Release Notes for Cisco IOS XE 3.6 Software for Cisco 5700 WLC

This Release Note document provides an overview of the features in the Cisco IOS XE 3.6 software on the Cisco 5700 Series Wireless LAN Controller (WLC).

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 Cisco WLC delivers wire-speed performance with services such as Advanced QoS, Flexible NetFlow Version 9, and downloadable access control lists (ACLs) enabled in a wireless network. The controller works with other controllers and access points (APs) to provide network managers with a robust wireless LAN solution. The Cisco 5700 WLC 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 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
May 17, 2019	• Added: What's New in Cisco IOS XE Release 3.6.10E • Caveats, page 36 – Added: Open Caveats for Cisco IOS XE Release 3.6.10E, page 37 – Added: Resolved Caveats for Cisco IOS XE Release 3.6.10E, page 38
Sept 12, 2018	• Added: What's New in Cisco IOS XE Release 3.6.9E • Caveats, page 36 – Added: Open Caveats for Cisco IOS XE Release 3.6.9E – Added: Resolved Caveats for Cisco IOS XE Release 3.6.9E
July 25, 2018	• Added: What's New in Cisco IOS XE Release 3.6.8E • Caveats, page 36 – Added: Open Caveats for Cisco IOS XE Release 3.6.8E – Added: Resolved Caveats for Cisco IOS XE Release 3.6.8E
July 13, 2017	• Caveats, page 36 – Added: Open Caveats – Added: Resolved Caveats for Cisco IOS XE Release 3.6.7E • Limitations and Restrictions, page 35 – Updated limitation list
April 27, 2017	• Resolved Caveats for Cisco IOS XE Release 3.6.6E, page 39 – Added: CSCus83638

What's New in Cisco IOS XE Release 3.6.10E

There are no new features in this release. See Caveats section.

What's New in Cisco IOS XE Release 3.6.9E

There are no new features in this release. See Caveats section.

What's New in Cisco IOS XE Release 3.6.8E

There are no new features in this release. See Caveats section.

What's New in Cisco IOS XE Release 3.6.7E

There are no new features in this release. See Caveats section.

What's New in Cisco IOS XE Release 3.6.6E

There are no new features in this release. See Caveats section.

What's New in Cisco IOS XE Release 3.6.5aE

There are no new features in this release. See Caveats section.

What's New in Cisco IOS XE Release 3.6.5E

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

- AP700i/w
- 1040
- 1140
- 1260
- 1530
- AP1570 (V02)
- AP1600i/e
- AP1700i
- AP2600i/e

- AP2700i/e
- AP3500i/e
- AP3600i/e
- AP3700p

For other updates in this release, see Caveats, page 36.

What's New in Cisco IOS XE Release 3.6.4E

- The TACACS+ login procedure using custom method list is simplified wherein configuring a default method list is no longer required when the same server group is used.

No new features or other enhancements are included in this release.

What's New in Cisco IOS XE Release 3.6.3E

- 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 6.
- 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>
```

- Credentials support in HTTP GET 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.

- Appending AP radio MAC or Service Set Identifier (SSID) or client MAC—External URLs sent to a client can be appended with an AP radio MAC address, or SSID, or client MAC address, or any of these combinations, so that a web authentication redirect URL sent to the wireless client is parsed by an external server based on the appended attribute configured in the parameter map. For example, an external server can use this attribute information present in the redirect URL to send the login page based on the AP location, or SSID, or the client MAC address. The following are the commands to configure this feature:

```
parameter-map type webauth external
type webauth
```

```
redirect for-login http://<login_URL>/login.html
redirect on-failure http://<URL>/failure.html
redirect on-success http://<URL>/success.html
redirect portal ipv4 <external-webserver-ip-address>
redirect append ap-mac tag apmac
redirect append wlan-ssid tag ssid
redirect append client-mac tag mac
```

- Multiprivilege level support to log in to web UI through TACACS+—In releases prior to Cisco IOS XE Release 3.6.3, users were restricted to privilege level 15. In this release, users with privilege level 1can log in, access, and monitor Cisco WLC through TACACS+ or local authentication. Users with privilege level 0 are denied access. However, we recommend that you do not configure TACACS privilege levels for some commands on Cisco WLC, as it returns privilege level 15 for all users, which can interfere with WEB user interface configuration.
- Cisco Aironet 1570 Series Access Point—This release supports the Cisco Aironet 1570 Series Access Point, in local mode.
- WebAuth sleeping client—This allows successfully authenticated devices to stay logged in for a configured period without reauthentication.

  The **sleeping-client timeout** *timeout-in-minutes* command is added under the webauth parameter map.

  Restrictions:

  – There is one-to-one mapping between the device MAC and username and password. After an entry is added to the sleeping-client cache, the device or the 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.
- LWA—Multiple WebServer Configuration for External WebAuth.

  You have to configure extended ACL on the box and add the deny rule to allow the external server ip address. An example is given below:

  ```
  Switch(config)# ip access-list extended BYPASS_ACL
  Switch(config-ext-nacl)# deny ip any host 10.1.1.1
  Switch(config-ext-nacl)# deny ip any host 20.1.1.1
  Switch(config-ext-nacl)# end

  Switch# show ip access-lists | sec BYPASS_ACL
  Extended IP access list BYPASS_ACL
      10 deny ip any host 10.1.1.1
      20 deny ip any host 20.1.1.1
  ```

  This release introduces a new CLI in global parameter-map to configure the BYPASS_ACL. So, to configure the extended BYPASS_ACL under global parameter-map, use the following commands:

  ```
  Switch(config)# parameter-map type webauth global
  Switch(config-params-parameter-map)# webauth-bypass-intercept BYPASS_ACL
  ```

  After the configuration, content of the BYPASS-ACL would be merged with intercept-acl or redirect acl. So, the traffic destined for the ip addresses which are configured in BYPASS_ACL would be allowed enabling the user to access multiple external servers during the authentication.

- CWA—Default Built-in Redirect URL ACL

  Permit 443 is not advised and to avoid the users from making mistakes while defining CWA ACL, a built-in ACL is provided, which needs some modification for bypassing traffic to CWA server. (the Controller or Switch creates a default URL Redirect- ACL with mandatory ACEs [permit http traffic, deny dns and dhcp] excluding "permit tcp any any eq 443".) Using this ACL, the user needs to configure only "deny" rule for ISE Server/Any external Server to access it.

  Default ACL Name: CISCO-CWA-URL-REDIRECT-ACL

  ACL Content:

