all future releases until it is resolved.

To view the details of the software bugs pertaining to your product, perform the following task:

Click the Caveat ID/Bug ID number in the table.

The corresponding Bug Search Tool page is displayed with details of the Caveat ID/Bug ID.

The Bug Search Tool (BST), which is the online successor to the 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 whose ID you do not have, perform the following procedure:

1. http://www.cisco.com/c/dam/en/us/td/i/templates/blank.gif Access the BST using your Cisco user ID and password at: https://tools.cisco.com/bugsearch/.

2. In the Bug Search window that is displayed, enter the necessary information in the corresponding fields.

For more information about how to use the Cisco Bug Search Tool effectively, including how to set email alerts for bugs and to save bugs and searches, see the Bug Search Tool Help & FAQ page.

Open Caveats

There are no open caveats in this release.

Resolved Caveats in Cisco IOS XE Release 3.7.5E

Use the BST to view the details of a caveat listed in this section. For more information about the Cisco BST, see the "Cisco Bug Search Tool" section on page 28

Caveat ID Number	Description
CSCud22987	Standby WCM: %OSAPI-4-TIME_SHIFT_DETECTED: Detected backward time shift
CSCus83638	5-GHz radio on Cisco AP beaconing but not accepting client associations
CSCut64800	NMSP status is always shown as enabled for Converged Access controllers
CSCuy32363	Converged Access: MDNS leaking when roaming to foreign in L2 sticky-anchor
CSCuy73225	CLI "show wireless client client-statistics summary" does not display some client statistics (RSSI, SNR, etc.)
CSCuy87158	AutoQoS enterprise does not install again after the classes are removed from the port policy
CSCva16996	Cisco 5760 WLC is sending null values for ipaddresstable in cldcClientByIpTable
CSCva65432	A-MSDU settings are not saved after reload
CSCvb54115	Ad-hoc rogues marked as external are removed after timeout
CSCvb90663	Cisco 5760 WLC: Rogue AP and rogue clients show values in different timezone than the one on Cisco WLC
CSCvc81187	Converged Access: show trace showing "% could not execute command due to incorrect data"

Resolved Caveats in Cisco IOS XE Release 3.7.4E

Use the BST to view the details of a caveat listed in this section. For more information about the Cisco BST, see the "Cisco Bug Search Tool" section on page 28

Bug ID	Headline
CSCuv50017	Airties WGB not getting IP address when connecting to Cisco 5760 WLC
CSCuw02750	Cisco 5760 WLC High Memory Utilization on dhcp_sensor
CSCuw24217	Login using TACACS+ and RADIUS using custom method list
CSCuw28104	Not able to configure local MAC address as username
CSCuw78795	REPLAY_ERR msg showing WLAN ID as VLAN ID of the AP
CSCuw97388	SNMP should allow 128 characters for ap groups description
CSCux65356	AP join failure due to ap_index out of sync between IOS and FED
CSCux79913	The client column in the load-info command is not making much sense
CSCuy29078	Cisco 5760 WLC FED reloads unexpectedly
CSCuy37932	Cisco 5760 WLC does not forward 224.0.0.1 link local packets to wireless clients
CSCuz01017	GUI does not show information about interference devices
CSCuz35087	Lobby ambassador username gives full GUI access

Resolved Caveats in Cisco IOS XE Release 3.7.3E

Use the BST to view the details of a caveat listed in this section. For more information about the Cisco BST, see the "Cisco Bug Search Tool" section on page 28.

Bug ID	Headline
CSCur48634	HA fails due to bulk synchronization failure with encrypted password
CSCus84849	IPDT difference in configuration and default configuration
CSCut21359	HA WLC not showing AP count right after second SSO until hours later
CSCut46955	APs unable to reassociate when simulator stopped and restarted
CSCut88813	WLAN cannot be configured with a space in PSK shared key
CSCut88813	WLAN cannot be configured with a space in psk shared key on NGWC 3.7
CSCuu15831	Switch reboots when SPAN configured under "cts manual"
CSCuu56466	"Total output drops" counter of a certain ports does not increment
CSCuu56511	OutDiscards counter does not increment
CSCuu82607	Evaluation of all for OpenSSL June 2015
CSCuu85807	Switch returns wrong OID when standalone
CSCuu86077	Sanity-Uplink ports going down

