Release Notes for Cisco Wireless Controllers and Lightweight Access Points for Cisco Wireless Release 8.2.100.0

First Published: December 15, 2015

This release notes document describes what is new in Cisco Wireless Release 8.2.100.0, instructions to upgrade to this release, and open and resolved caveats for this release. Unless otherwise noted, in this document, all Cisco Wireless Controllers are referred to as Cisco WLCs, and all Cisco lightweight access points are referred to as access points or Cisco APs.

Note

For information specific to the Cisco Mobility Express solution, see “Cisco Mobility Express Solution Release Notes” section on page 53.
## Revision History

<table>
<thead>
<tr>
<th>Modification Date</th>
<th>Modification Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 29, 2018</td>
<td>• Features Not Supported on Cisco Virtual WLCs, page 35</td>
</tr>
<tr>
<td></td>
<td>• Modified information about FlexConnect central switching.</td>
</tr>
<tr>
<td>October 16, 2017</td>
<td>• Features Not Supported on Cisco Aironet 1830 and 1850 APs, page 36</td>
</tr>
<tr>
<td></td>
<td>• Added SIP snooping with FlexConnect in local switching mode</td>
</tr>
<tr>
<td>October 10, 2017</td>
<td>• Features Not Supported on Cisco Virtual WLCs, page 35</td>
</tr>
<tr>
<td></td>
<td>• Added Wired Guest and FlexConnect central switching.</td>
</tr>
<tr>
<td>November 22, 2016</td>
<td>• Features Not Supported on Cisco 2504 WLC, page 33</td>
</tr>
<tr>
<td></td>
<td>• Added: EoGRE</td>
</tr>
<tr>
<td></td>
<td>• Features Not Supported on Cisco Virtual WLCs, page 35</td>
</tr>
<tr>
<td></td>
<td>• Added: EoGRE (Supported in only local switching mode)</td>
</tr>
<tr>
<td>September 27, 2016</td>
<td>• What’s new in this Release</td>
</tr>
<tr>
<td></td>
<td>• Added: Removal of Support for Rx SOP from Mesh Backhaul, page 11</td>
</tr>
<tr>
<td>May 17, 2016</td>
<td>• L3 Interfaces for Tunneling Protocols, page 12</td>
</tr>
<tr>
<td></td>
<td>• Added note on feature tunnel support.</td>
</tr>
<tr>
<td></td>
<td>• Upgrading to Cisco WLC Software Release 8.2.100.0, page 21</td>
</tr>
<tr>
<td></td>
<td>• Added this statement: “If you upgrade from Release 8.0.110.0 to a later release, the config redundancy mobilitymac mac-addr command's setting is removed. You must manually reconfigure the mobility MAC address after the upgrade.”</td>
</tr>
<tr>
<td>April 22, 2016</td>
<td>• Features Not Supported on Cisco Virtual WLCs, page 35</td>
</tr>
<tr>
<td></td>
<td>• Added Lync SDN.</td>
</tr>
<tr>
<td>March 21, 2016</td>
<td>• Features Not Supported on Cisco 2504 WLC, page 33</td>
</tr>
<tr>
<td></td>
<td>• Added Application Visibility and Control (AVC) for FlexConnect centrally switched access points to the list of not supported features.</td>
</tr>
<tr>
<td>March 16, 2016</td>
<td>• What’s New in this Release, page 5</td>
</tr>
<tr>
<td></td>
<td>• Added a Note on Release 8.2 related interface restrictions</td>
</tr>
<tr>
<td>March 8, 2016</td>
<td>• Resolved Caveats, page 40</td>
</tr>
<tr>
<td></td>
<td>• Added CSCuw03323 to the Resolved Caveats list.</td>
</tr>
<tr>
<td>March 4, 2016</td>
<td>• Upgrading to Cisco WLC Software Release 8.2.100.0, page 21</td>
</tr>
<tr>
<td></td>
<td>• Documented CSCux75436 kernel route issue.</td>
</tr>
<tr>
<td>March 3, 2016</td>
<td>• Mobility Express Features, page 54</td>
</tr>
<tr>
<td></td>
<td>• Added information about Cisco CMX support.</td>
</tr>
<tr>
<td>March 2, 2016</td>
<td>• Upgrading to Cisco WLC Software Release 8.2.100.0, page 21</td>
</tr>
<tr>
<td></td>
<td>• Added a statement that Cisco Aironet 3600 Series APs cannot recognize the reload command.</td>
</tr>
</tbody>
</table>
Table 1  Revision History

<table>
<thead>
<tr>
<th>Modification Date</th>
<th>Modification Details</th>
</tr>
</thead>
</table>
| February 21, 2016 | - 2.4-GHz Mesh, page 10  
|                   | - Rephrased the statements made in this section. |
| February 18, 2016 | - Features Not Supported on Cisco Aironet 1830 and 1850 APs, page 36  
|                   | - Added Telnet to the list of unsupported features |

Cisco Wireless Controller and Cisco Lightweight Access Point Platforms

The section contains the following subsections:

- Supported Cisco Wireless Controller Platforms, page 3
- Supported Access Point Platforms, page 4
- Unsupported Cisco Wireless Controller Platforms, page 5

Supported Cisco Wireless Controller Platforms

The following Cisco WLC platforms are supported in this release:

- Cisco 2500 Series Wireless Controllers (Cisco 2504 Wireless Controller)
- Cisco 5500 Series Wireless Controllers (5508 and 5520 Wireless Controllers)
- Cisco Flex 7500 Series Wireless Controllers (Cisco Flex 7510 Wireless Controller)
- Cisco 8500 Series Wireless Controllers (8510 and 8540 Wireless Controllers)
- Cisco Virtual Wireless Controllers on the Cisco Services-Ready Engine (Cisco SRE) or the Cisco Wireless LAN Controller Module for Cisco Integrated Services Routers G2 (UCS-E)

Note  Kernel-based virtual machine (KVM) is supported in Cisco Wireless Release 8.1 and later releases.

After KVM is deployed, we recommend that you do not downgrade to a Cisco Wireless release that is earlier than Release 8.1.

- Cisco Wireless Controllers for High Availability for Cisco 2504 WLC, Cisco 5508 WLC, Cisco 5520 WLC, Cisco Wireless Services Module 2 (Cisco WiSM2), Cisco Flex 7510 WLC, Cisco 8510 WLC, and Cisco 8540 WLC.

Note  AP Stateful switchover (SSO) is not supported on Cisco 2504 WLCs.

- Cisco WiSM2 for Catalyst 6500 Series Switches
- Cisco Mobility Express Solution
For information about features that are not supported on the Cisco WLC platforms, see “Features Not Supported on Cisco WLC Platforms” section on page 33.

**Supported Access Point Platforms**

The following access point platforms are supported in this release:

- Cisco Aironet 1040 Series Access Points
- Cisco Aironet 1140 Series Access Points
- Cisco Aironet 1260 Series Access Points
- Cisco Aironet 1600 Series Access Points
- Cisco Aironet 1700 Series Access Points
- Cisco Aironet 1830 Series Access Points
- Cisco Aironet 1850 Series Access Points
- Cisco Aironet 2600 Series Access Points
- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 3500 Series Access Points
- Cisco Aironet 3600 Series Access Points
- Cisco Aironet 3700 Series Access Points
- Cisco Aironet 600 Series OfficeExtend Access Points
- Cisco Aironet 700 Series Access Points
- Cisco Aironet 700W Series Access Points
- Cisco AP802 Integrated Access Point
- Cisco AP803 Integrated Access Point
- Cisco ASA 5506W-AP702
- Cisco Aironet 1530 Series Access Points
- Cisco Aironet 1550 Series Access Points
- Cisco Aironet 1570 Series Access Points
- Cisco Industrial Wireless 3700 Series Access Points

**Note**  The Cisco 1040 Series, 1140 Series, and 1260 Series access points have feature parity with Cisco Wireless Release 8.0. Features introduced in Cisco Wireless Release 8.1 and later are not supported on these access points.

For information about features that are not supported on some access point platforms, see Features Not Supported on Access Point Platforms, page 36.

**Note**  Cisco AP802 is an integrated access point on the Cisco 800 Series Integrated Services Routers (ISRs). For more information about the stock-keeping units (SKUs) for the AP802s and the Cisco ISRs, see the following data sheets:

- AP860:
What's New in this Release

- AP880:

- AP890:

Before you use a Cisco AP802 series lightweight access point with Cisco Wireless Release 8.2.100.0, you must upgrade the software in the Cisco 880 Series ISRs to Cisco IOS 15.1(4)M or later releases.

Unsupported Cisco Wireless Controller Platforms

The following Cisco Wireless Controller platforms are not supported:

- Cisco 4400 Series Wireless LAN Controller
- Cisco 2100 Series Wireless LAN Controller
- Cisco Catalyst 3750G Integrated Wireless LAN Controller
- Cisco Wireless Controller software for Cisco SRE Internal Services Module (ISM) 300, Cisco SRE Service Module (SM) 700, Cisco SRE Service Module (SM) 710, Cisco SRE Service Module (SM) 900, and Cisco SRE Service Module (SM) 910.
- Cisco Catalyst 6500 Series and 7600 Series WiSM
- Cisco Wireless LAN Controller Module (NM/NME)

What's New in this Release

- Cisco Smart Software Licensing, page 6
- Increased AP and Client Scale for Cisco Virtual Wireless Controller, page 7
- Access Point Provisioning using Plug-n-Play (PnP), page 7
- NetFlow Export 2.0, page 7
- AVC Enhancements, page 8
- Bonjour Gateway with Googlecast Support, page 8
- Enhanced wIPS Support for Hyperlocation Module with Advanced Security, page 8
- Cisco Air Time Fairness: Client Fair Sharing, page 9
- Cisco WLAN Express Enhancements, page 9
What's New in this Release

- 2.4-GHz Mesh, page 10
- Removal of Support for Rx SOP from Mesh Backhaul, page 11
- Pre-Shared Key Provisioning Support for Mesh Networks, page 11
- Dynamic Management User Login via AAA Server, page 11
- Test AAA Command for RADIUS, page 11
- Custom HTTP Port for Profiling, page 12
- L3 Interfaces for Tunneling Protocols, page 12
- Cisco 5520, 8510, and 8540 WLC Updates, page 12
- Support for Wi-Fi Certified Passpoint Release 2.0, page 12
- Bonjour Gateway on Cisco 2504 WLC, page 13
- Increased Channel and Tx Power Support for Various Countries, page 13
- Increased Country Code Support, page 14
- Security Update, page 15
- QoS Mapping, page 15
- Cisco Industrial Wireless 3702 Access Point Updates, page 15

Note
For information specific to the Cisco Mobility Express solution, see “Cisco Mobility Express Solution Release Notes” section on page 53.

Note
Release 8.2 does not support multiple non-AP Manager dynamic interfaces, untagged management interfaces, management interfaces mapped to physical ports, and non-LAG scenarios.

Cisco Smart Software Licensing

Cisco started the initiative of simplifying customer license management by building a Cisco Smart Software Manager portal. It helps the customers understand what licenses they have purchased and what licenses they are using. Various other Cisco products are already Smart Enabled and with the introduction of this release Cisco Smart Software Licensing will now be available on the following platforms:

- Cisco 5520 WLC (AIR-CT5520-K9)
- Cisco 8540 WLC (AIR-CT8540-K9)
- Cisco vWLC (L-AIR-CTVM-5-K9)

For more information, see the following:

- Cisco Smart Software Licensing Overview
- Cisco Smart Software Licensing section in the Cisco Wireless Controller Configuration Guide.
Increased AP and Client Scale for Cisco Virtual Wireless Controller

The capacity of Cisco Virtual Wireless Controllers (vWLCs) is increased with the introduction of a Large Scale vWLC.

Two new SKUs with two types of scaling configurations are available. During installation or upgrade, you can choose between Small Scale vWLC and Large Scale vWLC.

This table lists the two types of Cisco vWLCs, their requirements and capacity:

<table>
<thead>
<tr>
<th>vWLC Type</th>
<th>Virtual CPU</th>
<th>Memory</th>
<th>Number of APs Supported</th>
<th>Number of Clients Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small Scale vWLC</td>
<td>1</td>
<td>2 GB</td>
<td>200</td>
<td>6000</td>
</tr>
<tr>
<td>Large Scale vWLC</td>
<td>2</td>
<td>8 GB</td>
<td>3000</td>
<td>32000</td>
</tr>
</tbody>
</table>

Access Point Provisioning using Plug-n-Play (PnP)

The Access Point Provisioning using Plug-n-Play (AP PnP) solution provides staging parameters to an AP before it is associated with a Cisco WLC. Using this staging configuration, the AP gets the run-time configuration when it associates with a Cisco WLC. PnP is supported only on AP recovery images and is activated only for the zero-day deployment. PnP can no longer be initiated after the AP associates with a Cisco WLC for the first time.

The following AP scenario is supported:
- On-premise redirection—Customers hosting the PnP server in their network

The AP PnP solution is supported on the following APs:
- Cisco 702i AP
- Cisco 702W Series APs
- Cisco Aironet 1600 Series APs
- Cisco Aironet 1700 Series APs
- Cisco Aironet 2600 Series APs
- Cisco Aironet 2700 Series APs
- Cisco Aironet 3600 Series APs
- Cisco Aironet 3700 Series APs

NetFlow Export 2.0

The following are the template enhancements in NetFlow Version 9:
- New features can be added to NetFlow quickly, without breaking existing implementations.
- NetFlow is future-proofed against new or developing protocols, because NetFlow Version 9 can be adapted to provide support for those protocols.
- NetFlow Version 9 is the IETF standard mechanism for information export.
- Third-party business partners who produce applications that provide collector or display services for NetFlow are not required to recompile their applications each time a new NetFlow feature is added.
What's New in this Release

For more information, see the Configuring NetFlow section in the Cisco Wireless Controller Configuration Guide.

AVC Enhancements

In Release 8.2, the following features are available on Cisco WLCs:

- Protocol Pack 14.0
- NBAR Engine Release 3.16(23)

Features

- Faster upgrade and downgrade process—Downgrading from Release 8.2 to Release 8.1 changes the protocol pack to the previously installed protocol pack version, which is Protocol Pack 11.0.
- Traffic is classified instantly upon Cisco WLC bootup.
- Support for 1536 applications.

Note

Newer protocol packs are tied with Network-Based Application Recognition (NBAR) Engine Version 14 and later. Protocol packs that are earlier than Version 14 do not work with the new engine.

For more information, see the Release Notes for NBAR2 Protocol Pack 14.0.0 for Cisco Wireless Controllers.

Bonjour Gateway with Googlecast Support

Googlecast Service that uses the service key, _googlecast._tcp.local, is supported on the existing implementation of Bonjour gateway on Cisco WLC.

Enhanced wIPS Support for Hyperlocation Module with Advanced Security

wIPS support for the 40 MHz to 80 MHz range using Hyperlocation module is introduced. This feature detects alarms in the 40 MHz to 80 MHz range (if RRM channel scanning is selected) and provides information to Cisco Prime Infrastructure (PI). Channel width information is derived from the packet data rate and sent to the wIPS module, which stores channel width per alarm. Using the show capwap am alarm alarm-id command, you can view the channel width in which the attack has occurred.