```
ip access-list extended CISCO-CWA-URL-REDIRECT-ACL
remark Configure deny ip any host <server-ip> to allow access to <server-ip>
100 deny udp any any eq domain
101 deny tcp any any eq domain
102 deny udp any eq bootps any
103 deny udp any any eq bootpc
104 deny udp any eq bootpc any
105 permit tcp any any eq www
```

  You can see the ACL using **show ip access-list** command. After modifying the ACL, its available from the **show running-config** command output.

  Usage:

  1. Modify the Default ACL "CISCO-CWA-URL-REDIRECT-ACL" to add "deny ip any host <server-ip>" above 100. If there is a requirement to allow multiple servers, use multiple "deny" rules.
  2. Configure the Default ACL Name in ISE as redirect-url for CWA authorization profile.

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.

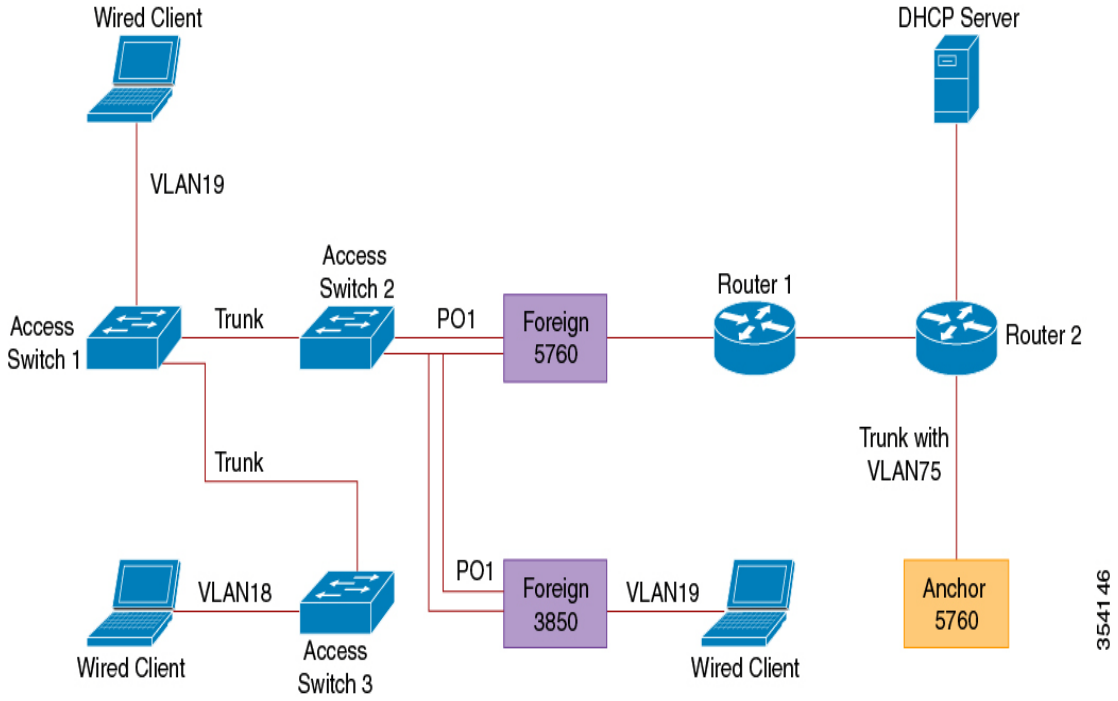
Before the guest access feature can be deployed, a mobility tunnel is established between the foreign anchor and guest anchor switches. The guest access feature works for both MC (Foreign Controller) to MC (Guest Anchor) and MA (Foreign Controller) to MC (Guest Anchor) models. The foreign anchor switch 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 3.6.2E

No features were added or enhanced for this release. For more information about updates in this release, see the "Caveats" section on page 36.

What's New in Cisco IOS XE Release 3.6.1E

- Support for Cisco Aironet 1700 Series Access Points
- VLAN tagging support for Cisco Aironet 700W Series Access Points
- MAC Authentication per WLAN
- Support for Cisco Prime Infrastructure 2.1.2

What's New in Cisco IOS XE Release 3.6.0E

What's New	Description
Use this URL to access the Cisco IOS XE Release 3E Documentation Roadmap: http://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-3e/tsd-products-support-series-home.html	Provides quick and easy access to all relevant documentation for specific platforms. Look for *Quick Links to Platform Documentation* on the respective platform documentation pages.
Integrated Documentation Guides	Provides platform and software documentation for these technologies: • *IP Multicast Routing Configuration Guide*
Open Plug-N-Play Agent	(LAN-Lite, LAN-Base, IP-Lite, IP-Base, IP Services and IP Enterprise Services) Switch-based agent support for zero-touch automated device installation solution called NG-PNP.
Cisco TrustSec Critical Authentication	(LAN-Base, IP-Lite, IP-Base, IP Services and IP Enterprise Services) Ensures that the Network Device Admission Control-authenticated 802.1X links between Cisco TrustSec devices are in open state even when the Authentication, Authorization, and Accounting (AAA) server is not reachable.
Enabling Bidirectional SXP Support	(LAN-Base, IP-Lite, IP-Base, IP Services and IP Enterprise Services) Enhances the functionality of Cisco TrustSec with Security Group Tag Exchange Protocol (SXP) V4 by adding support for SXP bindings that can be propagated in both directions between a speaker and a listener over a single connection.
Enablement of Security Group ACL at Interface Level	(LAN-Base, IP-Lite, IP-Base, IP Services and IP Enterprise Services) Controls and manages Cisco TrustSec access control on a network device based on an attribute-based access control list. When a security group access control list (SGACL) is enabled globally, the SGACL is enabled on all interfaces in the network by default. Use the Enablement of Security Group ACL at the Interface Level feature to disable the SGACL on a Layer 3 interface.
Role-Based CLI Inclusive Views	(LAN-Base, IP-Lite, IP-Base, IP Services and IP Enterprise Services) By default, enables a standard CLI view, including all commands.
Custom Web Authentication Result Display Enhancement	Displays the authentication results on the main HTML page, and not in a po-up window.

What's New	Description
Custom Web Authentication Download Bundle	Ensures that one or more custom HTML pages can be downloaded and configured from a single tar file bundle. The images and custom pages containing the images are also a part of the same downloadable tar file bundle.
Virtual IP Support for Images in Custom Web Authentication	Supports image file names without prefixes and removes the requirement of users having to specify the wireless management interface IP to indicate the source of image in the HTML code.
Service Discovery Gateway: mDNS Enhancements	Enables multicast Domain Name System (mDNS) to operate across Layer 3 boundaries.
HTTP Gleaning	(IP-Base, IP Services and IP Enterprise Services.) Allows the device sensor to extract the HTTP packet Type-Length-Value (TLV) to derive useful information about the end-device type.
Banner Page and Inactivity timeout for HTTP/S Connections	Allows you to create a banner page and set an inactivity timeout for HTTP or HTTP Secure (HTTPS) connections. The banner page allows you to log in to the server when the session is invalid or expired.
Secure CDP	(LAN-Lite, LAN-Base, IP-Lite, IP-Base, IP Services and IP Enterprise Services) Allows you to select the type, length, value (TLV) fields that are sent on a particular interface to filter information sent through Cisco Discovery Protocol packets.
Web Authentication Redirection to Original URL	(LAN-Base, IP-Lite, IP-Base, IP Services and IP Enterprise Services) Enables networks to redirect guest users to the URL they had originally requested. This feature is enabled by default and requires no configuration.
