Release Notes for Catalyst 3650 Series Switch, Cisco IOS XE Release 3.6.xE

First Published: June 27, 2014
Last Updated: May 31, 2019

OL-32647-01

This release note gives an overview of the features for the Cisco IOS XE 3.6.xE software on the Catalyst 3650 series switch.

Unless otherwise noted, the terms *switch* and *device* refer to a standalone switch and to a switch stack.

Contents

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

Introduction

The Catalyst 3650 switches are the next generation of enterprise class stackable access layer switches that provide full convergence between wired and wireless networks on a single platform. This convergence is built on the resilience of new and improved 160-Gbps StackWise-160 and Cisco StackPower. Wired and wireless security and application visibility and control are natively built into the switch.

The Catalyst 3650 switches also support full IEEE 802.3at Power over Ethernet Plus (PoE+), modular and field replaceable network modules, redundant fans, and power supplies. The Catalyst 3650 switches enhance productivity by enabling applications such as IP telephony, wireless, and video for a true borderless network experience.

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

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

What's New in Cisco IOS XE Release 3.6.10E

There are no new features in this release.

What's New in Cisco IOS XE Release 3.6.8E

There are no new features in this release.

What's New in Cisco IOS XE Release 3.6.7bE

There are no new features in this release.

What's New in Cisco IOS XE Release 3.6.7E

There are no new features in this release.

What's New in Cisco IOS XE Release 3.6.6E

There are no new features in this release.

What's New in Cisco IOS XE Release 3.6.5bE

There are no new features in this release.

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 (– 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 starting with Cisco IOS XE Release 3.6.5E are: Cisco Aironet 700, 700W, 1040, 1140, 1260, 1530, 1570, 1600, 1700, 2600, 2700, 3500, 3600, 3700.

What's New in Cisco IOS XE Release 3.6.4E

- Beginning with Cisco Wireless Release 8.1 and later, Mobility Agent related CLI/WebUI from AireOS-based controllers as Mobility Controller is no longer supported.
- Pairing of 3850, 3650 switches, or 4500E Sup-8E, as Mobility Agent is not supported with Cisco Wireless Release 8.1 and later releases.
- 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.

What's New in Cisco IOS XE Release 3.6.3E

- CDP Bypass—The sessions are established in single and multi-host modes for IP Phones. However, if voice VLAN and 802.1x on an interface port is enabled, then the CDP Bypass is enabled when the host mode is set to single or multi host mode.

Note By default the host mode is set to single mode in <legacy> mode and multi-authentication in the edge mode.

Use the following commands to configure CDP bypass:

```
Switch> enable
Switch# configure terminal
Switch(config)# interface <interface-id>
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan <vlan-id>
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication host-mode single | multi-host
Switch(config-if)# dot1x pae authenticator
```

- 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.

- Multiple VLAN support for Wired Guest Access—Wired guest anchor can now support multiple VLANs and multiple guest LANs. Different VLANs can be assigned for each security profile like openauth, webauth and web consent.For more on Wired Guest Anchor, see "Wired Guest Access with Both Anchor and Foreign" section on page 6.

Note The Catalyst 3650 switch cannot be used as an anchor controller.

- Long URL—Webauth parameter map supports external URL with a maximum length of 256 characters. While configuring login URL for webauth, care should be taken that the complete length of the redirected URL should not exceed 550 characters. Commands used to configure external webauth parameter map with long URL are given below:

```
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—Customers can customize the HTML pages to send credentials in HTTP GET Request.

Note We recommended password encryption while using the HTTP GET Request.

- Append AP radio mac or SSID or client mac—External URLs sent to the client can be appended with AP radio mac address or SSID or client mac address or any of these combinations, so that the webauth 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 commands to configure this feature are given below:

```
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
```

- Multi-privilege level support to login to WEB UI through TACACS+—In releases prior to 3.6.3, the users were restricted to privilege level 15. In this release, users with privilege level 1 is supported to login and access for monitoring the controller, through TACACS+ or local authentication.
- Cisco 1570 Series Access Point—This release supports Cisco 1570 Series Access Point, in local mode.
- LWA—Multiple WebServer Configuration for External WebAuth.

  The user has 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.

Wired Guest Access with Both Anchor and Foreign

Restrictions

- Wired guest VLAN on the access-switch should not have any SVI's present on any of the local switches. It should terminate directly on the foreign, so that the traffic is exported to the anchor.
- Anchor VLAN should not be allowed on the foreign controllers' 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 done during scheduled network downtime period.

Overview

In enterprise networks, there is typically a need for providing network access to its guests on the campus. The 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 way. 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 DMZ (Demilitarized Zone) 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 Catalyst 3650 switch as foreign anchor and Cisco 5760 Wireless LAN controller acting as Guest Anchor in the DMZ. The feature works in a similar fashion on Cisco Catalyst 3850 switch acting as foreign controller.

The guest user connects to the designated wired port on a access layer switch for access and optionally may be made to go through Web Consent or Web Authentication modes, depending upon the security requirements (details in later sections). Once 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 client connects for network access. It initiates tunnel requests. Guest anchor is the switch where the client actually gets anchored.

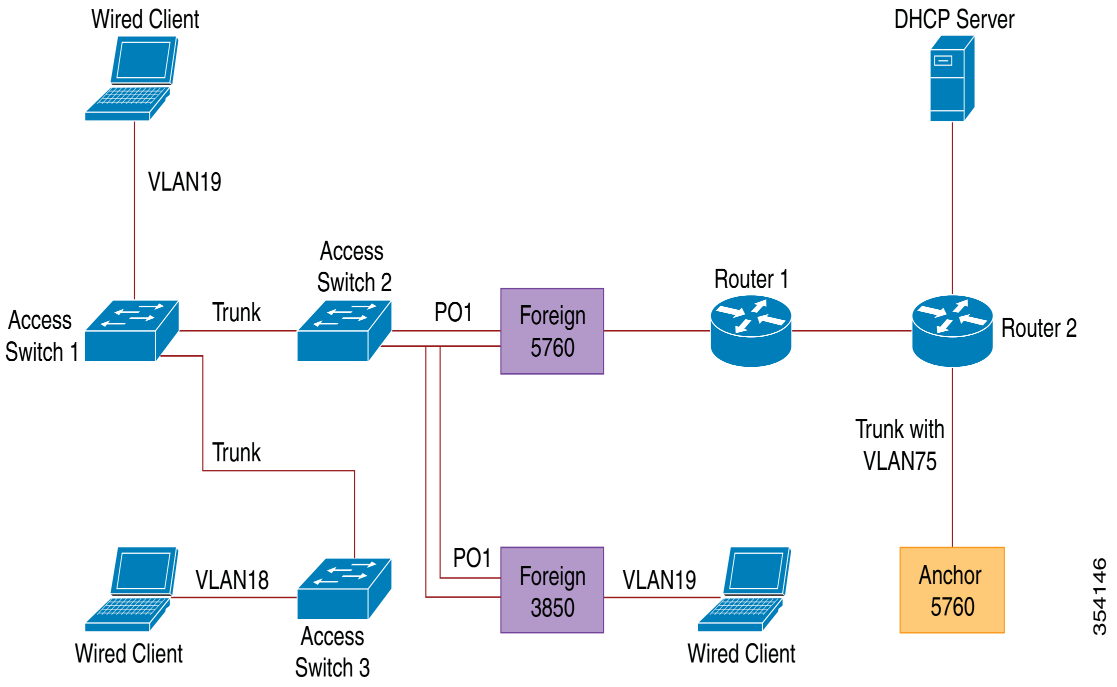
Before guest access feature can be deployed, there must be a mobility tunnel established between the foreign anchor and guest anchor switches. Guest access feature works for both MC (Foreign Controller)>> MC (Guest Anchor) and MA (Foreign Controller)>>MC (Guest Anchor) models. The foreign anchor switch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

Deployment Scenario

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

The diagram below shows the topology used in the deployment scenario:

Figure 1-1 Wired Guest Access with Both Anchor and Foreign



Open Authentication

Guest Anchor Configuration:

Step 1 Enable IPDT and DHCP snooping on client VLANs (VLAN75 in this example). Client VLAN has to 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 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 the Cisco WLC 5760 itself 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.