The wIPS alarm report contains the channel width of the attack and device capability (802.11a/b/g/n/ac). No wIPS-specific configuration is required to enable this feature. The only prerequisite is that RRM scanning must be enabled for this feature to work as expected.
Cisco Air Time Fairness: Client Fair Sharing

In Release 8.2, Cisco Air Time Fairness can be enforced on clients that are associated with an SSID/WLAN. This ensures that all clients within an SSID/WLAN are treated equally based on their utilization of the radio air time. This feature is useful in scenarios where one or a few clients could use the total air time available for an SSID/WLAN, thereby depriving Wi-Fi experience for other clients associated with the same SSID/WLAN.

For more information, see the Cisco Air Time Fairness section in the Cisco Wireless Controller Configuration Guide.

Cisco WLAN Express Enhancements

- New best practices added in Release 8.2. For details, see the “Complete List of Best Practices in Release 8.2” section on page 9.
- You have the option to ignore a recommended best practice by clicking the Ignore button. The Ignore button is visible (only for some best practices) when you click the + icon to select a recommended best practice. These best practices are added to the ignored list.
- The best practices information displayed when you click the Learn More button is integrated with the Cisco WLC software. The Learn More button is visible (only for some best practices) when you click the + icon to select a recommended best practice. Previously, this document was accessible on Cisco.com.
- Updates have been made to the Main Dashboard with the addition of new dashlets. For more information, see the Cisco Wireless Controller Online Help.

Complete List of Best Practices in Release 8.2

<table>
<thead>
<tr>
<th>Note</th>
<th>The best practices introduced in Release 8.2 are listed below in bold.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure</td>
<td></td>
</tr>
<tr>
<td>- AVC Visibility</td>
<td></td>
</tr>
<tr>
<td>- Band Select</td>
<td></td>
</tr>
<tr>
<td>- Controller High Availability</td>
<td></td>
</tr>
<tr>
<td>- Disable Aironet IE</td>
<td></td>
</tr>
<tr>
<td>- Disable Internal DHCP</td>
<td></td>
</tr>
<tr>
<td>- Disable Management over Wireless</td>
<td></td>
</tr>
<tr>
<td>- Fast SSID</td>
<td></td>
</tr>
<tr>
<td>- HTTPS for Management</td>
<td></td>
</tr>
<tr>
<td>- Load Balancing</td>
<td></td>
</tr>
<tr>
<td>- Load Balancing Window</td>
<td></td>
</tr>
<tr>
<td>- Local Profiling</td>
<td></td>
</tr>
<tr>
<td>- mDNS Gateway</td>
<td></td>
</tr>
<tr>
<td>- Multicast Forwarding</td>
<td></td>
</tr>
</tbody>
</table>
**What's New in this Release**

- Multicast Mobility
- Multicast VLAN
- NTP
- Tagged Management VLAN
- Virtual Gateway IP
- WLAN not on Management VLAN

**Security**

- 802.1X on AP
- CPU ACLs
- Client Exclusion
- Legacy IDS
- Local Management Password Policies
- Min Rogue RSSI Threshold
- Peer to Peer
- Rogue Policies
- SSH/Telnet Access
- User Login Policies
- WLAN with 802.1X
- WLAN with WPA2 and AES Policy

**RF Management**

- Auto Coverage Hole Detection
- Auto Dynamic Channel Assignment
- Auto Transmit Power Control
- Best Channel Width
- CleanAir Detection
- Client Band Select
- DCA Cisco AP Load
- Event Driven RRM
- High SSID Counts
- Wi-Fi Interference

---

**Note**

The 40-MHz Channel Width best practice is not available in Release 8.2.

---

**2.4-GHz Mesh**

Mesh functionality in 2.4 GHz is supported on all APs that support Mesh.
In addition, while both 2.4 GHz and 5 GHz can be used outdoor across the globe, in Israel, only 2.4 GHz can be used outdoor. Therefore, a new regulatory domain, –I, and country code, IO, is introduced to support the use of 2.4 GHz as outdoor mesh backhaul on Cisco Aironet 1530 and 1570 APs.

Removal of Support for Rx SOP from Mesh Backhaul

From Cisco Wireless Release 8.2, the Rx SOP feature in bridge mode is not supported in the mesh backhaul 5-GHz interface to improve backhaul stability.

Pre-Shared Key Provisioning Support for Mesh Networks

Support is added for the pre-shared key (PSK) functionality that can be provisioned from Cisco WLC and can help make a controlled mesh deployment and enhance mesh access point (MAP) security beyond the currently used default cisco PSK.

With this new feature, MAPs, which are not preset yet with a valid PSK can connect to Cisco WLC using the default cisco PSK, during the provisioning window controlled by the Administrator. However, it will then receive a new PSK from the Cisco WLC, and from that point on, will only be able to connect with that PSK, and no longer with the default passphrase cisco.

⚠️ Caution

If you want to downgrade from Release 8.2 to an earlier release, we recommend that you change the security method to EAP and then perform the downgrade operation.

Dynamic Management User Login via AAA Server

Management users who are logged in when external servers are not available must reauthenticate when the external RADIUS servers are available. Failing to do so will lead to termination of the user session to prevent potential operational and security risks. When RADIUS servers are not available, management users are authenticated locally. After the RADIUS servers are back online, management users are prompted to log in again within a specific timeframe.

For more information, see the Setting up TACACS+ section in the Cisco Wireless Controller Configuration Guide.

Test AAA Command for RADIUS

To troubleshoot AAA RADIUS interactions for WLAN authentication, test aaa commands are introduced:

- Test AAA RADIUS interactions for WLAN authentication by entering this command:

  \[
  \text{test aaa radius username } \text{username password } \text{password wlan-id } \\text{wlan-id [apgroup apgroupname server-index server-index]}
  \]

  The test command sends an access request the RADIUS server for client authentication. Access request exchange takes place between Cisco WLC and the AAA server, and the registered RADIUS callback handles the response.
  
  The response includes authentication status, number of retries, and RADIUS attributes.

- View the RADIUS response to test the RADIUS request by entering this command:
What's New in this Release

```
test aaa show radius
```

For more information, see the Troubleshooting AAA RADIUS Interactions for WLAN Authentication section in the Cisco Wireless Controller Configuration Guide.

Custom HTTP Port for Profiling

WLC can now send HTTP user agent information to ISE for devices that use custom port (not only port 80).

L3 Interfaces for Tunneling Protocols

Prior to Release 8.2, the management IP address was used as the tunnel endpoint. Release 8.2 has allowed the specification of any L3 dynamic interface as a tunnel endpoint, other than the management interface, if need be.

**Note**

This feature currently supports EoGRE and PMIPv6 types of tunnels for mobility tunnel termination.

Cisco 5520, 8510, and 8540 WLC Updates

- Out-of-Band Management Support—Prior to Cisco Wireless Release 8.2, we recommended that you do not use the service port for continuous SNMP polling and management functions, except when the management interface of the Cisco WLC is unreachable. In Cisco Wireless Release 8.2, this restriction is removed.

In Release 8.2, the following are supported on the Cisco 5520, 8510, and 8540 WLCs:
- SNMP polling v2 and v3
- Syslog messaging towards external server
- Any form of file transfer, including FTP, TFTP, and SFTP, to/from external server
- HTTP and HTTPS access to Cisco WLC
- SSH and Telnet
- Local EAP is supported
- Wired Guest Access is supported

Support for Wi-Fi Certified Passpoint Release 2.0

In order to support Passpoint Release 2.0 certification, the technical specification of HotSpot 2.0 Release 2 has been implemented, which allows an end user, upon reaching a Passpoint 2.0 WLAN, to sign up online, on the fly, to that WLAN, in the case where no previously known or preferred WLANs were available to allow secure connection.

This is made possible by adding configuration capability to a Cisco WLC to allow clients to connect to an Online Sign-Up (OSU) server and obtain WPA2-Enterprise credentials to perform their subsequent authentication with the secure Passpoint 2.0 WLAN.
For more information, see the Configuring Mobile Concierge chapter in the Cisco Wireless Controller Configuration Guide.

**Bonjour Gateway on Cisco 2504 WLC**

Limited Bonjour gateway is supported on Cisco 2504 WLC with support for up to 200 instance services.

**Increased Channel and Tx Power Support for Various Countries**

To maximize the amount of channels supported and transmit power that is specified in the wireless regulations, the following changes are made in the regulatory domains:

<table>
<thead>
<tr>
<th>Domain Change</th>
<th>Country</th>
<th>AP Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>–E to –S</td>
<td>Thailand, Vietnam</td>
<td>Indoor and Outdoor</td>
<td></td>
</tr>
<tr>
<td>–C to –S</td>
<td>Macau</td>
<td>Indoor</td>
<td></td>
</tr>
<tr>
<td>–N to –S(^1)</td>
<td>Hong Kong</td>
<td>Outdoor</td>
<td></td>
</tr>
</tbody>
</table>

Table 3: Regulatory Domain Change

<table>
<thead>
<tr>
<th>Domain Change</th>
<th>Country</th>
<th>AP Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>–E to –S</td>
<td>Thailand, Vietnam</td>
<td>Indoor and Outdoor</td>
<td></td>
</tr>
<tr>
<td>–C to –S</td>
<td>Macau</td>
<td>Indoor</td>
<td></td>
</tr>
<tr>
<td>–N to –S(^1)</td>
<td>Hong Kong</td>
<td>Outdoor</td>
<td></td>
</tr>
</tbody>
</table>

1. –S APs will work with the lower Tx power; –N will continue to use the higher power

**Platforms Supported**

- Indoor
  - Cisco Aironet 3700 Series Access Points
  - Cisco Aironet 2700 Series Access Points
  - Cisco Aironet 1830 and 1850 Access Points
What's New in this Release

Note The 1830 and 1850 APs already support the domain change for Thailand and Vietnam. In Release 8.2, the APs support the domain change for Macau.

- Cisco Aironet 1700 Series Access Points
- Cisco Aironet 700i and 700w Access Points

• Outdoor
  - Cisco Aironet 1570 Series Access Points
  - Cisco Aironet 1530 Series Access Points

Universal PIDs Supported

• Indoor
  - Cisco Aironet 3700 Series Access Points
  - Cisco Aironet 2700 Series Access Points
  - Cisco Aironet 1830 and 1850 Access Points

Note Supports Macau changes from –C to –S domain.

- Cisco Aironet 700i and 700w Access Points

• Outdoor
  - Cisco Aironet 1530 Series Access Points

Legacy APs

• Changes made in Cisco WLC to support –S domain for Hong Kong, Macau, Thailand, and Vietnam.
• Changes made in Cisco WLC to support –I domain for Algeria
• Previously supported domains can continue to associate with Cisco WLC and be supported in addition to the new domain APs.

Upgrade and Downgrade Scenarios

• When you upgrade to Release 8.2, the regular SKU APs will continue to associate with the Cisco WLC and be operational with both the radios.
• If a Cisco WLC is downgraded from Release 8.2, the indoor APs deployed in Hong Kong, Thailand, Vietnam, and Macau with –S domain and APs deployed in Algeria with –I domain will continue to associate with Cisco WLCs. However, the 802.11a radio will not be operational.

Increased Country Code Support

In Release 8.2, you can configure up to 110 country codes per Cisco WLC. Prior to Release 8.2, you could configure up to 20 country codes per Cisco WLC.
Security Update

Support for Transport Layer Security (TLS) v1.2 is added in Release 8.2.
The following are supported for web authentication and WebAdmin based on the configuration:

- TLSv1.2
- TLSv1.0
- SSLv3
- SSLv2

Note

DTLSv1.2 for CAPWAP is not supported.

QoS Mapping

The QoS Mapping feature maintains the QoS policies in situations where appropriate QoS markings that match the application type are not marked by clients or applications. The administrator maps the differentiated services code point (DSCP) to user-priority values in a Cisco WLC, which in turn provides better experience to users while using certain applications, such as voice or video applications.

For more information, see the Configuring QoS Mapping section in the Cisco Wireless Controller Configuration Guide.

Cisco Industrial Wireless 3702 Access Point Updates

- Flexible Antenna Port Support—The Cisco IW 3702 AP model with external antennas can operate in the 2.4-GHz and 5.0-GHz band in one of two antenna band modes.
  In the single-band mode:
  - the 5-GHz radio uses antenna ports C and D, each with a single band antenna
  - the 2.4-GHz radio uses antenna ports A and B, each with a single band antenna
  In the dual-band mode, four dual-band antennas are used and both the radios share these antennas.

- Daisy chaining is supported (support introduced in Release 8.1.111.0)

Software Release Support for Access Points

Table 4 lists the Cisco WLC software releases that support specific Cisco access points. The First Support column lists the earliest Cisco WLC software release that supports the corresponding access point. For APs that are not supported in ongoing releases, the Last Support column lists the last release that supports the corresponding APs.