Auto Configuration	(LAN-Lite, LAN-Base, IP-Lite, IP-Base, IP Services/ IP Enterprise Services) Determines the level of network access provided to an endpoint based on the type of the endpoint device. This feature also permits hardbinding between the end device and the interface. Autoconfig falls under the umbrella of Smart Operations solution.
Interface Templates	(LAN-Lite, LAN-Base, IP-Lite, IP-Base, IP Services and IP Enterprise Services) Provides a mechanism to configure multiple commands at the same time and associate them with a target, such as an interface. An interface template is a container of configurations or policies that can be applied to specific ports.
NMSP	Enables strong ciphers (SHA2) for NMSP connections.

What's New	Description
Embedded Event Manager (EEM) 4.0	Provides unique customization capabilities and event-driven automation within Cisco products.
CleanAir Express for 1600 APs	Supports CleanAir Express on the Cisco 1600 Series Access Points. For more information about CleanAir Express, see http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/cleanair-technology/aag_c22-594304.pdf
New AP Platform Support	Support the following APs in this release: • AP2700I, AP2700E • AP1532I, AP1532E **Note** The Cisco Aironet 1530 Series APs are supported only in local mode; the APs in mesh mode are not supported. • AP702W, AP702I
FQDN ACLs	Access control lists (ACLs), when configured using a fully qualified domain name (FQDN), enables ACLs to be applied based on the destination domain name. The destination domain name is then resolved to an IP address, which is provided to the client as part of DNS response. Guest users can log in using web authentication with parameter map that consists of FQDN ACL name. You can apply an access list to a specific domain. The RADIUS server then sends the AAA attribute fqdn-acl-name to the controller. The operating system checks for the pass-through domain list and its mapping, and permits the FQDN. The FQDN ACL allows clients to access only configured domains without authentication. The FQDN ACL is supported only for IPv4 wireless sessions.
Local Policies	Local policies can profile devices based on HTTP and DHCP to identify the end devices on the network. Users can configure device-based policies and enforce the policies per user or per device policy on the network. Local policies allow profiling of mobile devices and basic onboarding of the profiled devices to a specific VLAN. They also assign ACL and QoS or configure session timeouts.

What's New	Description
Auto MAC Learning of Valid Client via Cisco MSE	You can validate rogue clients by utilizing the resources available in the Cisco Mobility Services Engine (MSE). Using Cisco MSE, you can dynamically list the clients joining to the controller. The list of clients joined to the controller is stored in the Cisco MSE as a centralized location, where the controller communicates with Cisco MSE and validates the client before reporting if a rogue client is a valid one or not. Cisco MSE maintains the MAC addresses of clients joined to the controller. The communication between the controller and Cisco MSE is an on-demand service as the controller requests this service from Cisco MSE.
QoS Upstream	Marking and policing actions for ingress SSID and client policies are applied at an access point. The SSID and client ingress policies that you configure in the controller are pushed to the AP. The AP performs policing and marking actions for each packet. However, the controller selects the QoS policies. Marking and policing of egress SSID and client policies are applied at the controller. QoS statistics are collated for client and SSID targets in the ingress direction. Statistics are supported only for ingress policies with a maximum of five classes on wireless targets. For very large policies, statistics for ingress policies are not visible at the controller. The frequency of the statistics depends on the number of clients associated with the AP.
Implement Control part of AVC (Tie-in to QOS)	Application Visibility and Control (AVC) classifies applications using deep-packet inspection techniques with the Network-Based Application Recognition (NBAR2) engine, and provides application-level visibility and control (QoS) in wireless networks. After the applications are recognized, the AVC feature enables you to either drop, mark, or police data traffic. AVC is configured by defining a class map in a QoS client policy to match a protocol. AVC QoS actions are applied with AVC filters in both upstream and downstream directions. The QoS actions supported for upstream flow are drop, mark, and police, and those supported for downstream flow are mark and police. AVC QoS is applicable only when the application is classified correctly and matched with the class map filter in the policy map. **Note** This feature is applicable only to wireless clients.
Optical Feature Interface support	Supports new hardware for DWDM SFP+ and 10 G ZR SFP+ modules. For a list of all the supported SFP+ modules, see: http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_6974.html

What's New	Description
Flexible Netflow Enhancement	Supports NetFlow Data Export Format Version 10 (IPFIX). For more information, see the *Cisco Flexible NetFlow Configuration Guide*.
802.11r Mixed Mode Support	You do not have to create a separate WLAN for 802.11r support. You can specify the non-802.11r clients to associate with an SSID that is enabled with 802.11r.

Supported Hardware