```
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' and applies the subscriber policy 'OPENAUTH'. The 'OPENAUTH' policy as described below should be created first:

```
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 for VLAN

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

Step 4 The 'OPENAUTH' policy is referred to sequentially which in this case 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. Client VLAN75 only needs to exist on the guestanchor since it's 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 Tunnel request is initiated from the foreign to the guestanchor for the wired client and

A 'tunneladdsuccess' indicated that the tunnel build up process completed:

On the ACCESS-SWITCH1 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
```

WEBAUTH

Guest Anchor Configuration

Step 1 Enable IPDT and DHCP snooping on clientVLAN(s), in this case VLAN75. Client VLAN needs to be created on the guestanchor.

```
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 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 radius and 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 the Cisco WLC 5760 itself acting as the mobilityanchor.

```
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 need to be setup on the foreign.

```
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' and applies the subscriber policy 'WEBAUTH'. The 'WEBAUTH' policy as described below should be created first:

```
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 for VLAN

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

Step 4 The 'WEBAUTH' policy is referred to sequentially which in this case 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. Client VLAN75 only needs to exist on the guestanchor since it's 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 Tunnel request is initiated from the foreign to the guestanchor for the wired client and a 'tunneladdsuccess' indicated that the tunnel build up process is completed.

On the ACCESS-SWITCH1, 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

To have 2 guests LANs and assigning them to different clients we have to base them on the VLANs on which the clients are learned.

Guest Anchor Configuration

Step 1 Enable IPDT and DHCP snooping on client VLAN(s), in this case VLAN75. Client VLAN needs to be created on the guestanchor.

```
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 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 the Cisco WLC 5760 itself acting as the mobilityanchor. 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. As noted, client VLAN does not need to be setup on the foreign:

```
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' and applies the subscriber policy 'DOUBLEAUTH'. TThe vlan18, vlan19 class maps are explained in "Step4". Everything else is webauth using the second "always" class-map with "match-first" event The 'DOUBLEAUTH' policy as described below should be created first:

```
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 Mac learning should be configured on the Foreign for vlan 18 and 19.

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

Step 4 The 'vlan19' and 'vlan18' class-map contains the VLAN match criteria based on which we will differentiate which guest LAN the client falls in. It is defined below:

```
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 case 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. Client VLAN75 only needs to exist on the guestanchor since it's 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 Tunnel request is initiated from the foreign to the guestanchor for the wired client and A ‘tunneladdsuccess’ indicated that the tunnel build up process completed:

On the ACCESS-SWITCH's there are multiple Wired client connecting to wither vlan18 or vlan19 which can be then assigned the 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 3.6.2aE

No features were added or enhanced for this release. For more information about updates in this release, see the "Caveats" section on page 38.

What's New in Cisco IOS XE Release 3.6.1E

- Support for Device Sensor (LAN Base)
- 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 2.2 and 2.1.2

What's New in Cisco IOS XE Release 3.6.0E

Note **Device Classifier** has been disabled by default starting from Release 3.6.0E. Any features dependent on device classifier should enable it if required.

What's New	Description
Use this URL for 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 • Cisco Flexible Netflow Configuration Guide
Cisco IOS Device Sensor for ISE profiling	(IP Base and IP Services) Supports Cisco Identity Services Engine (ISE) profiling for connected devices by using IOS Device Sensor
VRF-aware support for IPv6 routing protocols	(IP Services) Introduces VRF-aware support for IPv6 routing protocols (VRF-aware OSPFv3, EIGRPv6, and BGPv6).
IEEE 802.1Q Tunnel (Q-in-Q)	(IP Base) Supports IEEE 802.1Q tunneling.
Medianet Support (MSP, Metadata (no QoS), Perfmon, Mediatrace)	(IP Base and IP Services) Supports Cisco Media Services Proxy, Cisco Medianet Metadata (no QoS), and Cisco Performance Monitor.
SMI Post-install	Eliminates the overhead of manual post install configuration on all the switches, in the smart install network.
Auto Security	Provides a single line CLI, to enable base line security features (Port Security, DHCP snooping, DAI)
Cisco EnergyWise	Introduces support for Cisco EnergyWise Version 2.8. For more information, see the Cisco EnergyWise software release notes and configuration guide.
IPv6 Unicast Reverse Path Forwarding	(IP Base and IP Services) Introduces support for Unicast Reverse Path Forwarding in IPv6.
WCCP in IP base	(IP Services or IP Base) Supports for Web Cache Communication Protocol (WCCP).
Object Tracking: IPv6 Route Tracking	(IP Base and IP Services) Expands the Enhanced Object Tracking (EOT) functionality to allow the tracking of IP version 6 (IPv6) routes.
IPv6 Static Route support for Object Tracking	Allows an IPv6 Static Route to be associated with a tracked-object.
Open Plug-N-Play Agent	Switch-based agent support for zero touch automated device installation solution called NG-PNP.
Cisco TrustSec Critical Authentication	Ensures that the Network Device Admission Control (NDAC)-authenticated 802.1X links between Cisco TrustSec devices are in open state even when the Authentication, Authorization, and Accounting (AAA) server is not reachable.

What's New	Description
Enabling Bidirectional SXP Support	Enhances the functionality of Cisco TrustSec with SXP version 4 by adding support for Security Group Tag (SGT) Exchange Protocol (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	(IP Base, IP Services) Controls and manages the 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 Interface Level feature to disable the SGACL on a Layer 3 interface.
Role-Based CLI Inclusive Views	(IP Base, IP Services) Enables a standard CLI view including all commands by default.
Custom Web Authentication Result Display Enhancement	Displays the authentication results on the main HTML page. There is no pop-up window to display the authentication results.
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 the custom pages containing the images are also 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.
HSRP: Global IPv6 Address	(IP Base, IP Services) Allows users to configure multiple non-link local addresses as virtual addresses. The Hot Standby Router Protocol (HSRP) ensures host-to-router resilience and failover, in case the path between a host and the first-hop router fails, or the first-hop router itself fails.
HTTP Gleaning	(IP Base, IP 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 on to the server when the session is invalid or expired.
Secure CDP	(LAN Base, IP Base, IP 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.
OSPFv3 Authentication Trailer	Provides a mechanism to authenticate Open Shortest Path First version 3 (OSPFv3) protocol packets as an alternative to existing OSPFv3 IPsec authentication.
Policy Based Routing: Recursive Next Hop	Enhances route maps to enable configuration of a recursive next-hop IP address that is used by policy-based routing (PBR).

What's New	Description
IPv6 Policy-Based Routing (IPv6 PBR)	(IP Services) Helps you manually configure how the received packets should be routed. You can identify packets by using several attributes and specify the next hop or the output interface to which the packet should be sent.
PBR Support for Multiple Tracking Options	Extends the capabilities of object tracking using Cisco Discovery Protocol (CDP) to allow the policy-based routing (PBR) process to verify object availability by using additional methods.
Web Authentication Redirection to Original URL	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	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	Provides a mechanism to configure multiple commands at the same time and associate it 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.
IPv6 Multicast Routing	(IP Services) Introduces IPv6 multicast routing.
Embedded Event Manager (EEM) 4.0	Provides unique customization capabilities and event driven automation within Cisco products.
MediaTrace 1.0	Provides the capability to diagnose Media Stream on top of various instrumentations in Cisco routers/switches and endpoints. Also addresses the MediaNet Video monitoring requirement to discover the signaling path and provides end-to-end diagnostics along the media stream routes.
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 is added to the following APs in this release: • AP2700I, AP2700E • AP1532I, AP1532E **Note** The Cisco Aironet 1530 Series APs are supported operating only in Local mode; these APs in mesh mode are not supported. • AP702W, AP702I