Note

Third-party antennas are not supported with Cisco indoor APs.
### Table 4  
**Software Support for Access Points**

<table>
<thead>
<tr>
<th>Access Points</th>
<th>First Support</th>
<th>Last Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>700 Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIR-CAP702I-x-K9</td>
<td>7.5.102.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-CAP702I-xK910</td>
<td>7.5.102.0</td>
<td>—</td>
</tr>
<tr>
<td>700W Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIR-CAP702Wx-K9</td>
<td>7.6.120.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-CAP702W-xK910</td>
<td>7.6.120.0</td>
<td>—</td>
</tr>
<tr>
<td>1000 Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIR-AP1010</td>
<td>3.0.100.0</td>
<td>4.2.209.0</td>
</tr>
<tr>
<td>AIR-AP1020</td>
<td>3.0.100.0</td>
<td>4.2.209.0</td>
</tr>
<tr>
<td>AIR-AP1030</td>
<td>3.0.100.0</td>
<td>4.2.209.0</td>
</tr>
<tr>
<td>Airespace AS1200</td>
<td>—</td>
<td>4.0</td>
</tr>
<tr>
<td>AIR-LAP1041N</td>
<td>7.0.98.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-LAP1042N</td>
<td>7.0.98.0</td>
<td>—</td>
</tr>
<tr>
<td>1100 Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIR-LAP1121</td>
<td>4.0.155.0</td>
<td>7.0.x</td>
</tr>
<tr>
<td>1130 Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIR-LAP1131</td>
<td>3.1.59.24</td>
<td>8.0.x</td>
</tr>
<tr>
<td>1140 Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIR-LAP1141N</td>
<td>5.2.157.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-LAP1142N</td>
<td>5.2.157.0</td>
<td>—</td>
</tr>
<tr>
<td>1220 Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIR-AP1220A</td>
<td>3.1.59.24</td>
<td>7.0.x</td>
</tr>
<tr>
<td>AIR-AP1220B</td>
<td>3.1.59.24</td>
<td>7.0.x</td>
</tr>
<tr>
<td>1230 Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIR-AP1230A</td>
<td>3.1.59.24</td>
<td>7.0.x</td>
</tr>
<tr>
<td>AIR-AP1230B</td>
<td>3.1.59.24</td>
<td>7.0.x</td>
</tr>
<tr>
<td>AIR-LAP1231G</td>
<td>3.1.59.24</td>
<td>7.0.x</td>
</tr>
<tr>
<td>AIR-LAP1232AG</td>
<td>3.1.59.24</td>
<td>7.0.x</td>
</tr>
<tr>
<td>1240 Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIR-LAP1242G</td>
<td>3.1.59.24</td>
<td>8.0.x</td>
</tr>
<tr>
<td>AIR-LAP1242AG</td>
<td>3.1.59.24</td>
<td>8.0.x</td>
</tr>
<tr>
<td>1250 Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIR-LAP1250</td>
<td>4.2.61.0</td>
<td>8.0.x</td>
</tr>
<tr>
<td>AIR-LAP1252G</td>
<td>4.2.61.0</td>
<td>8.0.x</td>
</tr>
<tr>
<td>AIR-LAP1252AG</td>
<td>4.2.61.0</td>
<td>8.0.x</td>
</tr>
<tr>
<td>1260 Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIR-LAP1261N</td>
<td>7.0.116.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-LAP1262N</td>
<td>7.0.98.0</td>
<td>—</td>
</tr>
<tr>
<td>1300 Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIR-BR1310G</td>
<td>4.0.155.0</td>
<td>7.0.x</td>
</tr>
<tr>
<td>1400 Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standalone Only</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>1600 Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIR-CAP1602I-x-K9</td>
<td>7.4.100.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-CAP1602I-xK910</td>
<td>7.4.100.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-SAP1602I-x-K9</td>
<td>7.4.100.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-SAP1602I-xK9-5</td>
<td>7.4.100.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-CAP1602E-x-K9</td>
<td>7.4.100.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-SAP1602E-xK9-5</td>
<td>7.4.100.0</td>
<td>—</td>
</tr>
<tr>
<td>Access Points</td>
<td>First Support</td>
<td>Last Support</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>1700 Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIR-CAP1702I-x-K9</td>
<td>8.0.100.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-CAP1702I-xK910</td>
<td>8.0.100.0</td>
<td>—</td>
</tr>
<tr>
<td>1830 Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIR-AP1832I-UXK9</td>
<td>8.1.120.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-AP1832I-x-K9</td>
<td>8.1.120.0</td>
<td>—</td>
</tr>
<tr>
<td>1850 Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIR-AP1852I-UXK9</td>
<td>8.1.111.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-AP1852I-UXK910</td>
<td>8.1.111.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-AP1852I-UXK9C</td>
<td>8.1.111.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-AP1852I-UXK910C</td>
<td>8.1.111.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-AP1852E-UXK9</td>
<td>8.1.111.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-AP1852E-UXK910</td>
<td>8.1.111.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-AP1852E-UXK9C</td>
<td>8.1.111.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-AP1852E-UXK910C</td>
<td>8.1.111.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-AP1852E-x-K9</td>
<td>8.1.111.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-AP1852E-x-K9C</td>
<td>8.1.111.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-AP1852E-x-K9C</td>
<td>8.1.111.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-AP1852I-x-K9</td>
<td>8.1.111.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-AP1852I-x-K9C</td>
<td>8.1.111.0</td>
<td>—</td>
</tr>
<tr>
<td>1800 Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AP801</td>
<td>—</td>
<td>5.1.151.0</td>
</tr>
<tr>
<td>AP802</td>
<td>—</td>
<td>7.0.98.0</td>
</tr>
<tr>
<td>AP802H</td>
<td>—</td>
<td>7.3.101.0</td>
</tr>
<tr>
<td>AP803</td>
<td>—</td>
<td>8.1.120.0</td>
</tr>
<tr>
<td>ASA5506W-AP702</td>
<td>—</td>
<td>8.1.120.0</td>
</tr>
<tr>
<td>2600 Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIR-CAP2602I-x-K9</td>
<td>7.2.110.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-CAP2602I-xK910</td>
<td>7.2.110.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-SAP2602I-x-K9</td>
<td>7.2.110.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-SAP2602I-x-K95</td>
<td>7.2.110.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-CAP2602E-x-K9</td>
<td>7.2.110.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-CAP2602E-xK910</td>
<td>7.2.110.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-SAP2602E-x-K9</td>
<td>7.2.110.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-SAP2602E-x-K95</td>
<td>7.2.110.0</td>
<td>—</td>
</tr>
<tr>
<td>2700 Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIR-CAP2702I-x-K9</td>
<td>7.6.120.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-CAP2702I-xK910</td>
<td>7.6.120.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-CAP2702E-x-K9</td>
<td>7.6.120.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-CAP2702E-xK910</td>
<td>7.6.120.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-AP2702I-UXK9</td>
<td>8.0.110.0</td>
<td>—</td>
</tr>
</tbody>
</table>
### Table 4: Software Support for Access Points (continued)

<table>
<thead>
<tr>
<th>Access Points</th>
<th>First Support</th>
<th>Last Support</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3500 Series</strong></td>
<td>AIR-CAP3501E</td>
<td>7.0.98.0</td>
</tr>
<tr>
<td>AIR-CAP3501I</td>
<td>7.0.98.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-CAP3502E</td>
<td>7.0.98.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-CAP3502I</td>
<td>7.0.98.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-CAP3502P</td>
<td>7.0.116.0</td>
<td>—</td>
</tr>
<tr>
<td><strong>3600 Series</strong></td>
<td>AIR-CAP3602I-x-K9</td>
<td>7.1.91.0</td>
</tr>
<tr>
<td>AIR-CAP3602I-xK910</td>
<td>7.1.91.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-CAP3602E-x-K9</td>
<td>7.1.91.0</td>
<td>—</td>
</tr>
<tr>
<td>AIR-CAP3602E-xK910</td>
<td>7.1.91.0</td>
<td>—</td>
</tr>
<tr>
<td>USC5101-AI-AIR-K9</td>
<td>7.6</td>
<td>—</td>
</tr>
<tr>
<td><strong>3700 Series</strong></td>
<td>AIR-CAP3702I</td>
<td>7.6</td>
</tr>
<tr>
<td>AIR-CAP3702E</td>
<td>7.6</td>
<td>—</td>
</tr>
<tr>
<td>AIR-CAP3702P</td>
<td>7.6</td>
<td>—</td>
</tr>
<tr>
<td><strong>600 Series</strong></td>
<td>AIR-OEAP602I</td>
<td>7.0.116.0</td>
</tr>
<tr>
<td><strong>1500 Mesh Series</strong></td>
<td>AIR-LAP-150</td>
<td>3.1.59.24</td>
</tr>
<tr>
<td>AIR-LAP-1510</td>
<td>3.1.59.24</td>
<td>4.2.207.54M</td>
</tr>
<tr>
<td>Access Points</td>
<td>First Support</td>
<td>Last Support</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>1520 Mesh Series</td>
<td>AIR-LAP1522AG</td>
<td>8.0.x</td>
</tr>
<tr>
<td></td>
<td>-A and N: 4.1.190.1 or 5.2 or later²</td>
<td>8.0.x</td>
</tr>
<tr>
<td></td>
<td>All other reg. domains: 4.1.191.24M or 5.2 or later¹</td>
<td>8.0.x</td>
</tr>
<tr>
<td></td>
<td>AIR-LAP1522HZ</td>
<td>8.0.x</td>
</tr>
<tr>
<td></td>
<td>-A and N: 4.1.190.1 or 5.2 or later¹</td>
<td>8.0.x</td>
</tr>
<tr>
<td></td>
<td>All other reg. domains: 4.1.191.24M or 5.2 or later¹</td>
<td>8.0.x</td>
</tr>
<tr>
<td></td>
<td>AIR-LAP1522PC</td>
<td>8.0.x</td>
</tr>
<tr>
<td></td>
<td>-A and N: 4.1.190.1 or 5.2 or later¹</td>
<td>8.0.x</td>
</tr>
<tr>
<td></td>
<td>All other reg. domains: 4.1.191.24M or 5.2 or later¹</td>
<td>8.0.x</td>
</tr>
<tr>
<td></td>
<td>AIR-LAP1522CM</td>
<td>8.0.x</td>
</tr>
<tr>
<td></td>
<td>7.0.116.0 or later</td>
<td>8.0.x</td>
</tr>
<tr>
<td></td>
<td>AIR-LAP1524SB</td>
<td>8.0.x</td>
</tr>
<tr>
<td></td>
<td>-A, C and N: 6.0 or later</td>
<td>8.0.x</td>
</tr>
<tr>
<td></td>
<td>All other reg. domains: 7.0.116.0 or later</td>
<td>8.0.x</td>
</tr>
<tr>
<td></td>
<td>AIR-LAP1524PS</td>
<td>8.0.x</td>
</tr>
<tr>
<td></td>
<td>-A: 4.1.192.22M or 5.2 or later¹</td>
<td>8.0.x</td>
</tr>
<tr>
<td>1530</td>
<td>AIR-CAP1532I-x-K9</td>
<td>7.6</td>
</tr>
<tr>
<td></td>
<td>AIR-CAP1532E-x-K9</td>
<td>7.6</td>
</tr>
<tr>
<td>1550</td>
<td>AIR-CAP1552C-x-K9</td>
<td>7.0.116.0</td>
</tr>
<tr>
<td></td>
<td>AIR-CAP1552E-x-K9</td>
<td>7.0.116.0</td>
</tr>
<tr>
<td></td>
<td>AIR-CAP1552H-x-K9</td>
<td>7.0.116.0</td>
</tr>
<tr>
<td></td>
<td>AIR-CAP1552I-x-K9</td>
<td>7.0.116.0</td>
</tr>
<tr>
<td></td>
<td>AIR-CAP1552EU-x-K9</td>
<td>7.3.101.0</td>
</tr>
<tr>
<td></td>
<td>AIR-CAP1552CU-x-K9</td>
<td>7.3.101.0</td>
</tr>
<tr>
<td></td>
<td>AIR-CAP1552WU-x-K9</td>
<td>8.0.100.0</td>
</tr>
</tbody>
</table>
Software Release Types and Recommendations

This section contains the following topics:

- Release Types, page 20
- Software Release Recommendations, page 21

## Release Types

<table>
<thead>
<tr>
<th>Table 5</th>
<th>Release Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Type</td>
<td>Description</td>
</tr>
<tr>
<td>Maintenance Deployment (MD) releases</td>
<td>Software releases that provide bug-fix support and ongoing software maintenance. These releases are categorized as Maintenance Deployment (MD) and may be part of the AssureWave program. These are releases with long life and ongoing software maintenance.</td>
</tr>
<tr>
<td>Early Deployment (ED) releases</td>
<td>Software releases that provide new features and new hardware platform support in addition to bug fixes. These releases are categorized as Early Deployment (ED). These are short-lived releases.</td>
</tr>
</tbody>
</table>
1. AssureWave is a Cisco program that focuses on satisfying customer quality requirements in key industry segments in the mobility space. This program links and expands on product testing conducted within development engineering, regression testing, and system test groups within Cisco. The AssureWave program has established partnerships with major device and application vendors to help ensure broader interoperability with our new release. The AssureWave certification marks the successful completion of extensive wireless LAN controller and access point testing in real-world use cases with a variety of mobile client devices applicable in a specific industry.

### Software Release Recommendations

**Table 6  Software Release Recommendations**

<table>
<thead>
<tr>
<th>Type of Release</th>
<th>Deployed Release</th>
<th>Recommended Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance Deployment (MD) releases</td>
<td>7.0 MD release train (latest release: 7.0.252.0)</td>
<td>7.4 MD release train (7.4.140.0 is the MD release)</td>
</tr>
<tr>
<td>Early Deployment (ED) releases for pre-802.11ac deployments</td>
<td>7.2 ED releases</td>
<td>7.4 MD release train (7.4.140.0 is the MD release)</td>
</tr>
<tr>
<td>Early Deployment (ED) releases for 802.11ac deployments</td>
<td>7.5 ED release</td>
<td>8.0 ED release (8.0.121.0 is 8.0MR2 on the 8.0 release train)</td>
</tr>
</tbody>
</table>

For detailed release recommendations, see the software release bulletin:


For more information about the Cisco Wireless solution compatibility matrix, see


### Upgrading to Cisco WLC Software Release 8.2.100.0

#### Guidelines and Limitations

- After upgrading to Release 8.2, the Cisco WLC might lose all IPv4 connectivity. The Cisco WLC can no longer service incoming SSH/Web sessions and is unable to ping other IPv4 stations. However, the default router is able to ping the Cisco WLC’s management interface.

  Every 10 seconds, a message similar to the following is sent to the msglog:

  
  This occurs in the following conditions:

  a. LAG is not configured.

  b. The management interface is untagged and is mapped to one physical port.

  c. When an untagged dynamic interface is added and mapped to port 2, the default route for the management interface is lost.

  The workaround is to configure all interfaces with VLANs.

  You can track this issue via CSCux75436.
- Effective with Release 8.2.100.0, you cannot download some of the older configurations from the Cisco WLC because of the Multicast and IP address validations introduced in this release. The platform support for global multicast and multicast mode are listed in the following table.

### Table 7  Platform Support for Global Multicast and Multicast Mode

<table>
<thead>
<tr>
<th>Platform</th>
<th>Global Multicast</th>
<th>Multicast Mode</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 5520, 8510, and 8540 WLCs</td>
<td>Enabled</td>
<td>Unicast</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Enabled</td>
<td>Multicast</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td>Unicast</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td>Multicast</td>
<td>No</td>
</tr>
<tr>
<td>Cisco Flex 7510 WLC</td>
<td>Multicast is not supported.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco 5508 WLC</td>
<td>Enabled</td>
<td>Unicast</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Enabled</td>
<td>Multicast</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td>Unicast</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td>Multicast</td>
<td>No</td>
</tr>
<tr>
<td>Cisco 2504 WLC</td>
<td>Only multicast mode is supported.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco vWLC</td>
<td>Multicast is not supported.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- In Release 8.2, the `reload` command is not recognized by Cisco Aironet 3600 Series APs. The workaround is to use the `debug capwap console cli` command.

- Cisco WLC Release 7.3.112.0, which is configured for new mobility, might revert to old mobility after upgrading to Release 7.6, even though Release 7.6 supports new mobility. This issue occurs when new mobility, which is compatible with the Cisco 5760 Wireless LAN Controller and the Cisco Catalyst 3850 Series Switch, are in use. However, old mobility is not affected.

The workaround is as follows:

a. Enter the following commands:
   ```
   config boot backup
   show boot
   
   Primary Boot Image.................. 7.6.100.0
   Backup Boot Image.................. 7.3.112.0 (default) (active)
   ```

b. After the reboot, press `Esc` on the console, and use the boot menu to select **Release 7.6**.

c. After booting on Release 7.6, set back the primary boot, and save the configuration by entering the following command:
   ```
   config boot primary
   ```

**Note** The epings are not available in the Cisco 5500 Series WLC when New Mobility is enabled.
If you downgrade from a Cisco WLC release that supports new mobility to a Cisco WLC release that does not support new mobility, for example, Cisco Wireless Release 7.6 to Release 7.3.x and you download the 7.6 configuration file with new mobility in enabled state, the release that does not support new mobility will have the new mobility feature in enabled state.