Cisco Catalyst 3850 Switch Models

Table 2 Cisco 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)
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

Table 2 Cisco Catalyst 3850 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
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
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 pluggable (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.

Cisco Catalyst 3650 Switch Models

Table 4 Cisco 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 Cisco 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 Cisco 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, see 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 Cisco Mobility Services Engine

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

Table 6 Cisco 5700 Series WLC-Supported Products

Product	Platform Supported
Access Point	Cisco Aironet 700, 700W, 1040, 1140, 1260, 1530, 1570, 1600, 1700, 2600, 2700, 3500, 3600, 3700
Cisco 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
	AIR-AP1572IC
	AIR-AP1572EC
Cisco Aironet 1600 Series	AIR-CAP1602E
	AIR-CAP1602I
Cisco Aironet 1700 Series	AIR-CAP1702I-x-K9
	AIR-CAP1702I-xK910
Cisco Aironet 2600 Series	AIR-CAP2602E
	AIR-CAP2602I
Cisco Aironet 2700 Series	AIR-CAP2702I-x-K9
	AIR-CAP2702E-x-K9
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	Cisco Catalyst 3850	Cisco Catalyst 3650	Cisco 5508 WLC or WiSM2	Cisco MSE	Cisco ISE	ACS	Cisco PI
03.06.10E	03.06.10E	03.06.10E	8.0.x	8.0[1]	2.4	5.2	3.1.4 DP6
03.06.09E	03.06.09E	03.06.09E	8.0.x	8.0[1]	2.4	5.2	3.1.4 DP6
03.06.08E	03.06.08E	03.06.08E	8.0.x	8.0[1]	1.3	5.2	3.1.4 DP6
03.06.07E	03.06.07E	03.06.07E	8.0.x	8.0[1]	1.3	5.2	3.1.4 DP6
03.06.06E	03.06.06E	03.06.06E	8.0.x	8.0[2]	1.3	5.2	3.1.4 DP6
03.06.05E 03.06.04E 03.06.03E 03.06.02E 03.06.01E 03.06.00E	03.06.2aE 03.06.01E 03.06.00E	03.06.2aE 03.06.01E 03.06.00E	8.0.x 7.6	8.0[1]	1.3 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, Cisco MSE 7.6 is not compatible with Cisco IOS XE Release 3.7E. Therefore, we recommend that you upgrade to Cisco MSE 8.0.
2. If Cisco MSE is deployed on your network, we recommend that you upgrade to Cisco Prime Infrastructure 2.1.2.
3. If Cisco 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. Cisco 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. Cisco 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 IOS Version	Cisco Wireless Control Module Version	Access Point Version
03.06.07E	15.3(3)E7	10.2.170.0	15.3(3)JN12
03.06.06E	15.3(3)E6	10.2.160.0	15.3(3)JN11
03.06.03E	15.2(2)E3	10.2.131.0	15.3(3)JN7
03.06.02E	15.2(2)E2	10.2.120.0	15.3(3)JN4
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, and to install the packages from a new software bundle file, use the **software install** privileged EXEC command. You can install the software bundle from the local storage media or it can be installed over the network using TFTP or FTP.

The **software install** 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
Universal	ct5760-ipservicesk9.SPA.03.06.02.E.152-2.E2.bin
Universal without DTLS	ct5760-ipservicesk9ldpe.SPA.03.06.02.E.152-2.E2.bin

Important Upgrade Note

- After you upgrade to Cisco IOS XE Release 3.6.xE, the web authentication 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 Choose **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 3.6.x 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 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	
Atheros HB92/HB97	8.0.0.320
Atheros HB95	7.7.0.358
Broadcom 4360	6.30.163.2005
Cisco CB21	v1.3.0.532
Dell 1395/1397/Broadcom 4312HMG(L)	5.30.21.0
Dell 1501 (Broadcom BCM4313)	v5.60.48.35/v5.60.350.11
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
Dell 1560	6.30.223.215
Engenius EUB 1200AC(USB)	1026.5.1118.2013
Intel 1000/1030	v14.3.0.6
Intel 4965	v13.4

Table 11 Client Types (continued)

Client Type and Name	Version
Intel 5100/5300	v14.3.2.1
Intel 6200	v15.15.0.1
Intel 6205	v15.16.0.2
Intel 6235	V15.10.5.1
Intel 6300	v15.16.0.2
Intel 7260(11AC)	17.16.0.4, Windows 8.1
Intel 7265	17.16.0.4
MacBook 2015	OSX 10.10.5
Macbook Air new	OSX 10.10.5
Macbook Air old	OSX 10.10.5
MacBook Pro	OSX 10.10.5
MacBook Pro with Retina Display	OSX 10.10.5
Netgear A6200 (USB)	6.30.145.30
Netgear A6210 (USB)	5.1.18.0
Handheld Devices	
Apple iPad Air	iOS 8.4.1(12H321)
Apple iPad Air 2	iOS 8.4.1(12H321)
Apple iPad Mini with Retina display	iOS 8.4.1(12H321)
Apple iPad2	iOS 8.4.1(12H321)
Apple iPad3	iOS 8.4.1(12H321)
Intermec CK70	Windows Mobile 6.5 / 2.01.06.0355
Intermec CN50	Windows Mobile 6.1 / 2.01.06.0333
Samsung Galaxy Tab Pro SM-T320	Android 4.4.2
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	
Apple iPhone 4S	iOS 8.4(12H143)
Apple iPhone 5	iOS 8.4(12H143)
Apple iPhone 5c	iOS 8.4.1(12H321)
Apple iPhone 5s	iOS 8.4.1(12H321)
Apple iPhone 6	iOS 8.4.1(12H321)
Apple iPhone 6 Plus	iOS 8.4.1(12H321)
Ascom i75	1.8.0
Cisco 7921G	1.4.5.3.LOADS
Cisco 7925G	1.4.5.3.LOADS
Cisco 8861	Sip88xx.10-2-1-16

Table 11 Client Types (continued)

Client Type and Name	Version
Google Nexus 5	Android 5.1
HTC One	Android 5.0
Nexus 6	Android 5.1.1
Nokia Lumia 1520	Windows Phone 8.1
OnePlusOne	Android 4.3
Samsung Galaxy Nexus	Android 4.0.2
Samsung Galaxy Nexus GTI9200	Android 4.4.2
Samsung Galaxy Note (SM-900)	Android 5.0
Samsung Galaxy S III	Android 4.3
Samsung Galaxy S4– GT-I9500	Android 5.0.1
Samsung Galaxy S5-SM-G900A	Android 4.4.2
Samsung Galaxy S6	Android 5.0.2
Sony Xperia Z Ultra	Android 4.4.2
Spectralink 8030	119.081/131.030/132.030