What's New	Description
FQDN ACLs	Access control lists (ACLs) when configured using 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 a part of DNS response. Guest users can log in using web authentication with parameter map that consists of FQDN ACL name. You can apply access list to a specific domain. RADIUS server has to send AAA attribute fqdn-acl-name to the controller. The operating system checks for the pass through domain list, its mapping, and permits the FQDN. FQDN ACL allows clients to access only configured domains without authentication. The FQDN ACL is supported only for IPv4 wireless session.
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
Auto MAC Learning of Valid Client via MSE	You can validate the rogue clients by utilizing the resources available in the Cisco Mobility Services Engine (MSE). Using MSE, you can dynamically list the clients joining to the controller. The list of clients joined to the controller is stored in the MSE as a centralized location, where the controller communicates with MSE and validates the client before reporting if the rogue client is a valid one or not. MSE maintains the MAC addresses of clients joined to the controller. The communication between the controller and MSE is an on-demand service as the controller requests this service from MSE.
QoS Upstream	Marking and policing actions for ingress SSID and client policies are applied at the 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 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 access point.
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 the 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 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 10G ZR SFP+ modules. For a list of all supported SFP+ modules, see http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_6974.html

What's New	Description
Syslog Trap Messages	Support for Syslog traps using the **snmp-server enable traps syslog** command. After enabling Syslog traps, specify the trap message severity by using the **logging snmp-trap** command. Use the **logging snmp-trap 0 7** command to enable all severity levels (0 to 7). To enable individual trap levels, configure the following commands: • **logging snmp-trap emergencies**: Enables only severity 0 traps. • **logging snmp-trap alert**: Enables only severity 1 traps. Note that, along with the Syslog traps, the Syslog history should also be applied. Without this configuration, Syslog traps are not sent. Use the **logging history informational** command to enable the Syslog history.
Flexible Netflow Enhancement	Support for IPv6 destination server export. For more information, see the Cisco Flexible NetFlow Configuration Guide. Support for 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.
Support for Cisco SFP+ Active Optical Cables	Support for Cisco SFP+ Active Optical Cables - Cisco SFP-10G-AOC1M Cisco SFP-10G-AOC2M Cisco SFP-10G-AOC3M, Cisco SFP-10G-AOC5M, Cisco SFP-10G-AOC7M, Cisco SFP-10G-AOC10. For a list of all supported SFP+ modules, see http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_6974.html

Supported Hardware

Catalyst 3850 Switch Models

Table 1 Catalyst 3850 Switch Models

Switch Model	Cisco IOS Image	Description
WS-C3850-24T-L	LAN Base	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 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 1 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
WS-C3850-12S-S	IP Base	12 SFP module slots, 1 network module slot, 350-W power supply
WS-C3850-24S-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 1 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
WS-C3850-12S-E	IP Services	12 SFP module slots, 1 network module slot, 350-W power supply
WS-C3850-24S-E	IP Services	24 SFP module slots, 1 network module slot, 350-W power supply

Network Modules

Table 2 lists the three optional uplink network modules with 1-Gigabit and 10-Gigabit slots. You should only operate the switch with either a network module or a blank module installed.

Table 2 Supported Network Modules

Network Module	Description
C3850-NM-4-1G	Four 1-Gigabit 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 3 Catalyst 3650 Switch Models

Switch Model	Cisco IOS Image	Description
WS-C3650-24TS-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
WS-C3650-48TS-L	LAN Base	Stackable 48 10/100/1000 Ethernet downlink ports, four 1-Gigabit SFP uplink ports, 250-W power supply
WS-C3650-24PS-L	LAN Base	Stackable 24 10/100/1000 PoE+[1] downlink ports, four 1-Gigabit SFP uplink ports, 640-W power supply
WS-C3650-48PS-L	LAN Base	Stackable 48 10/100/1000 PoE+ downlink ports, four 1-Gigabit SFP uplink ports, 640-W power supply
WS-C3650-48FS-L	LAN Base	Stackable 48 10/100/1000 Full PoE downlink ports, four 1-Gigabit SFP uplink ports, 1025-W power supply
WS-C3650-24TD-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
WS-C3650-48TD-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
WS-C3650-24PD-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
WS-C3650-48PD-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
WS-C3650-48FD-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
WS-C3650-48FQ-L	LAN Base	Stackable 48 10/100/1000 Full PoE downlink ports, four 10-Gigabit SFP+ uplink ports, 1025-W power supply
WS-C3650-48PQ-L	LAN Base	Stackable 48 10/100/1000 PoE+ downlink ports, four 10-Gigabit SFP+ uplink ports, 640-W power supply
WS-C3650-48TQ-L	LAN Base	Stackable 48 10/100/1000 Ethernet downlink ports, four 10-Gigabit SFP+ uplink ports, 250-W power supply
WS-C3650-24TS-S	IP Base	Stackable 24 10/100/1000 Ethernet downlink ports, four 1-Gigabit SFP uplink ports, 250-W power supply

Table 3 Catalyst 3650 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
WS-C3650-48TS-S	IP Base	Stackable 48 10/100/1000 Ethernet downlink ports, four 1-Gigabit SFP uplink ports, 250-W power supply
WS-C3650-24PS-S	IP Base	Stackable 24 10/100/1000 PoE+ downlink ports, four 1-Gigabit SFP uplink ports, 640-W power supply
WS-C3650-48PS-S	IP Base	Stackable 48 10/100/1000 PoE+ downlink ports, four 1-Gigabit SFP uplink ports, 640-W power supply
WS-C3650-48FS-S	IP Base	Stackable 48 10/100/1000 Full PoE downlink ports, four 1-Gigabit SFP uplink ports, 1025-W power supply
WS-C3650-24TD-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
WS-C3650-48TD-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
WS-C3650-24PD-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
WS-C3650-48PD-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
WS-C3650-48FD-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
WS-C3650-48FQ-S	IP Base	Stackable 48 10/100/1000 Full PoE downlink ports, four 10-Gigabit SFP+ uplink ports, 1025-W power supply
WS-C3650-48PQ-S	IP Base	Stackable 48 10/100/1000 PoE+ downlink ports, four 10-Gigabit SFP+ uplink ports, 640-W power supply
WS-C3650-48TQ-S	IP Base	Stackable 48 10/100/1000 Ethernet downlink ports, four 10-Gigabit SFP+ uplink ports, 250-W power supply
WS-C3650-24TS-E	IP Services	Stackable 24 10/100/1000 Ethernet downlink ports, four 1-Gigabit SFP uplink ports, 250-W power supply
WS-C3650-48TS-E	IP Services	Stackable 48 10/100/1000 Ethernet downlink ports, four 1-Gigabit SFP uplink ports, 250-W power supply

Table 3 Catalyst 3650 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
WS-C3650-24PS-E	IP Services	Stackable 24 10/100/1000 PoE+ downlink ports, four 1-Gigabit SFP uplink ports, 640-W power supply
WS-C3650-48PS-E	IP Services	Stackable 48 10/100/1000 PoE+ downlink ports, four 1-Gigabit SFP uplink ports, 640-W power supply
WS-C3650-48FS-E	IP Services	Stackable 48 10/100/1000 Full PoE downlink ports, four 1-Gigabit SFP uplink ports, 1025-W power supply
WS-C3650-24TD-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
WS-C3650-48TD-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
WS-C3650-24PD-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
WS-C3650-48PD-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
WS-C3650-48FD-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
WS-C3650-48FQ-E	IP Services	Stackable 48 10/100/1000 Full PoE downlink ports, four 10-Gigabit SFP+ uplink ports, 1025-W power supply
WS-C3650-48PQ-E	IP Services	Stackable 48 10/100/1000 PoE+ downlink ports, four 10-Gigabit SFP+ uplink ports, 640-W power supply
WS-C3650-48TQ-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 4 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 5 lists the supported products of the Catalyst 3650 Switch.

Table 5 Catalyst 3650 Switch 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 6 lists the specific supported Cisco access points.

Table 6 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 6 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 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 7 lists the software compatibility matrix.