- If you downgrade from Release 8.2.100.0 to a 7.x release, the trap configuration is lost and must be reconfigured.
- If you upgrade from Release 8.0.110.0 to a later release, the config redundancy mobilitymac mac-addr command's setting is removed. You must manually reconfigure the mobility MAC address after the upgrade.
- If you are upgrading from Release 8.0.140.0 or 8.0.15x.0 to a later release and also have the multiple country code feature configured, the feature configuration is corrupted after the upgrade. For more information, see CSCve41740.
- If you have ACL configurations in a Cisco WLC, and downgrade from a 7.4 or later release to a 7.3 or earlier release, you might experience XML errors on rebooting the Cisco WLC. However, these errors do not have any impact on any of the functionalities or configurations.
- If you are upgrading from a 7.4.x or earlier release to a release later than 7.4, the Called Station ID type information is mapped to the RADIUS Accounting Called Station ID type; which, by default, is set to apradio-mac-ssid. You can configure the RADIUS Authentication Called Station ID type information by using the config radius auth callStationIdType command.
- When FlexConnect APs (known as H-REAP APs in the 7.0.x releases) that are associated with a Cisco WLC that has all the 7.0.x software releases prior to Release 7.0.240.0, upgrade to Release 8.2.100.0, the APs lose the enabled VLAN support configuration. The VLAN mappings revert to the default values of the VLAN of the associated interface. The workaround is to upgrade from Release 7.0.240.0 and later 7.0.x releases to Release 8.2.100.0.

In case of FlexConnect VLAN mapping deployment, we recommend that the deployment be done using FlexConnect groups. This allows you to recover VLAN mapping after an AP rejoins the Cisco WLC without having to manually reassign the VLAN mappings.

- When a client sends an HTTP request, the Cisco WLC intercepts it for redirection to the login page. If the HTTP GET request that is intercepted by the Cisco WLC is longer than 2000 bytes, the Cisco WLC drops the packet. Track CSCuy81133 for a possible enhancement to address this restriction.
- We recommend that you install Release 1.9.0.0 of Cisco Wireless LAN Controller Field Upgrade Software (FUS), which is a special AES package that contains several system-related component upgrades. These include the bootloader, field recovery image, and FPGA/MCU firmware. Installing the FUS image requires special attention because it installs some critical firmware. The FUS image is independent of the runtime image. For more information, see http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/fus_rn_OL-31390-01.html.
- The FUS image installation process reboots the Cisco WLC several times and reboots the runtime image. The entire process takes approximately 30 minutes. We recommend that you install the FUS image in a planned outage window.
Upgrading to Cisco WLC Software Release 8.2.100.0

**Note**

If you are using a Cisco 2500 Series controller and you intend to use the Application Visibility and Control (AVC) and NetFlow protocol features, you must install Release 1.9.0.0 of Cisco Wireless LAN Controller FUS. This is not required if you are using other controller hardware models.

- After you upgrade to Release 7.4, networks that were not affected by the existing preauthentication access control lists might not work because the rules are now enforced. That is, networks with clients configured with static DNS servers might not work unless the static server is defined in the preauthentication ACL.

- On the Cisco Flex 7500 Series WLCs, if FIPS is enabled, the reduced boot options are displayed only after a bootloader upgrade.

**Note**

Bootloader upgrade is not required if FIPS is disabled.

- If you have to downgrade from one release to another, you might lose the configuration from your current release. The workaround is to reload the previous Cisco WLC configuration files saved on the backup server, or to reconfigure the Cisco WLC.

- It is not possible to directly upgrade to Release 8.2.100.0 release from a release that is earlier than Release 7.0.98.0.

- You can upgrade or downgrade the Cisco WLC software only between certain releases. In some instances, you must first install an intermediate release prior to upgrading to Release 8.2.100.0. Table 8 shows the upgrade path that you must follow before downloading Release 8.2.100.0.

**Caution**

If you upgrade directly to 7.6.x or a later release from a release that is earlier than 7.5, the predownload functionality on Cisco Aironet 2600 and 3600 APs fails. The predownload functionality failure is only a one-time failure. After the upgrade to 7.6.x or a later release, the new image is loaded on the said Cisco APs, and the predownload functionality works as expected.

<table>
<thead>
<tr>
<th>Current Software Release</th>
<th>Upgrade Path to 8.2.100.0 Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.x</td>
<td>You can upgrade directly to 8.2.100.0.</td>
</tr>
<tr>
<td>8.0.x</td>
<td>You can upgrade directly to 8.2.100.0.</td>
</tr>
</tbody>
</table>

- When you upgrade the Cisco WLC to an intermediate software release, you must wait until all of the access points that are associated with the Cisco WLC are upgraded to the intermediate release before you install the latest Cisco WLC software. In large networks, it can take some time to download the software on each access point.

- You can upgrade to a new release of the Cisco WLC software or downgrade to an earlier release even if Federal Information Processing Standard (FIPS) is enabled.
When you upgrade to the latest software release, the software on the access points associated with the Cisco WLC is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession.

We recommend that you access the Cisco WLC GUI using Microsoft Internet Explorer 10 or a later version or Mozilla Firefox 32 or a later version.

Note

Microsoft Internet Explorer 8 might fail to connect over HTTPS because of compatibility issues. In such cases, you can explicitly enable SSLv3 by entering the `config network secureweb sslv3 enable` command.

Cisco WLCs support standard SNMP MIB files. MIBs can be downloaded from the Software Center on Cisco.com.

The Cisco WLC software is factory installed on your Cisco WLC and is automatically downloaded to the access points after a release upgrade and whenever an access point joins a Cisco WLC. We recommend that you install the latest software version available for maximum operational benefit.

Ensure that you have a TFTP, FTP, or SFTP server available for the software upgrade. Follow these guidelines when setting up a server:

- Ensure that your TFTP server supports files that are larger than the size of Cisco WLC software Release 8.2.100.0. Some TFTP servers that support files of this size are tftpd32 and the TFTP server within the Prime Infrastructure. If you attempt to download the 8.2.100.0 Cisco WLC software and your TFTP server does not support files of this size, the following error message appears:

  TFTP failure while storing in flash.

- If you are upgrading through the distribution system network port, the TFTP or FTP server can be on the same subnet or a different subnet because the distribution system port is routable.

When you plug a Cisco WLC into an AC power source, the bootup script and power-on self test is run to initialize the system. During this time, press `Esc` to display the bootloader Boot Options menu. The menu options for the Cisco 5500 Series WLC differ from the menu options for the other Cisco WLC platforms.

Bootloader menu for Cisco 5500 Series WLC:

```
Boot Options
Please choose an option from below:
1. Run primary image
2. Run backup image
3. Change active boot image
4. Clear Configuration
5. Format FLASH Drive
6. Manually update images
Please enter your choice:
```

Bootloader menu for other Cisco WLC platforms:

```
Boot Options
Please choose an option from below:
1. Run primary image
2. Run backup image
3. Manually update images
4. Change active boot image
5. Clear Configuration
Please enter your choice:
```
Enter 1 to run the current software, enter 2 to run the previous software, enter 4 (on Cisco 5500 Series WLC), or enter 5 (on Cisco WLC platforms other than 5500 series) to run the current software and set the Cisco WLC configuration to factory defaults. Do not choose the other options unless directed to do so.

Note: See the Installation Guide or the Quick Start Guide pertaining to your Cisco WLC platform for more details on running the bootup script and power-on self test.

- The Cisco WLC bootloader stores a copy of the active primary image and the backup image. If the primary image becomes corrupted, you can use the bootloader to boot with the backup image. With the backup image stored before rebooting, choose Option 2: Run Backup Image from the boot menu to boot from the backup image. Then, upgrade with a known working image and reboot the Cisco WLC.

- You can control the addresses that are sent in the Control and Provisioning of Wireless Access Points (CAPWAP) discovery responses when NAT is enabled on the Management Interface using the following command:

  config network ap-discovery nat-ip-only { enable | disable }

  Here:
  - enable—Enables use of NAT IP only in a discovery response. This is the default. Use this command if all the APs are outside the NAT gateway.
  - disable—Enables use of both NAT IP and non-NAT IP in a discovery response. Use this command if APs are on the inside and outside the NAT gateway, for example, Local Mode and OfficeExtend APs are on the same Cisco WLC.

Note: To avoid stranding of APs, you must disable AP link latency (if enabled) before you use the disable option for the config network ap-discovery nat-ip-only command. To disable AP link latency, use the config ap link-latency disable all command.

- You can configure 802.1p tagging by using the config qos dot1p-tag { bronze | silver | gold | platinum } command. For Release 7.2.103.0 and later releases, if you tag 802.1p packets, the tagging has an impact on only wired packets. Wireless packets are impacted only by the maximum priority level set for QoS.

- You can reduce the network downtime using the following options:
  - You can predownload the AP image.
  - For FlexConnect access points, use the FlexConnect AP upgrade feature to reduce traffic between the Cisco WLC and the AP (main site and the branch). For more information about the FlexConnect AP upgrade feature, see the Cisco Wireless Controller Configuration Guide.

Note: Predownloading Release 8.2.100.0 on a Cisco Aironet 1240 access point is not supported when upgrading from a previous Cisco WLC release. If predownloading is attempted on a Cisco Aironet 1240 access point, an AP disconnect will occur momentarily.

- Do not power down the Cisco WLC or any access point during the upgrade process; otherwise, you might corrupt the software image. Upgrading a Cisco WLC with a large number of access points can take as long as 30 minutes, depending on the size of your network. However, with the increased
number of concurrent access point upgrades supported, the upgrade time should be significantly reduced. The access points must remain powered, and the Cisco WLC must not be reset during this time.

- To downgrade from Release 8.2.100.0 to Release 6.0 or an earlier release, perform either of these tasks:
  - Delete all the WLANs that are mapped to interface groups, and create new ones.
  - Ensure that all the WLANs are mapped to interfaces rather than interface groups.

- After you perform the following functions on the Cisco WLC, reboot the Cisco WLC for the changes to take effect:
  - Enable or disable link aggregation (LAG)
  - Enable a feature that is dependent on certificates (such as HTTPS and web authentication)
  - Add a new license or modify an existing license
  - Increase the priority of a license
  - Enable HA
  - Install the SSL certificate
  - Configure the database size
  - Install the vendor-device certificate
  - Download the CA certificate
  - Upload the configuration file
  - Install the Web Authentication certificate
  - Make changes to the management interface or the virtual interface
  - Make changes to TCP MSS settings

**Upgrading to Cisco WLC Software Release 8.2.100.0 (GUI)**

**Step 1**
Upload your Cisco WLC configuration files to a server to back up the configuration files.

*Note*
We highly recommend that you back up your Cisco WLC configuration files prior to upgrading the Cisco WLC software.

**Step 2**
Follow these steps to obtain Cisco Wireless Release 8.2.100.0 software:

- Click this URL to go to the Software Center:
- Choose Wireless from the center selection window.
- Click Wireless LAN Controllers.
  The following options are displayed. Depending on your Cisco WLC platform, select either of these options:
  - Integrated Controllers and Controller Modules
  - Standalone Controllers
- Select the Cisco WLC model number or name.
The Download Software page is displayed.

e. The software releases are labeled as follows to help you determine which release to download. Click a Cisco WLC software release number:

- **Early Deployment (ED)**—These software releases provide new features and new hardware platform support as well as bug fixes.
- **Maintenance Deployment (MD)**—These software releases provide bug fixes and ongoing software maintenance.
- **Deferred (DF)**—These software releases have been deferred. We recommend that you migrate to an upgraded release.

f. Click the filename (filename.aes).

g. Click Download.

h. Read the Cisco End User Software License Agreement and click Agree.

i. Save the file to your hard drive.

j. Repeat steps a. through i. to download the remaining file.

**Step 3** Copy the Cisco WLC software file (filename.aes) to the default directory on your TFTP, FTP, or SFTP server.

**Step 4** (Optional) Disable the Cisco WLC 802.11a/n and 802.11b/g/n networks.

**Note** For busy networks, Cisco WLCs on high utilization, and small Cisco WLC platforms, we recommend that you disable the 802.11a/n and 802.11b/g/n networks as a precautionary measure.

**Step 5** Choose Commands > Download File to open the Download File to Controller page.

**Step 6** From the File Type drop-down list, choose Code.

**Step 7** From the Transfer Mode drop-down list, choose TFTP, FTP, or SFTP.

**Step 8** In the IP Address text box, enter the IP address of the TFTP, FTP, or SFTP server.

**Step 9** If you are using a TFTP server, the default value of 10 retries for the Maximum Retries text field, and 6 seconds for the Timeout text field should work correctly without any adjustment. However, you can change these values, if desired. To do so, enter the maximum number of times that the TFTP server attempts to download the software in the Maximum Retries text box and the amount of time (in seconds) for which the TFTP server attempts to download the software, in the Timeout text box.

**Step 10** In the File Path text box, enter the directory path of the software.

**Step 11** In the File Name text box, enter the name of the software file (filename.aes).

**Step 12** If you are using an FTP server, perform these steps:

- a. In the Server Login Username text box, enter the username with which to log on to the FTP server.
- b. In the Server Login Password text box, enter the password with which to log on to the FTP server.
- c. In the Server Port Number text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

**Step 13** Click Download to download the software to the Cisco WLC.

A message appears indicating the status of the download.

**Step 14** After the download is complete, click Reboot.

**Step 15** If you are prompted to save your changes, click Save and Reboot.
Step 16 Click OK to confirm your decision to reboot the Cisco WLC.

Step 17 For Cisco WiSM2 on the Catalyst switch, check the port channel and re-enable the port channel if necessary.

Step 18 If you have disabled the 802.11a/n and 802.11b/g/n networks in Step 4, re-enable them.

Step 19 To verify that the 8.2.100.0 Cisco WLC software is installed on your Cisco WLC, click Monitor on the Cisco WLC GUI and view the Software Version field under Controller Summary.

Special Notes for Licensed Data Payload Encryption on Cisco Wireless LAN Controllers

Datagram Transport Layer Security (DTLS) is required for all Cisco 600 Series OfficeExtend Access Point deployments to encrypt data plane traffic between the APs and the Cisco WLC. You can purchase Cisco Wireless LAN Controllers with either DTLS that is enabled (non-LDPE) or disabled (LDPE). If DTLS is disabled, you must install a DTLS license to enable DTLS encryption. The DTLS license is available for download on Cisco.com.

Important Note for Customers in Russia
If you plan to install a Cisco Wireless LAN Controller in Russia, you must get a Paper PAK, and not download the license from Cisco.com. The DTLS Paper PAK license is for customers who purchase a Cisco WLC with DTLS that is disabled due to import restrictions, but have authorization from local regulators to add DTLS support after the initial purchase. Refer to your local government regulations to ensure that DTLS encryption is permitted.