SpectraLink 8450	3.0.2.6098/5.0.0.8774
Vocera B1000A	4.1.0.2817
Vocera B2000	4.0.0.345

Important Notes

- With Cisco Prime Infrastructure 2.1.1, the refresh configuration 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 3.6E:
  - Outdoor Access Points
  - Mesh, FlexConnect, and OfficeExtend access point deployment

Limitations and Restrictions

- We recommend that you configure the **access-session interface-template sticky timer** *timer-value* command at the global or interface configuration mode, and not within the template.

- The web UI access for the controller should be enabled only by using the IP address of the controller. For example, *http://<ip>*. We recommend that you do not use *https://<ip>/wireless* address, as it might result in Privilege Level 1 access. To mitigate this problem, you either refresh the browser or use *https://<ip>* address.
- The web UI home page may not load when the **ip http access class** command is enabled. When you encounter this issue, we recommend that you perform the following tasks:
  1. Run the **show iosd liin** command.
  2. Get the internet-address and configure the same IP as permit in the access list.
- For web UI access using the TACACS server, the custom method-list for authentication and authorization pointing to the TACACS server group does not work. Use the default authorization method list pointing to the same TACACS server group for the web UI to work.
- We recommend that you run the **exception dump device second flash** command after the install process. This helps to store the crash files in a secondary flash during a crash when there is no available space in the main memory area to store the crash information.
- Flex links are not supported. We recommend that you use spanning tree protocol (STP) as the alternative.
- Restrictions for Cisco TrustSec:
  - Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.
  - Cisco TrustSec for IPv6 is not supported.
  - Dynamic binding of IP-SGT is not supported for hosts on Layer 3 physical routed interfaces because the IP Device Tracking feature for Layer 3 physical interfaces is not supported.
  - Cisco TrustSec cannot be configured on a pure bridging domain with the IPSG feature enabled. You must either enable IP routing or disable the IPSG feature in the bridging domain.
  - Cisco TrustSec on the controller supports up to 255 security group destination tags for enforcing security group ACLs.

Caveats

Cisco Bug Search Tool

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. Access the BST using your Cisco user ID and password:

   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

Open Caveats for Cisco IOS XE Release 3.6.10E

There are no open caveats in Cisco IOS XE release 3.6.10E.

Open Caveats for Cisco IOS XE Release 3.6.9E

There are no open caveats in Cisco IOS XE release 3.6.9E.

Open Caveats for Cisco IOS XE Release 3.6.8E

There are no open caveats in Cisco IOS XE release 3.6.8E.

Open Caveats for Cisco IOS XE Release 3.6.7E

Bug ID	Headline
CSCve37498	Switch sends duplicate accounting message causing ISE to generate mis-configured NAS Alarms
CSCvf18046	Sticky timer stops if the connected device is moved from one port to the other port before timer expires

Resolved Caveats for Cisco IOS XE Release 3.6.10E

There are no resolved caveats in Cisco IOS XE release 3.6.10E.

Resolved Caveats for Cisco IOS XE Release 3.6.9E

There are no resolved caveats in Cisco IOS XE release 3.6.9E.

Resolved Caveats for Cisco IOS XE Release 3.6.8E

There are no resolved caveats in Cisco IOS XE release 3.6.8E.

Resolved Caveats for Cisco IOS XE Release 3.6.7E

Bug ID	Headline
CSCty18171	SNMP poll of CISCO-PROCESS-MIB cause high CPU and SNMP poll timeout
CSCuv22571	Device reloads unexpectedly due to memory corruption in slaJitterPacketBuild
CSCuw15256	PKI: certificate validation fails after reload
CSCux83859	Switch fails 802.1x when identity field in EAP ID response is blank
CSCva74457	Sticky interface template not working
CSCvc44866	SSH/vty sessions lock up leading to loss of access to device
CSCvd01096	ACL with log prints syslogs even when ACL target is admin shut
CSCvd01598	TACACS+ timeout retransmission is done 3 times prior marking server down
CSCvd35291	Removal of access-session template monitor; creates Drop MAC entries in CAM table
CSCve04704	Session blocked in Pending Deletion state due to SM Accounting Feature

Resolved Caveats for Cisco IOS XE Release 3.6.6E

Bug ID	Headline
CSCus83638	5-GHz radio on Cisco AP beaconing but not accepting client associations
CSCuz16135	If wireless is disabled, close the socket, listening on 5246 port
CSCva16996	Cisco 5760 WLC sending null values for ipaddresstable in cldcClientByIpTable
CSCva34854	AP not joining wireless E/D and IP forward-protocol UDP E/D
CSCva65432	NGWC 5760 A-MSDU settings are not saved after reload
CSCvb54115	Adhoc rogues marked as external are removed after timeout

Resolved Caveats for Cisco IOS XE Release 3.6.5Ea

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 37.

Bug ID	Headline
CSCuv87976	CLI Knob for handling leap second add/delete ignore/ handle.
CSCvb19326	NTP leap second addition is not working during leap second event.
CSCvb29204	BenignCertain on IOS and IOS-XE.

Resolved Caveats in Cisco IOS XE Release 3.6.5E

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 37

Bug ID	Headline
CSCut39010	Multiple APs reset with beacons stuck
CSCut56741	AP1600: Radio reset with "STOPPING CPQ FWD TRACE ON Bad CPQ removal"