Table 7 Software Compatibility Matrix

Catalyst 3650	Cisco 5700 WLC	Cisco 5508 or WiSM2	MSE	ISE	ACS	Cisco PI

03.06.08E	03.06.08E	8.0x	8.02	1.3	5.2	2.2(DP 10)
						3.1.4(DP 6)

03.06.07E	03.06.07E	8.0.x	8.02	1.3	5.2	2.2(DP 10)
						3.1.4(DP 6)

03.06.06E	03.06.06E	8.0.x	8.03	1.3	5.2	2.2(DP 10)
						3.1.4(DP 6)

03.06.05bE	03.06.2aE 03.06.01E 03.06.00E	8.0.x 7.6	8.0	1.3	5.2 5.3	2.2
03.06.05E	03.06.2aE 03.06.01E 03.06.00E	8.0.x 7.6	8.0	1.3	5.2 5.3	2.2
03.06.04E 03.06.03E 03.06.02aE 03.06.01E 03.06.00E	03.06.04E 03.06.02aE 03.06.01E 03.06.00E	8.0 8.0.x 7.6	8.0 8.0[1]	1.3 1.3 1.3 1.2	5.2 5.3	2.2 2.2 2.2 2.1.2 or 2.1.1 if MSE is also deployed[2] 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	7.6[3] 7.5[4]	7.6 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. Therefore, we recommend that you upgrade to MSE 8.0.

[2] If MSE is deployed on your network, we recommend that you upgrade to Cisco Prime Infrastructure 2.1.2.

[3] Cisco WLC Release 7.6 is not compatible with Cisco Prime Infrastructure 2.0.

[4] Prime Infrastructure 2.0 enables you to manage Cisco WLC c7.5.102.0 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*.

Wired Web UI (Device Manager) System Requirements

Hardware Requirements

Table 8 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1024 x 768	Small

[1] We recommend 1 GHz.

[2] We recommend 1 GB DRAM.

Software Requirements

- Windows 7, Windows Vista, Windows XP, Windows 2003, or Windows 2000
- Microsoft Internet Explorer 6.0 and 7.0, and Mozilla Firefox up to version 26.0, with JavaScript enabled.

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

Finding the Software Version and Feature Set

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
03.06.08E	15.2(2)E8	10.2.180.0	15.3(3)JN13
03.06.07E	15.2(2)E7	10.2.170.0	15.3(3)JN12

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
03.06.06E	15.2(2)E6	10.2.160.0	15.3(3)JN11
03.06.05E	15.2(2)E5	10.2.150.0	15.3(3)JN9
03.06.04E	15.2(2)E4	10.2.140.0	15.3(3)JN8
03.06.03E	15.2(2)E3	10.2.131.0	15.3(3)JN7
03.06.2E	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)JB5
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

The package files for the Cisco IOS XE software are stored on the system board flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch.

Note Although the **show version** output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration and does not change if you upgrade the software license.

You can also use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Upgrading the Switch Software

For information about how to upgrade the switch software, see the *System Management Configuration Guide, Cisco IOS XE Release 3E (Catalyst 3650 Switches)* at the following URL:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/software/release/3e/system_management/configuration_guide/b_sm_3e_3650_cg.html

Table 10 Software Images

Image	File Name
Universal	cat3k_caa-universalk9.SPA.03.06.00.E.152-2.E.bin
Universal without DTLS	cat3k_caa-universalk9ldpe.SPA.03.06.00.E.152-2.E.bin

Important Upgrade Note

After you upgrade to Cisco IOS XE Release 3.6E, 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 > Switches > Campus LAN Switches - Access > Cisco Catalyst 3650 Series Switches**.

Step 3 Click a switch model.

Step 4 Click **Wireless Lan Controller Web Authentication Bundle**.

Step 5 Choose Release 3.6.0 and click **Download**.

Step 6 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.

Note When you upgrade to Cisco IOS XE Release 3.6.5E the SSH access is lost, because it cannot use the CISCO_IDEVID_SUDI_LEGACY RSA server key. Before upgrade, generate the server key using the **crypto key generate rsa** command in global configuration mode.
To verify whether the RSA server key is available on your device, run the **show crypto key** command.

Features

The Catalyst 3650 switch supports three different feature sets:

- LAN Base feature set—Provides basic Layer 2+ features, including access control lists (ACLs) and quality of service (QoS) and up to 4094 VLANs.
- IP Base feature set—Provides Layer 2+ and basic Layer 3 features (enterprise-class intelligent services). These features include access control lists (ACLs), quality of service (QoS), ACLs, QoS, static routing, EIGRP stub routing, IP multicast routing, Routing Information Protocol (RIP), basic IPv6 management, the Open Shortest Path First (OSPF) Protocol, and support for wireless controller functionality.
- IP Services feature set—Provides a richer set of enterprise-class intelligent services and full IPv6 support. It includes IP Base features plus Layer 3 routing (IP unicast routing and IP multicast routing). The IP Services feature set includes protocols such as the Enhanced Interior Gateway Routing Protocol (EIGRP), the Open Shortest Path First (OSPF) Protocol, and support for wireless controller functionality.

Note A separate access point count license is required to use the switch as a wireless controller.

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

http://www.cisco.com/en/US/products/ps13133/products_data_sheets_list.html

Interoperability with Other Client Devices

This section describes the interoperability of this version of the switch 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

Table 11 Client Types (continued)

Client Type and Name	Version
Engenius EUB 1200AC(USB)	1026.5.1118.2013
Intel 1000/1030	v14.3.0.6
Intel 4965	v13.4
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

Table 11 Client Types (continued)

Client Type and Name	Version
Cisco 7921G	1.4.5.3.LOADS
Cisco 7925G	1.4.5.3.LOADS
Cisco 8861	Sip88xx.10-2-1-16
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

- A switch stack containing a mix of Catalyst 3850 and Catalyst 3650 switches is not supported.
- With Cisco Prime Infrastructure 2.1.1, the refresh config and inventory collection tasks from the switch might take anywhere from 20 minutes to 40 minutes. For more information, see CSCum62747 on the Bug Search Tool.
- Sometimes a delay is seen in the handling of ICMP reply packets when the packet timer is set to milliseconds (if the value is under 1 second). This is an expected behavior.
- Although visible in the CLI, the following commands are not supported:
  - **collect flow username**
  - **authorize-lsc-ap** (CSCui93659)
- Catalyst 3650 switch supports IEEE 802.3ae standard.
- The following features are not supported in Cisco IOS XE Release 3.6E:
  - Outdoor Access Points
  - Mesh, FlexConnect, and OfficeExtend access point deployment

- Wireless Guest Anchor Controller (The Catalyst 3850 switch can be configured as a foreign controller.)
- Resilient Ethernet Protocol
- Private VLANs
- MVR (Multicast VLAN Registration)
- IPv6 routing - OSPFv3 Authentication
- Call Home
- DVMRP Tunneling
- Port Security on EtherChannel
- 802.1x Configurable username and password for MAB
- Link State Tracking (L2 Trunk Failover)
- Disable Per VLAN MAC Learning
- IEEE 802.1X-2010 with 802.1AE support
- IEEE 802.1AE MACsec (MKA & SAP)
- Command Switch Redundancy
- CNS Config Agent
- Dynamic Access Ports
- IPv6 Ready Logo phase II - Host
- IPv6 IKEv2 / IPSecv3
- OSPFv3 Graceful Restart (RFC 5187)
- Fallback bridging for non-IP traffic between VLANs
- DHCP snooping ASCII circuit ID
- Protocol Storm Protection
- 802.1x NEAT
- Per VLAN Policy & Per Port Policer
- Packet Based Storm Control
- Ingress/egress Shared Queues
- Trust Boundary Configuration
- Cisco Group Management Protocol (CGMP)
- Device classifier for ASP
- IPSLA Media Operation
- Passive Monitoring
- Performance Monitor (Phase 1)
- AAA: RADIUS over IPv6 transport
- AAA: TACACS over IPv6 Transport
- Auto QoS for Video endpoints
- EX SFP Support (GLC-EX-SMD)
- IPv6 Strict Host Mode Support

  - IPv6 Static Route support on LAN Base images
  - VACL Logging of access denied
  - RFC5460 DHCPv6 Bulk Leasequery
  - DHCPv6 Relay Source Configuration
  - RFC 4293 IP-MIB (IPv6 only)
  - RFC 4292 IP-FORWARD-MIB (IPv6 only)
  - RFC4292/RFC4293 MIBs for IPv6 traffic
  - Layer 2 Tunneling Protocol Enhancements
  - UniDirectional Link Routing (UDLR)
  - Pragmatic General Multicast (PGM)
  - PVLAN, DAI, IPSG Interoperability
  - Ingress Rate Limiting
  - Ingress Strict Priority Queuing (Expedite)
  - Weighted Random Early Detect (WRED)
  - Improvements in QoS policing rates
  - Fast SSID support for guest access WLANs

- Be careful when connecting a “snagless” Ethernet cable to port 1 on a 48-port switch. The protective boot of the cable might inadvertently press the Mode button, causing the switch to erase its startup configuration and reboot. (CSCuj17317)

  There is no workaround except to avoid connecting a “snagless” Ethernet cable to port 1 on a 48-port switch.