Note Paper PAKs and electronic licenses that are available are outlined in the respective Cisco WLC platform data sheets.

Downloading and Installing a DTLS License for an LDPE Cisco WLC

Step 1 To download the Cisco DTLS license:

a. Go to the Cisco Software Center at this URL:
   https://tools.cisco.com/SWIFT/LicensingUI/Home

b. From the Product License Registration page from the Get Other Licenses drop-down list, click IPS, Crypto, Other ...

c. In the Wireless section, click Cisco Wireless Controllers (2500/5500/7500/WiSM2) DTLS License and click Next.

d. Follow the on-screen instructions to generate the license file. The license file information will be sent to you in an e-mail.

Step 2 Copy the license file to your TFTP server.

Step 3 Install the DTLS license either by using the Cisco WLC web GUI interface or the CLI:

• To install the license using the WLC web GUI, choose:
Management > Software Activation > Commands > Action: Install License

- To install the license using the CLI, enter this command:

```plaintext
license install tftp://ipaddress/path/extracted-file
```

After the installation of the DTLS license, reboot the system. Ensure that the DTLS license that is installed is active.

---

### Upgrading from an LDPE to a Non-LDPE Cisco WLC

**Step 1**

Download the non-LDPE software release:

a. Go to the Cisco Software Center at:
   
   ```plaintext
   ```

b. Choose the Cisco WLC model.

c. Click **Wireless LAN Controller Software**.

d. In the left navigation pane, click the software release number for which you want to install the non-LDPE software.

e. Choose the non-LDPE software release: AIR-X-K9-X.X.aes

f. Click **Download**.

g. Read the Cisco End User Software License Agreement and then click **Agree**.

h. Save the file to your hard drive.

**Step 2**

Copy the Cisco WLC software file (`filename.aes`) to the default directory on your TFTP server or FTP server.

**Step 3**

Upgrade the Cisco WLC with this version by performing Step 3 through Step 19 detailed in the “Upgrading to Cisco WLC Software Release 8.2.100.0” section on page 21.

---

### Interoperability with Other Clients

This section describes the interoperability of Cisco WLC Software, Release 8.2.100.0 with other client devices.

**Table 9** describes the configuration used for testing the client devices.

<table>
<thead>
<tr>
<th>Hardware/Software Parameter</th>
<th>Hardware/Software Configuration Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>8.2.100.0</td>
</tr>
<tr>
<td>Cisco WLC</td>
<td>Cisco 55xx Series Controller</td>
</tr>
<tr>
<td>Access points</td>
<td>3502, 3602, 1602, 2602, 1702, 2702, 3702, 702, 702W, 1852</td>
</tr>
<tr>
<td>Radio</td>
<td>802.11ac, 802.11a, 802.11g, 802.11n2, 802.11n5</td>
</tr>
</tbody>
</table>
Table 9  Test Bed Configuration for Interoperability (continued)

<table>
<thead>
<tr>
<th>Security</th>
<th>Open, WEP, PSK (WPA and WPA2), 802.1X (WPA-TKIP and WPA2-AES) (LEAP, PEAP, EAP-FAST, EAP-TLS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS</td>
<td>ACS 4.2, ACS 5.2</td>
</tr>
<tr>
<td>Types of tests</td>
<td>Connectivity, traffic, and roaming between two access points</td>
</tr>
</tbody>
</table>

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

Table 10  Client Types

<table>
<thead>
<tr>
<th>Client Type and Name</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop</td>
<td></td>
</tr>
<tr>
<td>Intel 4965</td>
<td>v13.4</td>
</tr>
<tr>
<td>Intel 5100/5300</td>
<td>v14.3.2.1</td>
</tr>
<tr>
<td>Intel 6200</td>
<td>15.15.0.1</td>
</tr>
<tr>
<td>Intel 6300</td>
<td>15.16.0.2</td>
</tr>
<tr>
<td>Intel 6205</td>
<td>15.16.0.2</td>
</tr>
<tr>
<td>Intel 1000/1030</td>
<td>v14.3.0.6</td>
</tr>
<tr>
<td>Intel 7260</td>
<td>17.16.0.4</td>
</tr>
<tr>
<td>Intel 7265</td>
<td>17.16.0.4</td>
</tr>
<tr>
<td>Intel 3160</td>
<td>17.16.0.4</td>
</tr>
<tr>
<td>Broadcom 4360</td>
<td>6.30.163.2005</td>
</tr>
<tr>
<td>Linksys AE6000 (USB)</td>
<td>5.1.2.0</td>
</tr>
<tr>
<td>Netgear A6200 (USB)</td>
<td>6.30.145.30</td>
</tr>
<tr>
<td>Netgear A6210(USB)</td>
<td>5.1.18.0</td>
</tr>
<tr>
<td>D-Link DWA-182 (USB)</td>
<td>6.30.145.30</td>
</tr>
<tr>
<td>Engenius EUB 1200AC(USB)</td>
<td>1026.5.1118.2013</td>
</tr>
<tr>
<td>Asus AC56(USB)</td>
<td></td>
</tr>
<tr>
<td>Dell 1395/1397/Broadcom 4312HMG(L)</td>
<td>5.30.21.0</td>
</tr>
<tr>
<td>Dell 1501 (Broadcom BCM4313)</td>
<td>v5.60.48.35/v5.60.350.11</td>
</tr>
<tr>
<td>Dell 1505/1510/Broadcom 4321MCAG/4322HM</td>
<td>5.60.18.8</td>
</tr>
<tr>
<td>Dell 1515(Atheros)</td>
<td>8.0.0.239</td>
</tr>
<tr>
<td>Dell 1520/Broadcom 4322HMS</td>
<td>5.60.48.18</td>
</tr>
<tr>
<td>Dell 1530 (Broadcom BCM4359)</td>
<td>5.100.235.12</td>
</tr>
<tr>
<td>Dell 1540</td>
<td>6.30.223.215</td>
</tr>
<tr>
<td>Cisco CB21</td>
<td>1.3.0.532</td>
</tr>
<tr>
<td>Atheros HB92/HB97</td>
<td>8.0.0.320</td>
</tr>
<tr>
<td>Atheros HB95</td>
<td>7.7.0.358</td>
</tr>
<tr>
<td>MacBook Pro</td>
<td>OSX 10.11.1</td>
</tr>
</tbody>
</table>
### Interoperability with Other Clients

#### Table 10  Client Types (continued)

<table>
<thead>
<tr>
<th>Client Type and Name</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>MacBook Air old</td>
<td>OSX 10.11.1</td>
</tr>
<tr>
<td>MacBook Air new</td>
<td>OSX 10.11.1</td>
</tr>
<tr>
<td>Macbook Pro with Retina Display</td>
<td>OSX 10.11.1</td>
</tr>
<tr>
<td>Macbook New 2015</td>
<td>OSX 10.11.1</td>
</tr>
</tbody>
</table>

#### Tablets

<table>
<thead>
<tr>
<th>Client Type and Name</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple iPad2</td>
<td>iOS 9.1(13B143)</td>
</tr>
<tr>
<td>Apple iPad3</td>
<td>iOS 9.1(13B143)</td>
</tr>
<tr>
<td>Apple iPad mini with Retina display</td>
<td>iOS 9.1(13B143)</td>
</tr>
<tr>
<td>Apple iPad Air</td>
<td>iOS 9.1(13B143)</td>
</tr>
<tr>
<td>Apple iPad Air 2</td>
<td>iOS 9.1(13B143)</td>
</tr>
<tr>
<td>Samsung Galaxy Tab Pro SM-T320</td>
<td>Android 4.4.2</td>
</tr>
<tr>
<td>Samsung Galaxy Tab 10.1- 2014 SM-P600</td>
<td>Android 4.4.2</td>
</tr>
<tr>
<td>Samsung Galaxy Note 3 - SM-N900</td>
<td>Android 5.0</td>
</tr>
<tr>
<td>Microsoft Surface Pro 3</td>
<td>Windows 8.1 Driver: 15.68.3073.151</td>
</tr>
<tr>
<td>Microsoft Surface Pro 2</td>
<td>Windows 8.1 Driver: 14.69.24039.134</td>
</tr>
<tr>
<td>Google Nexus 9</td>
<td>Android 6.0</td>
</tr>
<tr>
<td>Google Nexus 7 2nd Gen</td>
<td>Android 5.0</td>
</tr>
<tr>
<td>Intermec CK70</td>
<td>Windows Mobile 6.5 / 2.01.06.0355</td>
</tr>
<tr>
<td>Intermec CN50</td>
<td>Windows Mobile 6.1 / 2.01.06.0333</td>
</tr>
<tr>
<td>Symbol MC5590</td>
<td>Windows Mobile 6.5 / 3.00.0.0.051R</td>
</tr>
<tr>
<td>Symbol MC75</td>
<td>Windows Mobile 6.5 / 3.00.2.0.006R</td>
</tr>
</tbody>
</table>

#### Phones and Printers

<table>
<thead>
<tr>
<th>Client Type and Name</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 7921G</td>
<td>1.4.5.3.LOADS</td>
</tr>
<tr>
<td>Cisco 7925G</td>
<td>1.4.5.3.LOADS</td>
</tr>
<tr>
<td>Cisco 8861</td>
<td>Sip88xx.10-2-1-16</td>
</tr>
<tr>
<td>Ascom i75</td>
<td>1.8.0</td>
</tr>
<tr>
<td>Spectralink 8030</td>
<td>119.081/131.030/132.030</td>
</tr>
<tr>
<td>Apple iPhone 4S</td>
<td>iOS 9.1(13B143)</td>
</tr>
<tr>
<td>Apple iPhone 5</td>
<td>iOS 9.1(13B143)</td>
</tr>
<tr>
<td>Apple iPhone 5s</td>
<td>iOS 9.1(13B143)</td>
</tr>
<tr>
<td>Apple iPhone 5c</td>
<td>iOS 9.1(13B143)</td>
</tr>
<tr>
<td>Apple iPhone 6</td>
<td>iOS 9.1(13B143)</td>
</tr>
<tr>
<td>Apple iPhone 6 Plus</td>
<td>iOS 9.1(13B143)</td>
</tr>
<tr>
<td>HTC One</td>
<td>Android 5.0</td>
</tr>
</tbody>
</table>
Table 10  Client Types (continued)

<table>
<thead>
<tr>
<th>Client Type and Name</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>OnePlusOne</td>
<td>Android 4.3</td>
</tr>
<tr>
<td>Samsung Galaxy S4 T-I9500</td>
<td>Android 5.0.1</td>
</tr>
<tr>
<td>Sony Xperia Z Ultra</td>
<td>Android 4.4.2</td>
</tr>
<tr>
<td>Nokia Lumia 1520</td>
<td>Windows Phone 8.1</td>
</tr>
<tr>
<td>Google Nexus 5</td>
<td>Android 5.1</td>
</tr>
<tr>
<td>Nexus 6</td>
<td>Android 5.1.1</td>
</tr>
<tr>
<td>Samsung Galaxy S5-SM-G900A</td>
<td>Android 4.4.2</td>
</tr>
<tr>
<td>Huawei Ascend P7</td>
<td>Android 4.4.2</td>
</tr>
<tr>
<td>Samsung Galaxy S III</td>
<td>Android 4.3</td>
</tr>
<tr>
<td>SpectraLink 8450</td>
<td>3.0.2.6098/5.0.0.8774</td>
</tr>
<tr>
<td>Samsung Galaxy Nexus GTI9200</td>
<td>Android 4.4.2</td>
</tr>
<tr>
<td>Samsung Galaxy Mega SM900</td>
<td>Android 4.4.2</td>
</tr>
<tr>
<td>Samsung Galaxy S6</td>
<td>Android 5.1.1</td>
</tr>
</tbody>
</table>

Features Not Supported on Cisco WLC Platforms

This section lists the features that are not supported on the different Cisco WLC platforms:

- Features Not Supported on Cisco 2504 WLC, page 33
- Features Not Supported on Cisco WiSM2 and Cisco 5508 WLC, page 34
- Features Not Supported on Cisco Flex 7510 WLCs, page 34
- Features Not Supported on Cisco 5520, 8510, and 8540 WLCs, page 35
- Features Not Supported on Cisco Virtual WLCs, page 35
- Features Not Supported on Mesh Networks, page 36

Note

In a converged access environment that has Cisco WLCs running AireOS code, High Availability Client SSO and native IPv6 are not supported.

Features Not Supported on Cisco 2504 WLC

- Autostart
- Cisco WLC integration with Lync SDN API
- Application Visibility and Control (AVC) for FlexConnect local switched access points
- Application Visibility and Control (AVC) for FlexConnect centrally switched access points

Note

However, AVC for local mode APs is supported.
• Bandwidth Contract
• Service Port
• AppleTalk Bridging
• Right-to-Use Licensing
• PMIPv6
• EoGRE
• AP Stateful Switchover (SSO) and client SSO
• Multicast-to-Unicast
• Cisco Smart Software Licensing

---

**Note**
The features that are not supported on Cisco WiSM2 and Cisco 5508 WLC are not supported on Cisco 2504 WLCs too.

---

**Note**
Directly connected APs are supported only in the local mode.

---

### Features Not Supported on Cisco WiSM2 and Cisco 5508 WLC

• Spanning Tree Protocol (STP)
• Port Mirroring
• VPN Termination (such as IPsec and L2TP)
• VPN Passthrough Option

---

**Note**
You can replicate this functionality on a Cisco 5500 Series WLC by creating an open WLAN using an ACL.

---

• Configuration of 802.3 bridging, AppleTalk, and Point-to-Point Protocol over Ethernet (PPPoE)
• Fragmented pings on any interface
• Right-to-Use Licensing
• Cisco 5508 WLC cannot function as mobility controller (MC). However, Cisco 5508 WLC can function as guest anchor in a New Mobility environment.
• Cisco Smart Software Licensing

### Features Not Supported on Cisco Flex 7510 WLCs

• Static AP-manager interface

---

**Note**
For Cisco Flex 7500 Series WLCs, it is not necessary to configure an AP-manager interface. The management interface acts as an AP-manager interface by default, and the access points can join on this interface.

---
Features Not Supported on Cisco WLC Platforms

- TrustSec SXP
- IPv6 and Dual Stack client visibility

Note IPv6 client bridging and Router Advertisement Guard are supported.

- Internal DHCP server
- Access points in local mode

Note An AP associated with the Cisco WLC in the local mode should be converted to the FlexConnect mode or monitor mode, either manually or by enabling the autoconvert feature. On the Cisco Flex 7500 WLC CLI, enable the autoconvert feature by entering the `config ap autoconvert enable` command.

- Mesh (use Flex + Bridge mode for mesh-enabled FlexConnect deployments)
- Spanning Tree Protocol (STP)
- Cisco Flex 7500 Series WLC cannot be configured as a guest anchor Cisco WLC. However, it can be configured as a foreign Cisco WLC to tunnel guest traffic to a guest anchor Cisco WLC in a DMZ.
- Multicast

Note FlexConnect local-switched multicast traffic is bridged transparently for both wired and wireless on the same VLAN. FlexConnect access points do not limit traffic based on Internet Group Management Protocol (IGMP) or MLD snooping.