CSCut85027	AP is generating corrupted core dump
CSCuv08570	Lightweight access point loses all configuration at times after power cycle
CSCuv50017	Airties WGB not getting IP address when connecting to Cisco 5760 WLC
CSCuv62540	Adding –S domain support for Hong Kong, Macau, Thailand, and Vietnam
CSCuv73422	IOS-UX AP: NDP propagation for US country uses UX domain
CSCuw57588	Cisco 3600 AP reloads unexpectedly on am_xml_GetChildCount
CSCuw78795	REPLAY_ERR msg showing WLAN ID as VLAN ID of the AP
CSCux65356	Converged Access Solutions–AP join failure due to ap_index out of sync between IOS and FED
CSCuy01628	SSID output QoS shaper could drop CAPWAP fragments
CSCuy19990	IOS 15.2 802.1x critical VLAN feature - reinitialize is not working
CSCuy29078	Cisco 5760 WLC FED reloads unexpectedly
CSCuy32363	MDNS leaking when roaming to foreign in L2 sticky-anchor
CSCuy33187	Need FCC -B domain DFS support on Cisco 1600 AP
CSCuy37932	Cisco 5760 WLC does not forward 224.0.0.1 link local packets to wireless clients
CSCuy43392	Cisco 5760 WLC reloads unexpectedly at snmp_subagent
CSCuy81218	AP support of DFS detection in 100% transmission BW
CSCuz16907	Inversion issue of "wireless broadcast vlan x" command

Resolved Caveats in Cisco IOS XE Release 3.6.4E

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 37.

Bug ID	Headline
CSCui42745	GUI and CLI access to Cisco Catalyst 3850 in spite of no "wireless mgmt-via-wireless"
CSCun19445	Cisco AP 802.11 5-GHz channel switch mode 0 is not displayed in the show run command
CSCuo18999	IOSXE-7-PLATFORM: 3 process wcm: Device Type Unknown
CSCur48944	Issue noticed in Client Statistics Reports and Optimized Roaming
CSCus99901	Unsupported AP message on Cisco 3850 without wireless enabled

Bug ID	Headline
CSCut23325	Cisco 1700AP not encrypting ICMP and ARP sent from the client over the air
CSCut40305	Console logs are creating during AP-GUI login session and PSE status
CSCut88813	WLAN cannot be configured with a space in psk shared key on NGWC 3.7
CSCuu25580	VTY0-4 settings are modified if switch is accessed via WebUI
CSCuu42580	When calls are active, “sh wireless client calls active” shows calls as 0
CSCuu47016	Cisco Application Visibility and Control UDP Vulnerability
CSCuu79717	IPv6 RADIUS accounting is not working
CSCuu85713	Input queue full forced to restart the WLC to restore
CSCuu93296	EAP-TLS loosing device certificate in standalone mode after reboot
CSCuv02964	Memory leak in with 802.11x on IOS-XE switch
CSCuv04474	Cisco AP1700 reloads unexpectedly during multicast client traffic (cont.CSCuu89311)
CSCuv19773	NMSP attach suppress not being added into run-config on WS-C3850-24P
CSCuv22549	In WAN DTLS certificate packets come out of order could lead to AP join failure
CSCuv22936	AP Flapping -capwap keepalives are not replied to
CSCuv23475	CPUHOG and system unexpectedly reloads on “no network 0.0.0.0” with vnet configuration on intf
CSCuv26804	Iosd reloads unexpectedly with DHCP snooping enabled
CSCuv46710	Segmentation Fault in authentication manager
CSCuv60764	Session timeout is not applied on CoA
CSCuv65116	SNMP: Cannot clear PST Config for APs associated to Cisco 5760 WLC
CSCuw12199	Sends management IP as called-station-id
CSCuw13827	IOS XE 3.6.3E Stack AP configurations are not synced
CSCuw16669	CWA: web authentication redirect fails on mid auth-roaming between MAs in Cisco Converged Access Solution
CSCuw20068	Displays only Home and Monitor web GUI options
CSCuw38233	Mobility tunnel between MA/MC drops when default egress policy is set to deny
CSCuw38902	Web GUI: 500 internal error on Cisco IOS XE 3.7.1SE
CSCuw45473	CAPWAP AP not joining to Cisco 5760 using broadcast discovery request
CSCuw48448	APF-3-INVALID_RADIO_TYPE
CSCuw52729	Enabling AutoQoS causes “line vty 0 4 length” set to 0
CSCuw55669	Iosd unexpectedly reloads on switch and authentication manager
CSCuw61261	WLC reloads unexpectedly on ios_authproxy 3.6.3
CSCuw66585	Rogue rule for infrastructure SSID is not saved on reboot
CSCuw91099	HA unexpectedly reloads one after another
CSCuw93850	Unable to modify AP port QoS configuration if AutoQoS VoIP is applied
CSCuw97388	SNMP should allow 128 characters for AP groups description for NGWC NOVA
CSCux13679	MA announce Timeout timer leaking

Bug ID	Headline
CSCux28874	NGWC EAPOL M5 retransmissions does not increment replay counter
CSCux79913	The client column in the load-info command is incorrect

Resolved Caveats in Cisco IOS XE Release 3.6.3E

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 37.

Bug ID	Headline
CSCum01456	Windows 8 clients do not authenticate with AES on autonomous APs.
CSCun12965	Lightweight AP should not send jumbo frame by default.
CSCun56310	The following error message is observed continuously in WLC message logs: "LWAPP-3-VENDOR_PLD_VALIDATE_ERR:".
CSCuo56388	Controller is printing the following message: "%MM-3-INVALID_PKT_RECVD: 1 wcm: Received an invalid packet".
CSCup73878	The **show version** command output shows unnecessary information.
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.
CSCuq09859	APs sending GARP and ARP requests approximately every 2 seconds.
CSCuq48800	Low throughput due to UAPSD for Intel 7260 WiFi chipset.
CSCuq61018	"*%LB-2-LB_RESOURCE_UPDATE_FAILED:" logs seen on console.
CSCuq62007	IOSd crash occurred on 4500E platform after syncing it with MSE.
CSCuq86269	DFS detection due to Broadcom spurious emissions.
CSCuq86274	On very specific RF environment, 1530 may detect radar across all channels.