Scaling Guidelines

Table 12 Scaling Guidelines

System Feature	Maximum Limit
Number of HTTP session redirections system-wide (wired/wireless)	Up to 100 clients per second
Number of HTTPS session redirections system-wide (wired/wireless)	Up to 20 clients per second

Limitations and Restrictions

Note **Device Classifier** has been disabled by default starting from Release 3.6.0E. Any features dependent on device classifier should enable it if required.

- You cannot configure NetFlow export using the Ethernet Management port (g0/0).
- The maximum committed information rate (CIR) for voice traffic on a wireless port is 132 Mb/sec.
- VRRPv3 for IPv4 and IPv6 is not supported.

- 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 switch supports up to 255 security group destination tags for enforcing security group ACLs.
- When a logging discriminator is configured and applied to a device, memory leak is seen under heavy syslog or debug output. The rate of the leak is dependent on the quantity of logs produced. In extreme cases, the device may crash. As a workaround, disable the logging discriminator on the device.
- The WEB UI home page may not load when **ip http access class** command is enabled. When you encounter this issue, we recommend that you do the following:
  a. Run the **show iosd liin** command.
  b. Get the internet-address and configure the same IP as permit in the access-list.
- For WEB UI access using TACACS server, the custom method-list for authentication and authorization pointing to the TACACS server group does not work. You should 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 into a secondary flash during a crash when there is no available space in the main memory area to store the crash information.
- For routing protocols, when aggressive hello timer is configured, a timely delivery of control packets is not guaranteed. Do not configure timers shorter than 3 seconds for Hello interval and shorter than 9 seconds for Dead interval, across the protocols. If there is a requirement to use aggressive timers of 1 and 3 seconds for Hello and Dead interval respectively, the recommendation is to upgrade to Cisco IOS XE Denali 16.3 release or later.
- 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.
- With port-security configured on a port, switch may consume very first few frames that would be required to install newly learned or a re-learned MAC address in to the hardware. Those frames are not forwarded further to the network.

Caveats

Cisco Bug Search Tool

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

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

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

Open Caveats

Bug ID	Headline
CSCvc36982	3850-4K Interop: CTS/SAP links stuck in SAP_NE after cat4K VSS switchover.
CSCvc37207	3850 rtc time cannot update after power off/on the switch.

Resolved Caveats in Cisco IOS XE Release 3.6.10E

Bug ID	Headline
CSCvn72973	Device is getting crashed on the "cts role-based enforcement"

Resolved Caveats in Cisco IOS XE Release 3.6.9E

Bug ID	Headline
CSCvd46008	Cisco Catalyst 3650 and 3850 Series Switches suddenly stops providing PoE on certain ports
CSCvb59372	Double-free of VTY context causes a software-forced crash
CSCvd78456	Span config lost after reboot when using interface ranges
CSCvd96099	DOT1X %DATACORRUPTION-1-DATAINCONSISTENCY: copy error session_mgr

Bug ID	Headline
CSCvg79459	Automate-tester does not send probes when the server is dead
CSCvh89534	DACL applied to the incorrect interface.
CSCvj25236	IPDT flapping after upgrade
CSCvj29126	RADIUS client on network fails to solicit PAC key from CTS even though the device has a valid PAC

Resolved Caveats in Cisco IOS XE Release 3.6.8E

Bug ID	Headline
CSCur34138	Memory leak Process= NGWC SPI Async Response.
CSCvc47165	SFP port detect link-flap error and it's in error-disabled state on 3650.
CSCvd18991	Crash after RTU checksum is interrupted by script running CMDs.
CSCve14087	Nyquist: SGACL CoA fails if change made at ACE level.
CSCve37498	Switch sends duplicate accounting message, that causing ISE to generate Misconfigured NAS Alarms.
CSCve40391	GLC-GE-100FX link up as half for some time even with duplex full configuration after 3850 reload.
CSCve54486	Crash when attempting to assign nonexistent/shutdown VLAN to 802.1x port.
CSCvf07049	Bonjour/mDNS Traffic Routed without presence of Bonjour Gateway.
CSCve73570	If Descr cannot get StackSub interface information.
CSCvf50867	Controller port error Interface.
CSCvf58510	Finistar GLC-T is recognizable by C3650 but not transmitting or receiving data.
CSCvf61452	Spanning moves native vlan to inconsistent state.
CSCvf18046	sticky timer stops if connected device moved from one port to other within timer expiry.
CSCvf76512	Option 82 circuit-id-tag restricted by 6 bytes.
CSCvf91392	Catalyst switch crashes when editing wireless controller settings through web interface on c3650.
CSCvg75638	Switch reloads with SESA error code 7.

Resolved Caveats in Cisco IOS XE Release 3.6.7bE

Bug ID	Headline
CSCvf59705	ARP packets dropped silently on 3850
CSCvg42682	Key Reinstallation attacks against WPA protocol

Resolved Caveats in Cisco IOS XE Release 3.6.7E

Bug ID	Headline
CSCty18171	SNMP poll of CISCO-PROCESS-MIB may cause high CPU and SNMP poll timeout.
CSCuv22571	Memory corruption crash in slaJitterPacketBuild.
CSCuw15256	IOS PKI: Certificate validation fails after reload.
CSCvc38028	Packet loss seen after 2 mins from the time SSO is performed.
CSCvc44866	3850/3650 - ssh/vty sessions lock up leading to loss of access to device.
CSCvc51344	Few connected CISCO PD Ip Phones are not coming up after switch reload
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.
CSCvd17624	Packet drop due to IGR_MISC_FATAL_ERROR exception.
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 in Cisco IOS XE Release 3.6.6E

Bug ID	Headline
CSCun71347	Cisco Catalyst 3850 reloads unexpectedly in CEF: IPv4 process while processing ARP throttle elements.
CSCus79635	Wireshark file location flash:/usbflash0: does not capture.
CSCus83638	5-GHz radio on Cisco AP beaconing but not accepting client associations
CSCuu11760	Converged Access-QoS: Need to block priority percent command in policy-map.
CSCuu99371	Burst of syslogs may end up truncated.
CSCuv65173	Scrubs Delta FEP supply not responding in slot B.
CSCux14199	Error “Command rejected: Bad VLAN list” when default interface configuration is used.
CSCux14425	ACL matching IP option is not working with the **no ip unreachables** command.
CSCuy92908	Add inline power outputs to the **show tech** output.
CSCuy96474	Cisco Catalyst 3650 platform manager reloads unexpectedly after config-sync failure.
CSCuy97043	Remove invalid data cefcModuleAdminStatus MIB from Cisco Catalyst 3650 and 3850 platforms.
CSCuy99672	The switch system LED does not change to green after replacing the FAN.
CSCuz02766	IOSd reloads unexpectedly running 'EPC SM Liaison Update proc'.
CSCuz14485	Output rate is different from input rate on Cisco Catalyst 3650 and 3850 management port.