- PMIPv6
- Cisco Smart Software Licensing

Features Not Supported on Cisco 5520, 8510, and 8540 WLCs

- Internal DHCP Server
- Mobility controller functionality in converged access mode

Note Cisco Smart Software Licensing is not supported on Cisco 8510 WLC.

Features Not Supported on Cisco Virtual WLCs

- Cisco Aironet 1850 and 1830 Series APs
- Internal DHCP server
- TrustSec SXP
- Access points in local mode
- Mobility/Guest Anchor
- Wired Guest
Features Not Supported on Access Point Platforms

- Multicast

Note

FlexConnect local-switched multicast traffic is bridged transparently for both wired and wireless on the same VLAN. FlexConnect access points do not limit traffic based on IGMP or MLD snooping.

- FlexConnect central switching in large-scale deployments

Note

FlexConnect central switching is supported in only small-scale deployments, wherein the total traffic on Cisco WLC ports is not more than 500 Mbps.

FlexConnect local switching is supported.

- AP and Client SSO in High Availability
- PMIPv6
- EoGRE (Supported in only local switching mode)
- Workgroup Bridges
- Client downstream rate limiting for central switching
- SHA2 certificates
- Cisco WLC integration with Lync SDN API

Features Not Supported on Mesh Networks

- Load-based call admission control (CAC). Mesh networks support only bandwidth-based CAC or static CAC
- High availability (fast heartbeat and primary discovery join timer)
- AP acting as supplicant with EAP-FASTv1 and 802.1X authentication
- Access point join priority (mesh access points have a fixed priority)
- Location-based services

Features Not Supported on Access Point Platforms

- Features Not Supported on Cisco Aironet 1830 and 1850 APs, page 36
- Features Not Supported on Cisco Aironet 1550 APs (with 64-MB Memory), page 37

Features Not Supported on Cisco Aironet 1830 and 1850 APs

- Cisco Virtual Wireless Controller
- Mesh mode
- Flex mode
- Monitor mode
• Workgroup Bridge (WGB) mode
• Link aggregation (LAG)
• OfficeExtend mode
• Enhanced Local Mode (ELM)
• Integrated BLE
• Basic spectrum analysis
• USB-based Bluetooth Low Energy (BLE) device support
• Cisco CleanAir
• Cisco Wireless ClientLink 3.0
• Rogue Location Discovery Protocol (RLDP)
• Cisco Compatible eXtensions (CCX) Specification
• 802.1x supplicant for AP authentication on the wired port
• CKIP, CMIC, and LEAP with Dynamic WEP
• Static WEP key for TKIP or CKIP
• Dynamic Transmit Power Control (DTPC)
• Federal Information Processing Standard (FIPS) and Common Criteria
• 40-MHz Rogue detection
• Native IPv6
• Telnet
• SIP snooping with FlexConnect in local switching mode

Note
For Cisco Aironet1850 Series AP technical specifications with details on currently supported features, see the Cisco Aironet 1850 Series Access Points Data Sheet.

Features Not Supported on Cisco Aironet 1550 APs (with 64-MB Memory)

• PPPoE
• PMIPv6

Note
To see the amount of memory in a Cisco Aironet 1550 AP, enter the following command:

(Cisco Controller) >show mesh ap summary

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

To view the details of the software bugs pertaining to your product, perform the following task:
Click the Caveat ID/Bug ID number in the table.

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

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

To view the details of a caveat whose ID you do not have, perform the following procedure:

1. Access the BST using your Cisco user ID and password:
   https://tools.cisco.com/bugsearch/

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

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

## Open Caveats

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCux59615</td>
<td>8.2.100.0 has incorrect Build Name</td>
</tr>
<tr>
<td>CSCux15561</td>
<td>Cisco 3500 AP/Cisco 1260 AP gets into “ap:” mode after power cycle</td>
</tr>
<tr>
<td>CSCux21159</td>
<td>Autonomous Bridge—PSK corruption after non-root Bridge reboots</td>
</tr>
<tr>
<td>CSCuv14242</td>
<td>HTTP profiling support for Cisco 1850 AP</td>
</tr>
<tr>
<td>CSCuv51142</td>
<td>SCTG ST: Module reboots after sending LTE data of more than 1300 bytes</td>
</tr>
<tr>
<td>CSCux20138</td>
<td>Cisco 3602 AP memory leak at processor pool. Needs reboot to join Cisco WLC</td>
</tr>
<tr>
<td>CSCuw36523</td>
<td>AP crashdump validate_memory during Cisco WLC upgrade or downgrade operation</td>
</tr>
<tr>
<td>CSCuu63964</td>
<td>02044802: Apple clients cannot reconnect Cisco 1850i AP on forceful deauthentication</td>
</tr>
<tr>
<td>CSCux28011</td>
<td>DNS-ACL feature not working with Cisco 1850 AP</td>
</tr>
<tr>
<td>CSCuv61089</td>
<td>Cisco AP is duplicating packets to wireless clients and Cisco WLC</td>
</tr>
<tr>
<td>CSCur68316</td>
<td>Cisco 802AP-891 in FlexConnect mode are losing VLAN mapping after power cycle</td>
</tr>
<tr>
<td>CSCux17645</td>
<td>Mobility Express: Radio failure (firmware stopped responding) during upgrade from Cisco Wireless Release 8.1.131.0 to Cisco Wireless Release 8.2</td>
</tr>
<tr>
<td>CSCux02417</td>
<td>OTA and OTDS roaming performance does not meet 50-millisecond benchmark</td>
</tr>
<tr>
<td>CSCuw84036</td>
<td>LWAP FlexConnect mode generates traffic blackholing upon WGB PMC cache timeout</td>
</tr>
<tr>
<td>CSCux31277</td>
<td>Missing Carrier set on 2.4-Ghz radio for AP803H-AGN-Z-K9</td>
</tr>
<tr>
<td>CSCUt80914</td>
<td>SC3 mesh: Low uplink throughput from MAP1 with 80-MHz client [BZ1142]</td>
</tr>
<tr>
<td>CSCux12825</td>
<td>Cisco 1850 AP is doing ping to 8.8.8.8</td>
</tr>
<tr>
<td>CSCux12878</td>
<td>Cisco 1850 AP is trying to contact Meraki server</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCuq76115</td>
<td>WGB clients with DSCP marking to QoS queue mapping does not work on ISR819</td>
</tr>
<tr>
<td>CSCux11777</td>
<td>Cisco 1532 AP non-root bridge high retransmission and latency rate</td>
</tr>
<tr>
<td>CSCuw30644</td>
<td>Cisco 702W AP 2.4-GHz radio showing low to no throughput at random times</td>
</tr>
<tr>
<td>CSCuw65706</td>
<td>Cisco 1530 AP WGB drops Tx used with other 1530 WGB in the same MAC address range</td>
</tr>
<tr>
<td>CSCuw29564</td>
<td>Cisco APs show 0 neighbors on the 5-GHz band and client 802.11 packets are ignored</td>
</tr>
<tr>
<td>CSCuv32179</td>
<td>Low throughput with 3700 WGB 80 MHz</td>
</tr>
<tr>
<td>CSCuu11133</td>
<td>Wi-Fi TCP downlink degraded with SCTP module traffic</td>
</tr>
<tr>
<td>CSCux07090</td>
<td>AP CRASH watchdog reset (wcpd no heartbeat) coredump: process wcpd</td>
</tr>
<tr>
<td>CSCuw41092</td>
<td>Cisco AP does not send traffic indication in beacon for power-save client after FT</td>
</tr>
<tr>
<td>CSCux06806</td>
<td>ATF EnforcementConfig for network radio is not pushed to uploaded config</td>
</tr>
<tr>
<td>CSCux21420</td>
<td>Cisco WiSM2 stops responding under Task name: redXmlTransferMain</td>
</tr>
<tr>
<td>CSCux18548</td>
<td>Inter-WLC roaming is not successful for EoGRE tunnel</td>
</tr>
<tr>
<td>CSCuw97966</td>
<td>10G link down after reboot on Cisco 8510 WLC on Nexus 5k</td>
</tr>
<tr>
<td>CSCuv03963</td>
<td>Multiple Cisco 8510 WLCs using Cisco Wireless Release 8.0110.x DP stopped responding</td>
</tr>
<tr>
<td>CSCux28505</td>
<td>Cisco 8510 WLC stopped responding with &quot;fp_main_task&quot; on a Cisco Wireless Release 8.2.x image</td>
</tr>
<tr>
<td>CSCuw43910</td>
<td>Local switching/local authentication clients drop when latency is introduced</td>
</tr>
<tr>
<td>CSCux21803</td>
<td>Client does not receive broadcast ARP request after AP failover</td>
</tr>
<tr>
<td>CSCux26911</td>
<td>Cisco WLC stopped responding on the <code>config flexconnect arp-caching</code> command</td>
</tr>
<tr>
<td>CSCux00531</td>
<td>Cisco 2504 and 5508 WLCs have partial collection failure file transfer config</td>
</tr>
<tr>
<td>CSCux13657</td>
<td>Roaming of Mesh AP via backhaul is no longer working on 2.4-GHz client</td>
</tr>
<tr>
<td>CSCux22286</td>
<td><code>snmpset clMeshNodeRAPDownlinkBackhaul get-response</code> is the old value</td>
</tr>
<tr>
<td>CSCux00803</td>
<td>New Mobility clients stuck in DHCP_REQD state with NAT IP on Foreign WLC</td>
</tr>
<tr>
<td>CSCuw14938</td>
<td>New Mobility system does not respond on Task Name mmMaListen</td>
</tr>
<tr>
<td>CSCuw95402</td>
<td>SNMP does not return correct information for roaming client</td>
</tr>
<tr>
<td>CSCuw93917</td>
<td>NetFlow configuration cannot be modified after downgrading from Release 8.2 to Release 8.1</td>
</tr>
<tr>
<td>CSCux05901</td>
<td>Cisco 5508 WLC does not honor AAA override for upload bandwidth for web authentication</td>
</tr>
<tr>
<td>CSCux28768</td>
<td>Cisco 1142 AP radios appear to be operational on CLI but down on Cisco WLC (clients cannot connect)</td>
</tr>
<tr>
<td>CSCux17026</td>
<td>Frequent channel changes on 40-MHz DCA</td>
</tr>
<tr>
<td>CSCuw36069</td>
<td>Threshold MIBs incorrectly set for WSSI modules</td>
</tr>
<tr>
<td>CSCux14487</td>
<td>Cisco WLC becomes unresponsive during 802.11b advanced config is loading through CLI</td>
</tr>
</tbody>
</table>
## Resolved Caveats

### Table 12  Resolved Caveats

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuv99415</td>
<td>Access Point should boot up even if CAPWAP IOS download is corrupted</td>
</tr>
<tr>
<td>CSCuv41888</td>
<td>Cisco AP 1570 RCV153-3-JA3/JA4 image sends Bridge Protocol Data Units to the network</td>
</tr>
<tr>
<td>CSCuv03380</td>
<td>During Mesh Roam security error, Gateway is not reachable leading to CAPWAP Restart</td>
</tr>
<tr>
<td>CSCuu17338</td>
<td>Cisco AP 1142 Configuration loss occurs after cold reboot</td>
</tr>
<tr>
<td>CSCur76547</td>
<td>Access Point with static Internet Protocol configured behavior is seen in Dynamic Host Configuration Protocol (DHCP) client after reload</td>
</tr>
<tr>
<td>CSCuv40330</td>
<td>Deb CAPWAP shows IPv6 addresses incorrectly</td>
</tr>
<tr>
<td>CSCut86489</td>
<td>RADIUIS on Cisco WLC shows DOWN but is UP on the Access Points with Queue already full</td>
</tr>
<tr>
<td>CSCuv93051</td>
<td>Access Point unexpected reload seen due to ‘Signature Validation Failed’</td>
</tr>
<tr>
<td>CSCuv36306</td>
<td>Cisco AP 2702 In Monitor Mode sensord_crash File No CleanAir mSMTS</td>
</tr>
</tbody>
</table>
### Table 12  Resolved Caveats (continued)

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuv33747</td>
<td>Cisco AP 3600 ‘Tx jammed’ error is seen and radio is reset due to sensord stuck</td>
</tr>
<tr>
<td>CSCuu01474</td>
<td>“dot11 ant-band-mode” CLI is not present in 1570 AP</td>
</tr>
<tr>
<td>CSCus78002</td>
<td>Cisco AP1262 unexpected reload is seen right after STACKLOW for Dot11 DB Audit</td>
</tr>
<tr>
<td>CSCut82091</td>
<td>Cisco AP-3702/3602/1602 an unexpected reload is seen with this Process: “CAPWAP CLIENT”</td>
</tr>
<tr>
<td>CSCuw36636</td>
<td>Cisco Access Point shows no RST code when DFS triggers</td>
</tr>
<tr>
<td>CSCuv61271</td>
<td>Window DHCP BAD_ADDRESS displays for Access Points</td>
</tr>
<tr>
<td>CSCuv81004</td>
<td>Autonomous Access Point fails to create MCST key with single SSID multi VLAN AAA</td>
</tr>
<tr>
<td>CSCuv02592</td>
<td>Gig1 configuration is not restored when Access Point is reloaded on 2700/1700 APs</td>
</tr>
<tr>
<td>CSCus91214</td>
<td>Cisco AP802 15.3(3)JAB unexpectedly reloads always on issuing “dir all-filesystems” ISR C881W</td>
</tr>
<tr>
<td>CSCuw88703</td>
<td>Unable to start host pad after enable/disable Access Point</td>
</tr>
<tr>
<td>CSCuo95728</td>
<td>Cisco Access Point not validating UDP-Lite checksum</td>
</tr>
<tr>
<td>CSCut23325</td>
<td>Cisco 1700 AP not encrypting Internet Control Message Protocol (ICMP) and Address Resolution Protocol (ARP) sent from the client over the air</td>
</tr>
<tr>
<td>CSCuv54033</td>
<td>Egress Access Control List (ACL) not working when it is switched from Ingress to Egress</td>
</tr>
<tr>
<td>CSCuv86360</td>
<td>Error code mismatch on the Access Point during the debugs for Access Control List (ACL) is not found</td>
</tr>
<tr>
<td>CSCur58057</td>
<td>Flex Access Point loses some Wireless Local Area Networks (WLAN)s after radio resets</td>
</tr>
<tr>
<td>CSCuw61901</td>
<td>Local Auth Extensible Authentication (EAP)-Flexible Authentication via Secure Tunneling (FAST) not working for Flex AP Auth user with any connect</td>
</tr>
<tr>
<td>CSCuw28531</td>
<td>Network Address Translation (NAT) is not working with two different Wireless Local Area Networks (WLANs) in PPPoE submode</td>
</tr>
<tr>
<td>CSCut40485</td>
<td>Spurious messages seen on Access Point console</td>
</tr>
<tr>
<td>CSCuv08570</td>
<td>Cisco 1532 AP loses all configuration at times after power cycle</td>
</tr>
<tr>
<td>CSCuw02551</td>
<td>UX Access Point cannot use 80mhz bandwidth</td>
</tr>
<tr>
<td>CSCut40592</td>
<td>AC Rates are missing when speed set through GUI</td>
</tr>
<tr>
<td>CSCut85027</td>
<td>Cisco Access Point is generating corrupted core dump</td>
</tr>
<tr>
<td>CSCuw27198</td>
<td>Clarify debug dfs simulate command on Lightweight Access Point Protocol (LWAP)</td>
</tr>
<tr>
<td>CSCut68661</td>
<td>Cisco Access Point crash AP702 - ar9300_set_desc_link is seen</td>
</tr>
<tr>
<td>CSCur85640</td>
<td>8.1.10.72 - Access Points reboot with background scanning enabled after show ver command</td>
</tr>
<tr>
<td>CSCuu22083</td>
<td>Access Point unexpected reload is seen in MESH ASTools PROCESS during mesh initialization</td>
</tr>
<tr>
<td>CSCuu31357</td>
<td>Access Point unexpected reload is seen in [Adj Process] for VW-ap1530.cc6c.map2</td>
</tr>
</tbody>
</table>
### Caveats