CSCuq90632	3702 crashed with a traceback.
CSCuq99230	AP syslog fails due to default setting 'logging server-arp'.
CSCur08813	Windows 8 is not connecting to wireless when using 'aes-ccm tkip' on dot11radio.
CSCur10397	The ap core-dump ip validation is wrong.
CSCur17996	Switch loses country code after reboot.
CSCur22714	AP 3602 trying to contain its own RM3000AC module.
CSCur24512	3602i AP crash at dot11_driver_ie_find.
CSCur45862	AP's cannot discover WLC through option 43.
CSCur60244	Cisco 5760 WLC webauth on MAC filter failure fails on new mobility with Cisco 5500 WLC.
CSCur78836	AP forwards frame to STP Blocked interface.
CSCur87501	Post-ACL not applied after CWA CoA in New Mobility with 3850 as foreign.
CSCus03487	AP 3700 sends wrong TLV during power level negotiation.
CSCus13331	iosd crash in_be_http_epm_process_clean_up.
CSCus13594	Slow in getting the DHCP address in the AP 2700.

Bug ID	Headline
CSCus30769	BSSID containing itself and also adding itself to client exclusion list.
CSCus44831	1702 AP reports power error with 802.3af power source.
CSCus45806	Enable CDP Spare pair TLV for 1570 and 1530 series access points
CSCus48787	An AP radio may go down with log messages.
CSCus49126	AP 3702 floods RTS frames @ 8000pps to departed client.
CSCus50813	Client stuck in APPLYINGPOLICY (received 0 as EPM session handle).
CSCus53635	Add 802.11a Philipines country support for 1532I Aps joined to Cisco 5760 WLC.
CSCus73176	AIR-CT 5760 running Cisco IOS XE Release 03.03.05SE reboots without generating a crash file.
CSCus77477	NGWC Increase the number of URLs allowed in a DNS ACL in WLC.
CSCus91957	RogueAP trap from Cisco 5760 WLC has invalid rogueAP/detectingAP macs.
CSCut02707	Cisco 5760 WLC is crashing on memory allocation issue.
CSCut26137	3702 - Voice Queue stuck, with no new clients able to associate.
CSCut27272	CPU HOG and crash due to Auth Manager process.
CSCut27350	MA Load Balancing not working as expected.
CSCut30423	Cisco 5760 WLC fed crash is observed.
CSCut50679	The following memory leak is observed: “tlv_calloc memory leak (QoS related code)”.
CSCut64070	High CPU utilization by cli_agent.
CSCut68706	Auth Manager holding memory incrementing for version 152-3.E!!.
CSCut76129	There is a problem in loading in page CT5760.
CSCut76909	LAP is unable to setup DTLS, if packets arrive out of order in NGWC.
CSCut80382	A device experiences a hap reset after the FED service is abnormally terminated.
CSCut80510	The command **show proc mem detailed process iosd maps** is broken.
CSCut89864	FED crash on Cisco 5760 WLC running Cisco IOS XE Release 3.6.2 if WLAN name is greater than 22 character.
CSCut95175	MAC Address being truncated in the username field of accounting message.
CSCut98006	DFS detections due to high energy profile signature on 2600/3600.
CSCut98205	AIR-CT5760 lost configuration after upgrade/reboot.
CSCut99032	There are 2 channels 0,0 on 5ghz DCA list and cannot remove it.
CSCuu00760	Stale IPDT entries with %WCDB-3-WCDB_IP_CONFLICT error with guest anchor.
CSCuu04476	Cisco 5760 WLC random CLI hang and sometimes console lockup.
CSCuu05565	NDP packets not tx'ed on secondary20 channels
CSCuu10251	CMI show CLI crash when system runs low on memory.
CSCuu12308	CWA does not properly work with 2 anchors configured on the WLAN.
CSCuu14197	AIR-CT5760-K9 WCM crash in process process_get_next.
CSCuu18788	DATACORRUPTION-1-DATAINCONSISTENCY when polling ceExtSysBootImageList.

Bug ID	Headline
CSCuu23858	Persistent Device Propagation cannot be configured via GUI.
CSCuu27987	traceback @ ifm_allocate_capwap_port_spoke_id.
CSCuu29813	DHCP snoop on uplink VLAN create WCDB error, does not match binding VLAN.
CSCuu37077	3600P limited channels/power similar to CSCus35411.
CSCuu42396	AP radio FW image install failure in the bootup.
CSCuu45274	The **debug client mac-address** command shows association from other mac addresses.
CSCuu47450	7925 roam will fail intermittently (client stuck in authenticating state).
CSCuu50392	Auth Manager memory leak with ISE authentication.
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.
CSCuu61591	WLAN with space cannot be added to AP group.
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.
CSCuu71587	WPA-AES configuration is getting disabled on the CLI after WLC/switch reboot.
CSCuu73067	The **show ap join stats summary** command output shows error message.
CSCuu75209	WCM processing of rx packets after port initialization (ports 5246/5247).
CSCuu79865	IOSD not accepting QoS install request sent by WCM.
CSCuu81895	New 1572 out of box AP in local mode +recovery image not starting CAPWAP process.
CSCuu99792	WLAN Configuration is not applied due to “exceeds MAX_QUEUED_RECV_BUFS”.
CSCuv01091	Web UI shows an error while configuring the **ip http active-session-modules** command.
CSCuv06190	WCM crash in TCP library.
CSCuv06451	IOSd crash in eap_auth_terminal_state calling free_internal.
CSCuv07427	TCP connection cannot be established with Openflow agent.
CSCuv23751	When J4 is configured in NGWC WLC, "J4" is used as Country information on Beacon frame. Due to that, some clients including MAC book pro cannot recognize W53, W52 band.
CSCuv45515	Cisco 5760 WLC crash in fed al_fnf_get_iif_fnf_info.
CSCuv69297	CLI hangs on certain show commands.
CSCuv69997	Cisco 5760 WLC crash due to APF-3-VALIDATE_DOT11i_CIPHERS_FAILED Errors.
CSCuv23905	Client is stuck in APPLYINGPOLICY/Authentication state.

Resolved Caveats in Cisco IOS XE Release 3.6.2E

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 37.