Bug ID	Headline
CSCuu87659	CpmCPUTotal5minRev average value of stack switch 2 on Catalyst 3850 is incorrect
CSCuu97048	Traffic is dropped due to static mac entry on foreign interface
CSCuu97550	FB 4500X - SNMP dot1dTpFdbPort retuning incorrect value
CSCuv02964	Memory leak in with dot1x on IOS-XE switch
CSCuv07427	TCP connection cannot be established with Openflow agent
CSCuv13351	MAC address is learned on RSPAN VLAN after stack switchover
CSCuv19773	“nmsp attach suppress” not being added into run-config on WS-C3850-24P
CSCuv20921	MAC address-table learning command should not be allowed for RSPAN VLAN
CSCuv22736	After reload, C3850-NM-4-10G/GLC-SX-MM not linkup with speed nonegotiate
CSCuv62574	GRE tunnel in up/down state when tunnel source configured via interface
CSCuv78424	Unicast ARP packets are duplicated
CSCuw19798	GRE Tunnel not working on Catalyst 3850
CSCuw22050	Switch reports power device detected when non device is connected
CSCuw36865	L2 switched traffic matched by L3 SVI VACL in the output direction
CSCuw39020	Access-session vlan-assignment ignore-errors breaks dynamic vlan assign
CSCuw73525	DHCPv6 Guard does not block rogue DHCP server to provide IPv6 address
CSCuw98232	Fixing the build breakage which happened with CSCuv62574
CSCup77718	Need to have ap_mac and client_mac attributes in LWA URL
CSCup93935	RRM must not push DFS channel change to all of RF group
CSCuq60981	Mab is not taking priority over dot1x in concurrent authentication
CSCur57112	Controller redirecting the wrong URL
CSCur84447	Memory Leak at “CMI IOSd” process
CSCur87501	Post-ACL is not applied after CWA CoA in New Mobility with Catalyst 3850 as foreign
CSCus13331	EPM redirect crash
CSCus58734	“AUTHMGR-4-UNAUTH_MOVE” messages thrown on console when client roam
CSCus77477	Cisco NGWC increases the number of URLs allowed in a DNS ACL in WLC
CSCut42591	MAC flapping and crash on unauthorized ports with authentication control-direction in
CSCut55195	Mobility tunnel not coming up with Layer 3 interface

Bug ID	Headline
CSCut88813	WLAN cannot be configured with a space in psk shared key on NGWC 3.7
CSCut89766	Observe FED crashed caused member removal from stacks
CSCuu04476	VTY/Console lockup on random socket or TCP based CLI
CSCuu08764	NVGEN IP DHCP snooping commands by default for Cisco 5760 WLC
CSCuu28768	C2960 ARP Table adding MACs on Incorrect Interface
CSCuu32303	AP radio interfaces admin down state after WLC reboot
CSCuu40853	FFM crash observed with guest access scale scenario
CSCuu43279	IOSd crash while performing SSO and issuing show DTLS related commands
CSCuu45274	The debug client mac-address command output shows association from other mac addresses
CSCuu45282	The debug ap mac-address wcm command output should show the whole ap join flow
CSCuu50539	Cisco 5760 WLC should not crash if LAP HA WLC IP address pointer is NULL
CSCuu50589	Voice Clients Blacklisted due to %SPI-3-QOS_INSTALL_CLIENT_POLICY
CSCuu58492	The show tech wireless command stops at wireless linktest statistic
CSCuu59697	AP does not forward EAPoL-Key M1 to client when AVC is enabled
CSCuu62624	The show tech wireless command should contain additional outputs
CSCuu65749	_be_spi_dtls_ios_rsc_info_create_internal causing memory leak
CSCuu65757	__be_PKI_name_list_add causing memory leak
CSCuu69033	Memory leak observed at spi_qos_tam_pm_update_stats_handler
CSCuu69111	EAP framework memory leak observed on Cisco 5760 WLC
CSCuu71587	WPA-AES configuration is getting disabled on the CLI after WLC/switch reboot
CSCuu72324	FED memory leak @ fed/feature/qos/src/fed_qpm_ffm_api.c:1431
CSCuu75209	WCM processing of rx packets after port initialization (ports 5246/5247)
CSCuu79865	IOSd not accepting QoS install request sent by WCM
CSCuu85713	Input queue full forced to restart the WLC to restore
CSCuu91567	Data rate shown on NGWC for 11ac is not clear
CSCuu92609	Cisco 5760 WLC is not sending discovery response to APs
CSCuu99792	WLAN configuration is not applied due to “exceeds MAX_QUEUED_RECV_BUFS”
CSCuv06190	WCM crash in TCP library
CSCuv06451	IOSd crash in eap_auth_terminal_state calling free_internal
CSCuv09994	SNMP memory leak at snmp_spi_util