Bug ID	Headline
CSCuz24063	Storm-control configured on port-channel cannot reflect to member link.
CSCuz28295	TCN generate late and MAC learn issue on Cisco Catalyst 3650 stack after RSTP TCN.
CSCuz29721	Memory leak under HTTP EPM Redirect Daemon.
CSCuz30314	Memory leak in DSensor Cache PROTO and epm authz_sess_info.
CSCuz48450	Cisco Catalyst 3650 802.1x different behavior in IOS XE Release 3.6.0/3.6.3.
CSCuz48487	Cisco Catalyst 3850 drops MacSec traffic.
CSCuz57493	High CPU observed in punjectrx fed-ots-main thread.
CSCuz60141	SDP drops causing stack issues.
CSCuz61004	EMM script event mat MAC-address is not working on version 3.6.4.
CSCuz63194	Remove switchport block unicast from ASP Macro for IP Phones.
CSCuz69805	ACL deny counter does not match on Cisco Catalyst 3850 when use HSRP VIP as gateway.
CSCuz71966	speed auto 10 100 disappeared from the output of the **show running-config** command after reload.
CSCuz83883	IPv6 neighbor discovery packet (NDP) processing behavior.
CSCuz86625	Need CLI to tune buffers on egress port without service policy.
CSCuz87489	No crash info generated since core resource was not set.
CSCuz89095	Cisco Catalyst 3850 switch at provisioned state after a random reload/power outage.
CSCuz94722	MacSec link not encrypting traffic in half duplex.
CSCuz98374	Cisco Catalyst 3850 incorrectly set more-fragment flag for double fragmentation.
CSCva02227	Cisco Catalyst 3850s in stack do not return ports 45-48 when polled through SNMP.
CSCva08676	LED of backup port still shows amber after deleting flex link configuration.
CSCva09951	MAC address-table static H.H.H vlan xx drop command not work on Cisco Catalyst 3850.
CSCva17430	Media services proxy process reloads unexpectedly.
CSCva21500	Cisco Catalyst 3650 interface does not come up when speed nonegotiate is applied.
CSCva22352	Switch delete fails to complete after memory exhaustion.
CSCva22373	Impacting stack-manager events should be printed as a syslog.
CSCva22423	LACP rate fast unbundle due to aggressive timer.
CSCva22528	Cisco Catalyst 3850: traffic only flowing between ports on port ASIC.
CSCva34598	Down change delay expired of track, without counting delay down time.
CSCva37063	Improve the script that logs the last-reload reason when Cisco Catalyst 3850 reloads.
CSCva40478	IP DHCP snooping trust on port-channel does not reflect on member link.
CSCva43372	Interoperability - remote side CRC error.
CSCva46457	Cisco Catalyst 3850 stack reloads unexpectedly with static MAC-address maped to multiple port-channel.
CSCva47779	Cisco Catalyst 3850 IP source guard drops legitimate user traffic.
CSCva48042	SNMP Trap cefcFRU is not sent when fan module is removed and inserted.

Bug ID	Headline
CSCva48826	The **show udld neighbors** command should show empty for GLC-T ports.
CSCva59493	Cisco Catalyst 3650 returning incorrect OID sysObjectID for NAC.
CSCva61347	Multicast packets can not be forwarded after power off/on the master SW.
CSCva65105	Cisco Catalyst 3650 stack: specific VLAN down when switchover.
CSCva69778	Cisco Catalyst 3850: wrong temperature syslog OVERTEMP severity level.
CSCva71899	Cisco Catalyst 3650: Ports reporting Power Good wait timer timed out.
CSCva79547	Zero Rx counters and total traffic loss on te1/1/3 port.
CSCva81608	Cisco Catalyst 3850: Egress QoS policies are failing to get installed in hardware.
CSCva87959	Device reloads unexpectedly due to IP Source Guard during VLAN ID from L3 key lookup.
CSCva92074	%PLATFORM_PM-6-MODULE_ERRDISABLE output when inserting SFP.
CSCva93962	Cisco Catalyst 3650, 3850 WCCP redirect-list do not work using range ACL.
CSCvb19326	NTP leap second addition is not working during leap second event.
CSCvb22505	Port security MAC address not aging out when relearned from a channel.
CSCvb26637	IGMPv2 leave messages sent back to ingress interface.
CSCvb30709	Display relevant registers in PoE in test command.
CSCvb45547	Cisco Catalyst 3850 stack with FSPAN configuration, when ACL is added fed reloads unexpectedly.
CSCvb48311	Installer process hangs while executing compatibility checks.
CSCvb52653	Memory corruption occurs on stack failure.
CSCvb60207	Span destination do not capture all packets on Cisco Catalyst 3650.
CSCvb69066	The traffic not passing on the interface with GLC-GE-100FX on Cisco Catalyst 3650 on code 3.6.5.
CSCvb73327	The **show platform software ilpower details** command shows only first switch's interfaces detail
CSCvb95864	Buffer allocations are incorrect after configuring softmax multiplier.
CSCvc12067	The **duplex auto** command displayed in the output of the **show running-config** command.

Resolved Caveats for Cisco IOS XE Release 3.6.5bE

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

Resolved Caveats in Cisco IOS XE Release 3.6.5E

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 coredump
CSCuu86712	FED Process Traceback @al_lookup_add_generic_entry while enabling IPSG
CSCuv02254	Logging message of FAN OIR is not displayed on 3650.
CSCuv08570	Lightweight access point loses all config at times after power cycle
CSCuv18572	Suppress extra "power supply [X] is not responding" messages
CSCuv50017	Airties WGB not getting Ip address when connecting to 5760
CSCuv62540	Adding -S domain support for Hong Kong, Macau, Thailand and Veitnam
CSCuv73422	IOS-UX AP:NDP propagation for US country uses UX domain
CSCuw02650	Ping packet loss (20~27s) during a switch add into stack
CSCuw16591	VACL in Cat3850 is dropping traffic that should be permitted
CSCuw38988	C3850: show interface transceiver slow in response, console/VTY may hang
CSCuw57588	C3600 AP crash on am_xml_GetChildCount
CSCuw78795	NGWC REPLAY_ERR msg showing WLAN ID as VLAN ID of the AP
CSCux64558	Inline power stops being provided on the port in err-disabled state.
CSCux65356	NGWC AP join failure due to ap_index out of sync between IOS and FED
CSCux71386	After clear counters is issued, the Xmit-err shows a very huge number
CSCux77360	Cat3650-24TS-S connection issue with FUJITSU switch SR-S324TL2
CSCux99191	Trunk link flaps when protected by MACsec and native VLAN is configured
CSCuy01628	NGWC ssid output qos shaper could drop capwap fragments
CSCuy19990	IOS 15.2 802.1x critical vlan feature - reinitialize is not working
CSCuy29078	5760 WLC FED crash
CSCuy32255	"test cable-diagnostics tdr interface" reloads a 3850
CSCuy32363	NGWC MDNS leaking when roaming to foreign in L2 sticky-anchor
CSCuy33187	Need FCC B domain DFS support on Skyros/AP1600
CSCuy43392	5760 crash at snmp_subagent
CSCuy43459	Crash while polling module details
CSCuy44807	Switch crashes with Segmentation fault(11), Process = NGWC DOT1X Process
CSCuy46096	Uncabling SFP port up/up when "speed nonegotiate" configured
CSCuy81218	AP support of DFS detection in 100% transmission BW
CSCuy83302	Catalyst 3850 - Port-security may interfere with spantree bpdu guard
CSCuz06686	Port-channel no drops although member port drops on C3650/C3850
CSCuz16907	Inversion issue of "wireless broadcast vlan x" command
CSCuz21596	Catalyst 3850 Cannot get "unrouted VLAN" information

Bug ID	Headline
CSCuy19327	Template gets applied/removed continuously when we connect laptop
CSCux11452	Cat3850 crash when execute "no queue-limit" command
CSCur31055	Ten gig links gets err-disable after enable "UDLD enable" on 3850

Resolved Caveats in Cisco IOS XE Release 3.6.4E

Bug ID	Headline
CSCui42745	GUI/CLI access to Cisco Catalyst 3850 in spite of no “wireless mgmt-via-wirele
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 3850 without wireless enabled
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
CSCut87285	MAC address being learnt on an individual Port-channel member interface
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 dot1x 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 unexpected reload on “no network 0.0.0.0” with vnet configuration on intf
CSCuv26804	Iosd reloads unexpectedly with DHCP snooping enabled
CSCuv39850	Switch crashes @auth_mgr_show_method_status_list
CSCuv46710	Segmentation Fault in Auth Manager
CSCuv60764	Session timeout is not applied on CoA
CSCuv65116	SNMP: Cannot clear PST Config for aps associated to 5760
CSCuw01266	ffm crash when adding 3.3.5 to 3.6.3 stack