**Table 12 Resolved Caveats (continued)**

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCut81253</td>
<td>Ethernet Bridging does not work on Returned Accounts Procedure (RAP) with 5ghz backhaul</td>
</tr>
<tr>
<td>CSCuw18306</td>
<td>Mesh AP 5GHz channel on non-configured channel in Dynamic Channel Assignment (DCA) list on Cisco WLC</td>
</tr>
<tr>
<td>CSCuu77304</td>
<td>Clients are deauthenticated from OEAP 600 Local Area Network (LAN) ports</td>
</tr>
<tr>
<td>CSCuv69967</td>
<td>OEAP600 wired 802.1x remote Local Area Network (LAN) forward traffic is seen in 802.1x Required State</td>
</tr>
<tr>
<td>CSCut15726</td>
<td>“AP MAC address” changes to “AP MAC address (Ethernet to CM)”</td>
</tr>
<tr>
<td>CSCux12850</td>
<td>Connection monitor is active on 1850 AP</td>
</tr>
<tr>
<td>CSCuv53770</td>
<td>Version reported as Cisco Cheetah AP in Cisco Discovery protocol (CDP) neighbor information</td>
</tr>
<tr>
<td>CSCut99150</td>
<td>Cisco 2702 AP is requesting as a Type 1 power device instead of Type 2</td>
</tr>
<tr>
<td>CSCuv959274</td>
<td>1142 CPU spike and utilization is 100% all the time</td>
</tr>
<tr>
<td>CSCuw91227</td>
<td>Air Time Fairness (ATF) is not supported on Cisco 1700 AP model</td>
</tr>
<tr>
<td>CSCuv10692</td>
<td>AckFailureCount is getting huge value in short period</td>
</tr>
<tr>
<td>CSCuw57578</td>
<td>Access Point send retry packets are more than configured “packet retries”</td>
</tr>
<tr>
<td>CSCut56741</td>
<td>Cisco AP1600: Radio reset with “STOPPING CPQ FWD TRACE ON Bad CPQ removal”</td>
</tr>
<tr>
<td>CSCut57453</td>
<td>Cisco AP2700 in mesh bridge mode disconnects from Returned Accounts Procedure (RAP) frequently</td>
</tr>
<tr>
<td>CSCuv39290</td>
<td>Cisco AP2700/3700 PAK Stuck is seen on Returned Accounts Procedure (RAP) Radio d1 reset: fp cl</td>
</tr>
<tr>
<td>CSCuw27385</td>
<td>Cisco Access Point: 3702 radio reset 'transmitter seems to have stopped' error is seen.</td>
</tr>
<tr>
<td>CSCuu02281</td>
<td>Access Points on Cisco WLC with wireless networks gets disabled while detecting rogues</td>
</tr>
<tr>
<td>CSCuu06047</td>
<td>Packet drops on Cisco 2702 Access Point in Flex Local Auth/Local Switch mode</td>
</tr>
<tr>
<td>CSCut95812</td>
<td>QN - Access Point Radio Reset with Beacons Stuck</td>
</tr>
<tr>
<td>CSCut95835</td>
<td>QN - Access Point Radio Reset with PAK Stuck</td>
</tr>
<tr>
<td>CSCut66360</td>
<td>Cisco AP1570 does not display operating temperature for some Access Points</td>
</tr>
<tr>
<td>CSCuu46746</td>
<td>Radio resets with off channel request stuck</td>
</tr>
<tr>
<td>CSCut64553</td>
<td>Reduce RAM disk usage to allow DFS Debugging</td>
</tr>
<tr>
<td>CSCuv34176</td>
<td>SF3:Transmitter Stop Radio is reset due Delivery Traffic Indication Message Multicast PAK stuck[BZ 976]</td>
</tr>
<tr>
<td>CSCuo33980</td>
<td>Workgroup Bridge roaming delay up to 10 seconds is seen</td>
</tr>
<tr>
<td>CSCuv48278</td>
<td>Unable to connect clients in 802.11ac Mode for -D domain</td>
</tr>
<tr>
<td>CSCuw87468</td>
<td>Rogue containment not working on 8.0.120.0 for Cisco AP3700 with Wireless Security Module (WSM) module</td>
</tr>
<tr>
<td>CSCuv35186</td>
<td>Tx power change is not working as expected for Radio Resource Management (RRM) Interop.</td>
</tr>
</tbody>
</table>
### Table 12  Resolved Caveats (continued)

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuw23023</td>
<td>Cisco 3700 Access Point Sniffer Mode not capturing on 5ghz radio with Rx-SOP set</td>
</tr>
<tr>
<td>CSCut30549</td>
<td>Inconsistent Access Point inventory information is seen between Cisco WLC and Access Point.</td>
</tr>
<tr>
<td>CSCuv27320</td>
<td>Wired clients in 702w Access Point leaking traffic across Ports/VLANS</td>
</tr>
<tr>
<td>CSCuw57048</td>
<td>Workgroup Bridge (WGB) roams with “Had to lower data rate”; minimum-rate is not configured</td>
</tr>
<tr>
<td>CSCut94260</td>
<td>Access Point Wireless Intrusion Prevention System (WIPS) module sending random characters in the alarm message</td>
</tr>
<tr>
<td>CSCuw57588</td>
<td>Cisco C3600 AP unexpected reload is seen on am_xml_GetChildCount</td>
</tr>
<tr>
<td>CSCut40794</td>
<td>Access Point Impersonator alarm is seen for Cisco AP 3602i</td>
</tr>
<tr>
<td>CSCuv26697</td>
<td>Cisco 1532 Access Points not passing VLAN Trunking Protocol (VTP) info over the bridge link</td>
</tr>
<tr>
<td>CSCur62558</td>
<td>Add Link Layer Discovery Protocol (LLDP) support for autonomous Access Points</td>
</tr>
<tr>
<td>CSCuu45186</td>
<td>dot11 ARP-cache does not works well</td>
</tr>
<tr>
<td>CSCuq03928</td>
<td>IPv6 MIB support to show dual stack</td>
</tr>
<tr>
<td>CSCup82047</td>
<td>Syslog trap level for Access Point is inconsistent in controller</td>
</tr>
<tr>
<td>CSCuw44480</td>
<td>802dot11r client fails Authorization if self reset is done before user idle timeout expires</td>
</tr>
<tr>
<td>CSCuv69535</td>
<td>Graphical User Interface (GUI) access to IR829 AP is broken</td>
</tr>
<tr>
<td>CSCut54776</td>
<td>Invalid value returned for walk, cLIpv6AclCounterClear</td>
</tr>
<tr>
<td>CSCuw99278</td>
<td>Air Time Fairness (ATF) Policy id range mis-match is seen in Cisco WLC CLI and GUI</td>
</tr>
<tr>
<td>CSCun52472</td>
<td>“show dtls connection” shows blank in Access Point Name column for Capwap_Data</td>
</tr>
<tr>
<td>CSCus50404</td>
<td>Access Point Name is mismatched between Controller and Access Point</td>
</tr>
<tr>
<td>CSCut97161</td>
<td>Static IPv6 Config on Access Point does not take effect, need to reboot Access Point</td>
</tr>
<tr>
<td>CSCur98573</td>
<td>Memory increase on Datagram Transport Layer Security (DTLS) connections is seen when &gt;500 APs join 5508 WLC</td>
</tr>
<tr>
<td>CSCuv97132</td>
<td>Show Access Point image all output will not fetch spamPreDownloadInProgress</td>
</tr>
<tr>
<td>CSCuu48845</td>
<td>Simple Network Management Protocol (SNMP) Error thrown when IPv4 static IP is set for AP</td>
</tr>
<tr>
<td>CSCuw59579</td>
<td>Simple Network Management Protocol (SNMP): returns reversed DNS IP address when configured from Prime</td>
</tr>
<tr>
<td>CSCuu51641</td>
<td>WiSM2: ‘config ap tcp-mss-adjust enable all 1363’ is missing in High Availability (HA) configuration.</td>
</tr>
<tr>
<td>CSCuu88193</td>
<td>Wrong info shown on controller with no crash file in Access Point core</td>
</tr>
<tr>
<td>CSCut78949</td>
<td>XML validation error is seen while downloading configuration</td>
</tr>
<tr>
<td>CSCuw06127</td>
<td>Silent crash in 8.0.120 is seen due to memory leak in Cisco Discovery Protocol (CDP) Main</td>
</tr>
</tbody>
</table>
### Caveats

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuw09545</td>
<td>Incorrect DHCP “Pool Usage” on the Cisco WLC when queried via Simple Network Management Protocol (SNMP)</td>
</tr>
<tr>
<td>CSCut24658</td>
<td>Option 82 remote-id attribute “apname-vlan_id” information is not shown</td>
</tr>
<tr>
<td>CSCuu99344</td>
<td>Cisco WLC unexpectedly reloads Dynamic Host Configuration Protocol (DHCP) packet content while on new mobility</td>
</tr>
<tr>
<td>CSCus86831</td>
<td>Cisco WLC uses old Access Point-Group name in Ethernet over GRE (EoGRE) DHCP option 82</td>
</tr>
<tr>
<td>CSCut37572</td>
<td>“show ap eogre” displays status for LOCAL mode Access Point</td>
</tr>
<tr>
<td>CSCut76523</td>
<td>Access Point should drop client data traffic when Access Point sends Internet Control Message Protocol (ICMP) error message to client</td>
</tr>
<tr>
<td>CSCux07616</td>
<td>Client cannot get Dynamic Host Configuration Protocol (DHCP) over Ethernet over GRE (EoGRE) when Dynamic Host Configuration Protocol (DHCP) required is enabled on Wireless Local Area Network (WLAN)</td>
</tr>
<tr>
<td>CSCut47494</td>
<td>Client is unable to join in Local switching Open Wireless Local Area Network (WLAN) with Local mode Access Point</td>
</tr>
<tr>
<td>CSCut44073</td>
<td>Ethernet over GRE (EoGRE) static Profile Name is not displayed in Cisco WLC traplog it displays empty</td>
</tr>
<tr>
<td>CSCut47036</td>
<td>Ethernet over GRE (EoGRE): Access Point current active gateway/gateway status is not synced to standby</td>
</tr>
<tr>
<td>CSCuu07760</td>
<td>Ethernet over GRE (EoGRE): Need warning message when * is configured</td>
</tr>
<tr>
<td>CSCuv34973</td>
<td>Fast SSID switching causes SIMPLE IP to be treated as a Ethernet over GRE (EoGRE) client</td>
</tr>
<tr>
<td>CSCut78696</td>
<td>Show run-config commands shows the Ethernet over GRE (EoGRE) Show commands</td>
</tr>
<tr>
<td>CSCuu17340</td>
<td>Cisco WLC unexpected reload on Tunnel Process Task is seen while adding gateway name 129 max character from UI</td>
</tr>
<tr>
<td>CSCus68335</td>
<td>Cisco WLC: Deletes the command config Access Point Ethernet duplex in full speed</td>
</tr>
<tr>
<td>CSCuw63311</td>
<td>Increased Ping latency &amp; Reduced traffic is seen on 8510</td>
</tr>
<tr>
<td>CSCuw24476</td>
<td>Increased Ping latency &amp; Reduced traffic is seen on 8510 with Quality of service (QoS) rate limiting</td>
</tr>
<tr>
<td>CSCuw12544</td>
<td>Rate-limiting is causing 500ms gap of traffic when roaming</td>
</tr>
<tr>
<td>CSCuv30948</td>
<td>Local Net Users is not saved in config backup</td>
</tr>
<tr>
<td>CSCuu12045</td>
<td>Mobility media access control (MAC) configuration should not be uploaded in the configuration file</td>
</tr>
<tr>
<td>CSCuu71471</td>
<td>Maximum Transmission Unit (MTU) value stacks in High Availability (HA)</td>
</tr>
<tr>
<td>CSCuu83548</td>
<td>Traceback observed in export-foreign standby Cisco WLC while disassociating client</td>
</tr>
<tr>
<td>CSCuu13860</td>
<td>'autoconvert flexconnect' is stored as 'disable' on startup-commands</td>
</tr>
<tr>
<td>CSCut61668</td>
<td>Application Identifiers (AID) errors is seen on the controller for Flexconnect Access Points</td>
</tr>
</tbody>
</table>

**Table 12**  Resolved Caveats (continued)
### Caveats

CSCuu07274 BGL-Alpha: “FP0.00:failed to find scb” error prints at 5500 standby console

CSCut57138 BGL-Alpha: The system has failed decoding vendor specific payload

CSCuu11959 Cisco 7925 phone using Cisco Centralized Key Management (CCKM) does not roam gracefully in FlexConnect environment.

CSCus30338 Clients with Static IP gets authenticated for Dynamic Host Configuration Protocol (DHCP) Required wireless local area network (WLAN)

CSCut60058 CTRLR does not deauthenticate clients when AAA Flex-ACL is not present on Access Point

CSCuu93296 Extensible Authentication Protocol Transport Layer Security (EAP-TLS) loosing device certificate in standalone mode after reboot

CSCuu43770 Flex connect Central-DHCP Values is not getting applied to Flex Connect Access Points

CSCuw31813 Flex Local Auth, client roaming in-out-in during dot1x

CSCuu80153 Flex Analog Voice Channel (AVC) unable to update rate limit value

CSCut55043 FlexConnect Group with space in name renders terminal session unusable

CSCut68635 FT- Username is not getting updated in standby. Access VLAN is not updated in active

CSCur40277 High traffic loss is seen for Flex Access Point clients once CAPWAP tunnel is re-established

CSCuu07744 Interface not created when we have both Access Control List (ACL) and WLAN-VLAN mapping

CSCuu89294 Primary Access Point in Flex Group is not saved in Cisco WLC cfg nor commands backup

CSCuu87832 Mobility Express: Client not moving to exclude state after association failure

CSCut81484 TB observed on Access Point when we have more number of rules on 8500

CSCuu72585 When Access Point in flexconnect mode, Cisco WLC AAA override occurs causing traffic Blackholing

CSCut10131 Cisco WLC fails to resend ciscoLwappDot11ClientMovedToRunState traps

CSCuv20940 Client fails to ping IPv6 gateway, clients with High Availability (HA) switchover

CSCut40919 Configuration download fails via service port using IPv6 addressing.