Bug ID	Headline
CSCuv22549	In WAN, DTLS cert packets come out of order could lead to AP join failure
CSCuv23751	'JP' should be used as world mode in Beacon/Probe Res
CSCuv23905	Client stuck in APPLYINGPOLICY/Authentication state
CSCuv34504	Bypass the traffic based on the ACL during authentication.
CSCuv36461	Memory leak at SPI iif reg(PC: 0xF64E0E91)
CSCuv45515	Cisco 5760 WLC crash in fed al_fnf_get_iif_fnf_info
CSCuv50834	High CPU due to hung NMSP Session
CSCuv69997	Cisco 5760 WLC crashes due to APF-3-VALIDATE_DOT11i_CIPHERS_FAILED Errors
CSCuw52729	Enabling auto QoS causes “line vty 0 4” length set to 0
CSCuw55669	Crash is seen in IOSd on switch and auth-mgr
CSCuw61261	Controller crashes on ios_authproxy.
CSCus99269	dACL should not be synced to MA and should be allowed on MA as well
CSCut87285	MAC address being learnt on an individual Port-channel member interface
CSCuu34717	Catalyst 3850 cts enforcement for multicast traffic
CSCuv14890	DHCPv6 solicit frame (IPv6 multicast) frame replication issues
CSCuw28638	Catalyst 3650 rebooting during EAP-TLS authentication
CSCuw38233	Mobility tunnel between MA/MC drops when default egress policy is deny
CSCuw82216	Upgrade in install mode corrupts the flash - EXT2-fs error

Resolved Caveats in Cisco IOS XE Release 3.7.2E

Use the BST to view the details of a caveat listed in this section. For more information about the Cisco BST, see the “Cisco Bug Search Tool” section on page 28.

Bug ID	Headline
CSCup13927	Client deletion takes 10 seconds when fast SSID is enabled
CSCut56289	FED stops working in fed_dtls_lookup_si task
CSCur78320	Cisco 5760 WLC—Bulk Sync Failure when AP CDP is disabled globally
CSCus89066	Unable to change WLAN security with wpa1(AES and TKIP) through web interface.
CSCut76129	The problem in loading in page CT5760
CSCut93158	Web interface is not displaying all character when SSID is configured with 32 characters.
CSCuu71450	Client traffic fails after MA to MC roaming.

Resolved Caveats in Cisco IOS XE Release 3.7.1E

Use the BST to view the details of a caveat listed in this section. For more information about the Cisco BST, see the "Cisco Bug Search Tool" section on page 28.

Bug ID	Headline
CSCur44010	HA IOSd crash in crypto_lib_keypair_delete
CSCur41848	Subnet broadcast and Multicast is not working
CSCup92808	No CWA redirect for client in case it roamed in webauth-reqd state
CSCur24788	CWA flow break if accounting enabled in GA scenario
CSCur79033	In the client details, VLAN group name is not shown
CSCur33695	Packet drop observed AMSDU enabled and AMPDU disabled.
CSCur61190	FED crash observed after SSO in 5760
CSCut01521	Crash with web authentication / sleeping client
CSCus91957	RogueAP trap from 5760 has invalid rogueAP/detectingAP macs

Resolved Caveats in Cisco IOS XE Release 3.7.0E

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 28.