Bug ID	Headline
CSCuw12199	Sends management IP as called-station-id
CSCuw13827	Cisco 5760 WLC 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	Cisco 3850 Switch and Cisco 5760 WLC web GUI display only Home and Monitor options
CSCuw38233	Mobility tunnel between MA/MC drops when default egress policy is set to deny
CSCuw38902	Cisco 5760 WLC web GUI: 500 internal error on Cisco IOS XE 3.7.1SE
CSCuw39020	access-session vlan-assignment ignore-errors breaks dynamic vlan assign
CSCuw45473	CAPWAP AP not joining to Cisco 5760 using broadcast discovery request
CSCuw48448	NAPF-3-INVALID_RADIO_TYPE
CSCuw52729	Enabling auto qos 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 infrastucture SSID is not saved on reboot.
CSCuw82216	Catalyst3850: Upgrade in install mode corrupts the flash - EXT2-fs error.
CSCuw91099	HA unexpectedly reloads one after another
CSCuw93850	Cisco 3850 not able 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
CSCux28874	NGWC EAPOL M5 retransmissions does not increment replay counter
CSCux79913	The client column in the load-info command is incorrect
CSCuh10592	Sys Pwr and PoE Pwr remain GOOD even when Status is Disabled
CSCup76821	System fan 1 inserted/removed logs prompts continuously-fan 1 is removed
CSCuq61882	Warning: policy_in_attach (p1) is not empty
CSCur54635	Cat3850/SSH: Traceback and dummy watched message after switch deployment
CSCur62204	Improve debug-ability of the offload module
CSCur66937	SPAN replication does not retain DSCP marking
CSCus93445	Traceback with amur mr1 with CSR %ENT_API-4-NOPARENT: Parent physica
CSCut64208	IP CEF load-sharing algorithm original option not working on NG3K
CSCuu18029	3650/3850 May Experience RP Protocol Flaps with Aggressive Timers.
CSCuu56511	OutDiscards counter does not increment
CSCuv13351	MAC address is learned on RSPAN vlan after stack switchover
CSCuv20921	MAC address-table learning command should not be allowed for RSPAN vlan
CSCuv59145	Duplex is full one end and half on the other with speed nonegotiate
CSCuv60283	Linkdown occur when SFP OIR on the error-disable port.
CSCuv62794	MAC address doesn't update when flex-link switchover.
CSCuv78424	Unicast ARP packets are duplicated

Bug ID	Headline
CSCuv78597	Interoperability issue between CTS MACSec and Port-security
CSCuv83370	3650/3850 switch may reload after issuing a \"show tech-support\"
CSCuv96828	Cat3k SNMP ctspPeerPolicyUpdatedNotif notification is disabled.
CSCuw06439	3850 does not assign/remove SGT tag to ARP traffic
CSCuw08107	C3650 core in show process cpu history's last 72 hours output incomplete
CSCuw08386	3850 SFP send TX power even if SFP IF is shut down state
CSCuw11414	Crash while updating the external vlan database.
CSCuw14212	Stack merge issues for large stacks, double failure scenario in a stack.
CSCuw22050	Switch reports Power device detected when non device is connected
CSCuw23090	3650 trunk interface malfunction issue when \"speed nonegotiate\" applied
CSCuw36865	L2 switched traffic matched by L3 SVI VACL in the output direction
CSCuw46389	No Output for "show ip cef exact-route platform srcIp dstIp" on NG3K
CSCuw47981	RSPAN not working properly on C3650
CSCuw66770	udld err-disbale on remote device when reload 3650
CSCuw67734	entAliasMappingIdentifier broken on 03.07.02E
CSCuw68593	Copper link to media converter doesn't come up after fiber side PC reset
CSCuw91080	Cat3850 stack standby side span broken after reload the stack
CSCuw95074	3650 Packets with fragment offset bit hit wrong class-map
CSCuw97476	Q-in-Q configured on 3850 stack is not working appropriate
CSCux10319	Multiple stack members crash with ffm_link_is_to_same_target
CSCux16628	IPv6 traffic to FF02::2 and FF02::3 send to CPU without IPv6 enabled
CSCux19272	FED crash at fed_init_l3if_stats
CSCux22760	On reload, 1G SFP is connected/up on 3750x while 3850 is notconnect/down
CSCux28536	Interface stays in down state after link flap on the neighbor
CSCux32504	DHCP client in native vlan do not receive an ip address
CSCux40358	Pim Auto-rp information lost on device
CSCux51492	NGWC crashes in task fed-ots-nfl decoding v9 template
CSCux54732	NSF Takes 30s to Process after Reloading Stack Master.
CSCux56459	Stack reload due to double free (FREEFREE)
CSCut84793	NG3k standby switch reloads due to ISSU Incompatibility
CSCuu95853	CWS: Crash seen in sadb
CSCux77511	3850: Webauth not working when incorrect username/password entered
CSCuu85298	FIB/LFIB inconcistency after BGP flap
CSCuv07111	IOS and IOS-XE devices changing the next-hop on BGP route with own IP
CSCuu21448	ISIS Metric with Multiple instances using ciiCircLevelMetric OID
CSCuv00910	bgp afi1/safi1 and afi1/saf4 only peers in the same update-group
CSCuv16769	ISIS: Old path not deleted in Global RIB when new path is filtered out

Bug ID	Headline
CSCuv31135	Disable connected-check in one side only makes route as unreachable
CSCuv76906	"bfd" disappears after issuing "snmp-server host x.x.x.x ABC bfd"
CSCum41167	Importing multipath routes changes next-hop to 0.0.0.0 and traffic fails
CSCuj81067	Memory leak in crypto_create_pkcs7_msg
CSCuq36627	WAAS Express:Failed to create SSL session. (no available resources)
CSCuq46932	Crash on dhcpd_find_binding_by_hw
CSCur28336	Memory leak and possible crash when using a logging discriminator
CSCur45606	Logging discriminator does not work
CSCuw06202	Vstack Download-Config causes 4500 to become unresponsive
CSCuw73525	3650 DHCPv6 Guard does not block rogue DHCP server to provide IPv6 addr
CSCux38988	Redundancy config-sync failures mcl define interface range adds fifth,
CSCuo93205	Enable SSL Server Identity Check during SSL handshake

Resolved Caveats in Cisco IOS XE Release 3.6.3E

Bug ID	Headline
CSCui35423	DHCP bindings are not happening at first try
CSCul30895	Syslog messages not generated for BFD neighbor up/down events
CSCul73513	Clock is not matching between server-client after leap configuration
CSCum01456	Windows 8 clients do not authenticate with AES on autonomous APs.
CSCum17258	EPM_SESS_ERR: Error in activating feature (EPM ACL PLUG-IN)
CSCum65703	Inconsistency on config \"privilege\" commands as seen in running-config
CSCun12965	Lightweight AP should not send jumbo frame by default.
CSCun40727	%PLATFORM_PBR-3-UNSUPPORTED_RMAP: Route-map not supported
CSCun56310	The following error message is observed continuously in WLC message logs: “LWAPP-3-VENDOR_PLD_VALIDATE_ERR:”.
CSCun63989	Express setup logs (express_setup.debug) should include more details
CSCuo56388	Controller is printing the following message: “%MM-3-INVALID_PKT_RECVD: 1 wcm: Received an invalid packet”.
CSCuo59909	3850 stack: false PSECURE_VIOLATION message
CSCup66629	Traceback @psecure_platform_delete_all_addrs on executing neg events
CSCup73878	The show version command output shows unnecessary information.
CSCup77718	Need to have ap_mac and client_mac attributes in LWA URL.
CSCup81878	standby reload - Line by Line Sync fail while deleting dynamic NTP peer
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.