Bug ID	Headline
CSCus86196	Cannot access Web GUI with "500 internal error"
CSCus54365	Cisco 5760 WLC Memory leak since upgrade to 3.6.0
CSCus55254	Redirect fails randomly once there are more than 7 HTTP connections
CSCus13576	Memory leaks at pki_ssl_type.c
CSCus81079	WGA does not work when wired client is on access VLAN not same as native
CSCup03310	WCM memory leak @spi_openssl_dtls_Connection_ha_shadow_create_internal
CSCus44854	RADIUS attribute 31 formatting does not affect MAC authentication
CSCus70212	Swapping between two WLANs is not working on Apple client with fast SSID enabled
CSCus97742	WCM Crash at spamGetLCBFromMacTemp
CSCur24788	CWA flow break if accounting enabled in GA scenario
CSCur59580	Cisco 5760 WLC-HA crash on Cisco IOS XE Release 3.3.3
CSCus58769	Error while accessing wizard if gi0/0 has no IP
CSCuo07995	IOSD leak @ be_ip2access_add_acl_item2
CSCuo31164	Match prefix is removed from SNMP V3 configuration after host command
CSCup98782	Fed crash observed at web-auth pending process after extended test
CSCuq00349	5760 Amber LED on first port of port channel of Flexlink Backup Port
CSCun06200	CoA session terminates issued from ISE active sessions page are failing for wireless endpoints
CSCur48634	HA fails due to bulk synchronization failure with encrypted password
CSCuq20305	Routing protocol control packets should not be dropped
CSCuq40329	snmp_subagent crash on 3.13.71EZP
CSCus48938	Eqc in an infinite loop
CSCuq59661	QoS policy on SSID not installed when policy removed and reapplied
CSCur13155	FED crash applying ACL policies due to corrupted memory on Cisco IOS XE Release 3.3.4
CSCur64098	Port policy gets uninstalled on FED if apply the multi-destination policers
CSCur30539	HTTPD context does not cleared if web-auth required through virtual IP
CSCus17182	Option to disable success message before the page get redirected to URL
CSCup32681	Standby in Unknown state after forced switchover
CSCup31330	IOSd crash @ ios_syncblk_release_w_pc_inline
CSCup92808	No CWA redirect for client in case it roamed in webauth-reqd state
CSCur54755	Allow configuration of server and supplicant timeout for CTS dot1x
CSCur64098	Port policy gets uninstalled on FED if apply the multi-dest policers.
CSCus90675	Client stuck in IPLEARN with aaa override and dynamic VLAN

Bug ID	Headline
CSCuq89707	IOS AP OpenSSL August 2014 vulnerabilities
CSCuq90632	AP3702 crashed with a traceback
CSCuq86750	NDP packets on 3700 abnormally low TX power
CSCus35411	AP3702P access points has only 36, 40 two channels available
CSCur88864	3600 APs with AC module shows 100% Rx utilization on slot-2
CSCus49126	AP3702 floods RTS frames at@ 8000pps to departed client

Resolved Caveats in Cisco IOS XE Release 3.6.1E

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 37.

Bug ID	Headline
CSCuq32016	Incorrect AFD client SSID association
CSCur50946	APs manufactured in August/September/October 2014 unable to join an IOS-XE controller
CSCuh14797	Client not authenticating due to wrong mobility peer detail in anchor
CSCul44417	Support Local MAC filter entries on a per WLAN basis for NGWC
CSCuo63950	WCM crash on customer production network Tx power auto CLI
CSCuo67946	Client statistics are not updated after roaming
CSCuo75037	High AP Priority Flaps Continuously
CSCuo77295	Secondary Cisco 5760 WLC crashed during reverting back from Primary
CSCuo78990	WCM Crash @ eip_wcm_RRM_LRAD_DATA_t_neighbor
CSCuo79134	Cisco 5760 WLC MC client stops updating PMK from other MC if mobility name is changed
CSCuo86406	–D regulatory domain not supported with India (IN) country code in NGWC
CSCuo87797	Voice call going into best effort in upstream traffic
CSCup29935	RRM ceases to function completely if standard switch added as MA
CSCup43034	WCM crash running 03.03.03 __be_qos_tam_db_fe_install_pm_on_target
CSCup59493	NGWC: W56 Static TxPower level changes to Max after AP reboot
CSCup60078	7921/7925 phone not able to place call after failover
CSCup62150	Client QoS policy is not applied for inter-controller roamed client
CSCup63909	Roaming fails when Anchored phone roams back from foreign
CSCup73590	WCM crash in Mobility code:maHandleLocalClientDelete / mmMaUdsSend
CSCup79131	WCM crash wcdb_spi_client_state_change
CSCuq12503	Web GUI does not work on 3850
CSCuq30940	SNMP changes for supporting Cisco AP1570E/I and Cisco AP1700E/I in PI
CSCuq48106	DHCP req sent while switching SSIDs mapped to different VLAN groups fail
CSCuq52024	NGWC changes for Aux port feature in Cisco AP1700.

Bug ID	Headline
CSCuq58700	“Wlan PSK profile applied to NGWC with invalid argument “clear””
CSCuq80970	AP setting page Apply button is not working
CSCuq86355	Failed to create multicast tunnel with standby Cisco 5760 WLC
CSCuq98331	Web UI: User’s page keeps loading on GUI
CSCur17400	Packet drop observed in AP while traffic is having DSCP value
CSCur40052	IOS-XE Plain text admin credentials saved to file
CSCur35879	Parameter-map cannot be deleted after “wlan” int is shut
CSCup76410	IOSd crash on Cisco 5760 WLC running 3.6SE at get_logo_location

Resolved Caveats in Cisco IOS XE Release 3.6.0E

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 37.

Bug ID	Headline
CSCui69119	IPDT: rejected channel conf and standby failed to boot up
CSCun68485	Router ACL (RACL) on SVI in output direction applied to bridged traffic
CSCun78227	Incorrect temperature thresholds reported via SNMP
CSCun97765	Unable to disable IPDT

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.