Bug ID	Headline
CSCue32004	When you change an AP name, make the AP name change in AP join stats
CSCuh14797	Client not authenticating due to wrong mobility peer detail in Anchor
CSCuh53553	mbuf leak on Action frames type 10 subtype 23
CSCul44417	Support Local MAC filter entries on a per WLAN basis
CSCul96802	Max User Session not working
CSCum66082	IRCM: Client able to pass traffic in CWA_RE
CSCum94954	MAC filtering is not working in debugs
CSCun53957	NGWC display AP NSI Key on GUI
CSCuo47903	No CWA redirect for client in case it roamed in webauth-reqd state
CSCuo58932	WGB wired clients unable to pass traffic with mobility configured
CSCuo63950	WCM crash on customer production network txpower auto CLI
CSCuo71505	WGB Wired client does not go into RUN state in export anchor scenario
CSCuo78990	WCM Crash @ eip_wcm_RRM_LRAD_DATA_t_neighbor
CSCuo79216	IOSD leak @ be_ifm_send_radio_event
CSCuo79272	IOSD leak @ be_dtls_malloc
CSCuo87797	Voice Call upstream traffic marked down to zero dscp

Bug ID	Headline
CSCuo88604	1k AP join takes 1 hour
CSCuo93558	APs on NGWC do not register
CSCuo98816	Delete Payload not sent to previous AP when roaming to new AP
CSCup05243	NGWC GUI disable option to select multiple parameters
CSCup08994	Change the AVC cumulative usage counters to uint64 in display/output
CSCup17578	Cyprus AP support
CSCup43034	WCM crash at __be_qos_tam_db_fe_install_pm_on_target
CSCup59493	NGWC: W56 Static TxPower level changes to Max after AP reboot
CSCup60078	Wireless TSPEC phone not able to place call after SSO failover
CSCup72845	MAC filtering & AAA override with NGWC does not update interface name
CSCup73590	WCM crash in Mobility code: maHandleLocalClientDelete / mmMaUdsSend
CSCup74747	NGWC 3850 & 5760 - NAS-Port-Type Missing In Accounting Request
CSCup98782	Fed crash observed at webauth pending process after extended test
CSCuq00349	5760 Amber LED on first port of port channel of Flexlink Backup Port
CSCuq20970	Default multicast / broadcast forwarding mode cause latency
CSCuq25195	Adjust AFD for every client and BSSID add/del.
CSCuq32016	AMUR-MR1: Incorrect AFD client ssid association
CSCuq38516	IOSd crash at emweb_http_process
CSCuq45867	Syslog messages contain too little information
CSCuq48106	DHCP req sent while switching ssids mapped to different vlan groups fail
CSCuq58700	“Wlan PSK profile applied to NGWC with invalid argument “”clear”””
CSCuq72715	Fiber link between Cat4k and WLC5760 down after WLC5760 reload
CSCuq79546	IOSd reboots on 5760 running 3.3.4 at be_epm_redirect_cache_entry_get
CSCuq83758	Subnet broadcast forwarding is not working in katana.
CSCuq95020	AP heartbeat packets going to best effort queue
CSCur17400	Downstream Packet drop in AP when traffic has non-zero DSCP value
CSCur35879	“parameter-map cannot be deleted after “”wlan”” int is shut”
CSCur40052	IOS-XE Plaintext admin credentials saved to file
CSCur50946	APs mfg in Aug./Sept./Oct. 2014 unable to join an IOS-XE controller

Bug ID	Headline
CSCur56367	AIR-CT5760-HA-K9 loses its license after reboot
CSCur59580	5760-HA crash on 3.3.3
CSCup12631	WebGUI displays WSMA errors on some pages after TACACS authentication
CSCuq40329	snmp_subagent crash on 3.13.71EZP
CSCuq59720	AIR-CT5760 Anchor running 03.06.00SE flapping with IOSd crash
CSCuo52196	Encryption configuration lost after stack switchover
CSCup39353	IOSd reboots at @ ios_syncmgr_lock_pop_errmsg
CSCup16325	IOSd stack crash
CSCuo07995	IOSD leak @ be_ip2access_add_acl_item2
CSCuh09324	UDP entries not deleted from flowmgr table
CSCuq59661	QoS policy on SSID not installed when policy removed and reapplied
CSCuo07525	Crash in TAM when policy applied on client and then on SSID
CSCul96802	Max User Session not working with NGWC

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 IOS XE 3E Release documentation at this URL:

  http://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-3e/tsd-products-support-series-home.html
- 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.