Bug ID	Headline
CSCuq53140	High cpu seen while sending IPV6 traffic
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.
CSCuq98818	Beni: EC with native vlan, UDLD, vlan not defined b/w Mingla and Katana
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.
CSCur09175	IPDT is turned on automatically even when dot1x configs are disabled
CSCur10397	The ap core-dump ip validation is wrong.
CSCur11439	Energywise Activitycheck power off phone with an active call
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.
CSCur58372	\"snmp-server enable traps syslog\" still in \"show run all\" after removal
CSCur59242	Crash due to tplus_client_stop_timer
CSCur60244	5760 webauth on mac filter failure fails on new mobility with 5500 WLC.
CSCur78836	AP forwards frame to STP Blocked interface.
CSCur86947	dummy mcast pkt is not sent out when hsrp mac is there in mac-table
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.
CSCus13476	CSR handled only one MACSec interface's authentication
CSCus13594	Slow in getting the DHCP address in the AP 2700.
CSCus13924	[Beni-E1]:Found Traceback & crash with identity configurations.
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
CSCus46844	802.1x 3650 Radius Response not picket up by AAA code
CSCus47009	Switch does not increment the \"Received on untrusted ports\" DHCP counter
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 5760.
CSCus73176	AIR-CT5760 running 03.03.05SE reboots without a crash file generated

Bug ID	Headline
CSCus73423	Back to back ping fails in L3 etherchannel with cts dot1x config
CSCus74073	MACsec causing blackhole
CSCus75480	XE:CMD to enable ExpressSetup after initial configuration has occurred
CSCus77477	NGWC Increase the number of URLs allowed in a DNS ACL in WLC.
CSCus79132	Dot1x authentication legacy behaviour broken
CSCus90426	Consistency b/w ciscoEnvMonSupplyStatusTable & entPhysicalTable Entry
CSCus91957	RogueAP trap from 5760 has invalid rogueAP/detectingAP macs.
CSCut02707	5760 3.7 crashing on memory allocation issue.
CSCut05808	UDP(1975) causes Error msg %IPC-2-INVALIDZONE: on 3750X
CSCut06428	backup flexlink with multicast fast-convergence is leaking igmp leave
CSCut10251	Some commands are not in running-config after AUTOINSTALL finishes
CSCut13064	BPDU filter not work on output port when disable STP
CSCut13753	ACL's not syncing to the member swithes on stack reload or member reload
CSCut20271	C3560X response ARP request from management port
CSCut26137	3702 - Voice Queue stuck, with no new clients able to associate.
CSCut27272	CPUHOG and crash due to Auth Manager process
CSCut27350	MA Load Balancing not working as expected.
CSCut30423	WLC 5760 fed crash.
CSCut50625	switch crash with dot1x traceback
CSCut50679	The following memory leak is observed: "tlv_calloc memory leak (QoS related code)".
CSCut68387	FED Memory corruption Crash due to CGM
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.
CSCut79680	ip default-gateway is not seen in running-config after AUTOINSTALL
CSCut80382	NGWC : FED crash
CSCut80510	The command show proc mem detailed process iosd maps is broken.
CSCut87425	CPU hog in \"EEM TCL Proc\" after TCL script termination with long runtime
CSCut89864	FED crash on 5760 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.
CSCut98110	3850: ARP ACL ace log restriction should be removed
CSCut98205	AIR-CT5760 lost configuration after upgrade/reboot.
CSCut98228	Edison: Enhancement for the buffer multiplier feature
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	WLC 5760 Random CLI hang and sometimes console lockup.

Bug ID	Headline
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.
CSCuu22144	Vlan1 IP apply method inconsistencies across Static / DHCP / TFTP
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
CSCuu34717	3850 cts enforcement for multicast traffic
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	5760 should not crash if LAP HA WLC IP address pointer is NULL.
CSCuu50589	Voice Clients Blacklisted due to %SPI-3-QOS_INSTALL_CLIENT_POLICY.
CSCuu56466	\"Total output drops\" counter of a certain ports does not increment
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	amur mr2:__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.
CSCuu69332	Frame with special DesMac is forwarded by STP block port
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.
CSCuu82134	IBC:VSS-Predator: Active Predator went SMI upgrade but not standby
CSCuu90639	IP address is missing by end of Autoinstall
CSCuu99792	WLAN Configuration is not applied due to “exceeds MAX_QUEUED_RECV_BUFS”.

Bug ID	Headline
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.
CSCuv14890	DHCPv6 solicit frame (IPv6 multicast) frame replication issues
CSCuv18572	Remove false-positive \"power supply [X] is not responding\" messages
CSCuv20618	3650 - Disabling Speed and Duplex or Auto MDIX Causes Link Down
CSCuv23751	NGWC: 'JP' should be used as world mode in Beacon/Probe Res
CSCuv23905	Sanity:-Client stuck in APPLYINGPOLICY/Authentication state
CSCuv45515	5760 crash in fed al_fnf_get_iif_fnf_info.
CSCuv69297	CLI hangs on certain show commands.
CSCuv69997	5760 crash due to APF-3-VALIDATE_DOT11i_CIPHERS_FAILED Errors.

Resolved Caveats in Cisco IOS XE Release 3.6.2aE

Bug ID	Headline
CSCul30533	The switch system LED does not change to green after inserting the fans
CSCun29064	The show switch details displays incorrect output.
CSCuo00561	Switch unusable for eight minutes after “default interface” with L3 CTS config
CSCup40892	Wireless clients may be stuck in idle state when FQDN feature is enabled
CSCup55828	Need error message when using a wrong image to do software install
CSCuq89605	Switch does not show the configured duplex value.
CSCur12236	6500 interface shows up/up although connected 3650 is down
CSCur20444	I/O memory leak due to DHCPv6 packets.
CSCur21080	SMI director does not support WS-C2960CX-8PC-L as client
CSCur25796	Phones on protected switch ports unable to communicate with each other.
CSCur48634	HA fails due to Bulk synch failure with encrypted password.
CSCur64098	Port policy gets uninstalled on FED if apply the multi-dest policers.
CSCur74702	Wrong SMI vStack group selected due to incorrect client MAC matched.
CSCur76332	EtherChannel Load Balancing with IP address displays false port number
CSCur86077	ciscoEnvMonTemperatureThreshold object reports Incorrect values
CSCus29565	Auth session is not cleared after the supplicant disconnects.
CSCus31640	Wireless client redirect not working for 3850 48-port when on port 1-24
CSCus75890	Switch does not resync to NTP server after clock set command or reload
CSCus97274	dACL Intermittently Fails to Attach to 802.1x interface

Bug ID	Headline
CSCut74201	3850 3560 upgrade fails from 3.6.2 to 3.6.2a in install mode
CSCut75225	some 3850 3650 may fail upgrade or boot 3.6.2

Resolved Caveats in Cisco IOS XE Release 3.6.1E

Bug ID	Headline
CSCur50946	APs manufactured in August/September/October 2014 unable to join an IOS-XE controller
CSCuq02810	STP check bypassed for data traffic sent to switch mac address
CSCum47115	EtherType 888e unicast can not pass 2960 with new releases
CSCun80959	Desg port on the RootBridge experienced block forward for 30 sec
CSCuq26920	3850/3650 Access-List not permitting ICMP Fragments
CSCup96299	IPv6 Multicast RIB entry refer to wrong distance
CSCuq10827	C3560X cHsrpGrpStandbyState is incorrect
CSCur00722	Hard Reset of the Active Sup cause switch to power cycle
CSCur03368	IOS-XE for Nova devices: GNU Bourne Shell \"Shellshock\" Vulnerability
CSCur28989	SSO Bulk-sync PRC Failure Due to configure exclude interface command

Resolved Caveats in Cisco IOS XE Release 3.6.0E

Bug ID	Headline
CSCuh89574	Catalyst 5760 software forced reload IOSD hap_sup_reset
CSCui69119	IPDT: rejected channel conf and standby failed to boot up
CSCuj17317	XE: Certain snagless cables may press on the mode button causing reload
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** > **Switches**. 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
- Catalyst 3650 switch documentation at this URL:

  http://www.cisco.com/go/cat3650_docs
- 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.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.