CSCuu08592 Override Interface-Interface group not applied on reauthentication for IPv6 clients

CSCuu72081 Cisco WLC: IPV6-3-CREATE_BINDING_FAILED error gets flooded

CSCuw13264 IPv6-3-CREATE_BINDING_FAILED error gets flooded

CSCuv27120 Cannot configure IP address x.x.x.255 or x.x.x.0 as gateway is seen.

CSCuw35349 Dynamic Host Configuration Protocol (DHCP) registration keeps failing when mask from Cisco WLC interface does not match client received mask

CSCuu51747 Dynamic Interface accepts name as empty string in Cisco WLC CLI

### Table 12 Resolved Caveats (continued)

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCu07274</td>
<td>BGL-Alpha: “FP0.00:failed to find scb” error prints at 5500 standby console</td>
</tr>
<tr>
<td>CSCut57138</td>
<td>BGL-Alpha: The system has failed decoding vendor specific payload</td>
</tr>
<tr>
<td>CSCuu11959</td>
<td>Cisco 7925 phone using Cisco Centralized Key Management (CCKM) does not roam gracefully in FlexConnect environment.</td>
</tr>
<tr>
<td>CSCus30338</td>
<td>Clients with Static IP gets authenticated for Dynamic Host Configuration Protocol (DHCP) Required wireless local area network (WLAN)</td>
</tr>
<tr>
<td>CSCut60058</td>
<td>CTRLR does not deauthenticate clients when AAA Flex-ACL is not present on Access Point</td>
</tr>
<tr>
<td>CSCuu93296</td>
<td>Extensible Authentication Protocol Transport Layer Security (EAP-TLS) loosing device certificate in standalone mode after reboot</td>
</tr>
<tr>
<td>CSCuu43770</td>
<td>Flex connect Central-DHCP Values is not getting applied to Flex Connect Access Points</td>
</tr>
<tr>
<td>CSCuw31813</td>
<td>Flex Local Auth, client roaming in-out-in during dot1x</td>
</tr>
<tr>
<td>CSCuu80153</td>
<td>Flex Analog Voice Channel (AVC) unable to update rate limit value</td>
</tr>
<tr>
<td>CSCut55043</td>
<td>FlexConnect Group with space in name renders terminal session unusable</td>
</tr>
<tr>
<td>CSCut68635</td>
<td>FT- Username is not getting updated in standby. Access VLAN is not updated in active</td>
</tr>
<tr>
<td>CSCur40277</td>
<td>High traffic loss is seen for Flex Access Point clients once CAPWAP tunnel is re-established</td>
</tr>
<tr>
<td>CSCuu07744</td>
<td>Interface not created when we have both Access Control List (ACL) and WLAN-VLAN mapping</td>
</tr>
<tr>
<td>CSCuu89294</td>
<td>Primary Access Point in Flex Group is not saved in Cisco WLC cfg nor commands backup</td>
</tr>
<tr>
<td>CSCuu87832</td>
<td>Mobility Express: Client not moving to exclude state after association failure</td>
</tr>
<tr>
<td>CSCut81484</td>
<td>TB observed on Access Point when we have more number of rules on 8500</td>
</tr>
<tr>
<td>CSCuu72585</td>
<td>When Access Point in flexconnect mode, Cisco WLC AAA override occurs causing traffic Blackholing</td>
</tr>
<tr>
<td>CSCut10131</td>
<td>Cisco WLC fails to resend ciscoLwappDot11ClientMovedToRunState traps</td>
</tr>
<tr>
<td>CSCuv20940</td>
<td>Client fails to ping IPv6 gateway, clients with High Availability (HA) switchover</td>
</tr>
<tr>
<td>CSCut40919</td>
<td>Configuration download fails via service port using IPv6 addressing.</td>
</tr>
<tr>
<td>CSCuu08592</td>
<td>Override Interface-Interface group not applied on reauthentication for IPv6 clients</td>
</tr>
<tr>
<td>CSCuu07107</td>
<td>Simple Network Management Protocol (SNMP) walk on clsNetworkRouteConfigTable fails</td>
</tr>
<tr>
<td>CSCut72081</td>
<td>Cisco WLC: IPV6-3-CREATE_BINDING_FAILED error gets flooded</td>
</tr>
<tr>
<td>CSCuw13264</td>
<td>IPv6-3-CREATE_BINDING_FAILED error gets flooded</td>
</tr>
<tr>
<td>CSCuv27120</td>
<td>Cannot configure IP address x.x.x.255 or x.x.x.0 as gateway is seen.</td>
</tr>
<tr>
<td>CSCuw35349</td>
<td>Dynamic Host Configuration Protocol (DHCP) registration keeps failing when mask from Cisco WLC interface does not match client received mask</td>
</tr>
<tr>
<td>CSCuu51747</td>
<td>Dynamic Interface accepts name as empty string in Cisco WLC CLI</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCu04464</td>
<td>License command causes Cisco WLC unexpected reload (possible buffer size overwrite)</td>
</tr>
<tr>
<td>CSCu98217</td>
<td>VSRE While upgrade from 8.0 to 8.1 Lic End User License Agreement (EULA) is changed to not accepted</td>
</tr>
<tr>
<td>CSCu90165</td>
<td>Calibration debugs not available</td>
</tr>
<tr>
<td>CSCu58800</td>
<td>S60 Payload mismatch (PLM) Path Loss Measurement should be disabled by default</td>
</tr>
<tr>
<td>CSCuw34311</td>
<td>Cisco WLC drops Received Signal Strength Indicator (RSSI) reporting with Fast locate feature</td>
</tr>
<tr>
<td>CSCu99533</td>
<td>Lync: Old history calls are not getting deleted once we reach max.</td>
</tr>
<tr>
<td>CSCu03329</td>
<td>Simple Network Management Protocol (SNMP) Get is not fetching latest value for port, protocol &amp; status</td>
</tr>
<tr>
<td>CSCu37414</td>
<td>CI: Jian High Availability (HA) has Trivial File Transfer Protocol (TFTP) failure while storing on flash error</td>
</tr>
<tr>
<td>CSCuv87458</td>
<td>“show mesh config” doesn’t show mesh CA status when Carrier Access Codes (CAC) is enabled.</td>
</tr>
<tr>
<td>CSCu65562</td>
<td>8.1.14.13 - Subset channel isn't removed after channel change</td>
</tr>
<tr>
<td>CSCu97385</td>
<td>Access Point name chopped for “show mesh cac access (long AP name)”</td>
</tr>
<tr>
<td>CSCu91086</td>
<td>Client associated to Mobile Application Part (MAP) doesn’t get AAA override in Flex+Bridge mode</td>
</tr>
<tr>
<td>CSCuv76883</td>
<td>Error inconsistent to Ethernet state when change mode “bridge“ -&gt; “local”</td>
</tr>
<tr>
<td>CSCu77412</td>
<td>High memory usage from mesh-msg_task due to weird Bridge Group Name present</td>
</tr>
<tr>
<td>CSCu05488</td>
<td>Inconsistent/incorrect backhaul info/missing a channel for Radio frequency (RF) used</td>
</tr>
<tr>
<td>CSCu37465</td>
<td>Incorrect “AP MAC” in the response of “show mesh stats &lt;AP Name&gt;”</td>
</tr>
<tr>
<td>CSCu96201</td>
<td>Invalid characters shown on the Bridge Group Name</td>
</tr>
<tr>
<td>CSCu48172</td>
<td>Locally Significant Certificate (LSC) Access Point provisioning happening after Mobile Application Part (MAP) is disconnected for long time</td>
</tr>
<tr>
<td>CSCuv16895</td>
<td>Mobile Application Part (MAP) count is shown wrongly in “show mesh ap summary” command in Cisco WLC CLI</td>
</tr>
<tr>
<td>CSCu38592</td>
<td>Mesh Backhaul shows up as “auto” instead of actual data rate</td>
</tr>
<tr>
<td>CSCu72171</td>
<td>No response “config mesh link data &lt;AP name&gt;” non-mesh or mesh Access Point</td>
</tr>
<tr>
<td>CSCu04864</td>
<td>No response of “show mesh as tools stats” or with Cisco Access Point name</td>
</tr>
<tr>
<td>CSCu55891</td>
<td>Non-mesh Access Points not detected for “show mesh queue-stats AP name” and “all”</td>
</tr>
<tr>
<td>CSCu59340</td>
<td>Signal-to-Noise Ratio (SNR) alarms for mesh APs have invalid content, is not working as expected</td>
</tr>
<tr>
<td>CSCu60912</td>
<td>Virtual LAN (VLAN) Support check or uncheck no updated in “Mesh” bar after Apply</td>
</tr>
<tr>
<td>CSCu85294</td>
<td>Cisco WLC CLI “show mesh neigh detail” command showing unreasonable years</td>
</tr>
</tbody>
</table>
### Table 12  Resolved Caveats (continued)

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuw31820</td>
<td>Cisco WLC Consolidation Point unexpected reload is seen due to System unexpected reload for apfMsConnTask_6</td>
</tr>
<tr>
<td>CSCut92776</td>
<td>Configuration mobility group does not accept 24th member in case of IPv6</td>
</tr>
<tr>
<td>CSCuv43484</td>
<td>Device is switching to Multiple Access (MA) mode after mobility new-architecture enable</td>
</tr>
<tr>
<td>CSCut42569</td>
<td>GA: Client is not anchored after changing export anchor config on wireless local area network (WLAN)</td>
</tr>
<tr>
<td>CSCuu26369</td>
<td>Message “Handoff 802.1x PEM state “is not filtered by debug client</td>
</tr>
<tr>
<td>CSCuv85747</td>
<td>Mobility Member entries going stale</td>
</tr>
<tr>
<td>CSCuv83941</td>
<td>8510: Error enabling global multicast with CAPWAP mode unicast</td>
</tr>
<tr>
<td>CSCuw50324</td>
<td>Unexpected reload seen on high CPU usage</td>
</tr>
<tr>
<td>CSCut88319</td>
<td>FF08:/16 range of organization-local IPv6 multicast addresses</td>
</tr>
<tr>
<td>CSCuv22052</td>
<td>Link local multicast control traffic sent by Access Points, Internet Group Management Protocol (IGMP) Snooping Enabled</td>
</tr>
<tr>
<td>CSCuv43125</td>
<td>mdnsQueryDelayHandler tracebacks in 8.0 WLC flooding syslog server</td>
</tr>
<tr>
<td>CSCuu10781</td>
<td>Multicast configuration mismatch on Web / CLI</td>
</tr>
<tr>
<td>CSCut36686</td>
<td>FlexAVC: 8.1.10.201 WLAN ID displayed incorrect on Access Point</td>
</tr>
<tr>
<td>CSCut63331</td>
<td>FlexAVC - not able to change value of marking once configured</td>
</tr>
<tr>
<td>CSCut48743</td>
<td>FlexAVC - policy-map not getting deleted/added when Access Point is in AP group</td>
</tr>
<tr>
<td>CSCut39707</td>
<td>FlexAVC profile should not show about not supported WLANs</td>
</tr>
<tr>
<td>CSCut85185</td>
<td>FlexAVC-WLAN_specific mapping is not pushing to Access Point</td>
</tr>
<tr>
<td>CSCuu91001</td>
<td>NetFlow record sent without client IP address</td>
</tr>
<tr>
<td>CSCut70083</td>
<td>show run-config command is not showing FlexAVC rules</td>
</tr>
<tr>
<td>CSCuw39667</td>
<td>WiSM2 unexpected reload/rebooting on task emWeb</td>
</tr>
<tr>
<td>CSCut45024</td>
<td>Cisco WLC showing 0 as application in FlexAVC stats</td>
</tr>
<tr>
<td>CSCuv86494</td>
<td>Cisco WLC clears Access Point MAC before deleting client, sends NetFlow with Zero AP MAC</td>
</tr>
<tr>
<td>CSCuu28666</td>
<td>BGI-Alpha: SNTP-3-SOCK_OPT_FAILED: Failed to set the socket option</td>
</tr>
<tr>
<td>CSCus97953</td>
<td>8510 Silent unexpected reload seen- Uhhuh. NMI received for unknown reason 2d</td>
</tr>
<tr>
<td>CSCuw28246</td>
<td>CT8540 / CT5520 dose not detect power supply cable failure</td>
</tr>
<tr>
<td>CSCuu16052</td>
<td>Does not set DF bit for non-CAPWAP traffic from Cisco WLC such as RADIUS</td>
</tr>
<tr>
<td>CSCut26363</td>
<td>GUI and telnet very slow, almost unresponsive</td>
</tr>
<tr>
<td>CSCuw03414</td>
<td>WiSM2 8.0.102.0 unexpected reload on apfMsConnTask_2 reason “System Crash”</td>
</tr>
<tr>
<td>CSCuv79793</td>
<td>Cisco WLC is leaking packets from virtual IP onto Local Area Network (LAN)</td>
</tr>
<tr>
<td>CSCuv01337</td>
<td>“config pmipv6 add profile” error not clear when profile length&gt;32</td>
</tr>
<tr>
<td>CSCut74263</td>
<td>Mobile Access Gateway (MAG) on Access Point: Access Point does not clear bindings after session/user timeout &amp; deauth</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSCut64180</td>
<td>Access Point holds BW after call when Cisco WLC High Availability SO happens during call setup</td>
</tr>
<tr>
<td>CSCuw21213</td>
<td>Downstream: QoS Bronze Profile not marking traffic to AF11 on Flex</td>
</tr>
<tr>
<td>CSCut96390</td>
<td>Inconsistent counter behavior of Signalling Connection Control Part (SCCP) call when Address complete message (ACM) is not enabled</td>
</tr>
<tr>
<td>CSCuu96349</td>
<td>QosMap shows pre-configured values after upgrade from 8.1 CCO</td>
</tr>
<tr>
<td>CSCu20097</td>
<td>Token Bucket leak is seen when QoS Roles is setup and when working with WebAuth</td>
</tr>
<tr>
<td>CSCuv88984</td>
<td>“show ap universal summary” CLI dos not exist</td>
</tr>
<tr>
<td>CSCu07817</td>
<td>Access Point is not detecting Rogues when joined to controller in IPv6 pref. mode</td>
</tr>
<tr>
<td>CSCuv34472</td>
<td>Longevity: Ambassador in longevity unexpectedly reloads with Task:Emweb in 8.1.104.38</td>
</tr>
<tr>
<td>CSCuw38795</td>
<td>5508 Cisco WLC unexpected reloads upon pushing RF calibration template from PI</td>
</tr>
<tr>
<td>CSCuw38022</td>
<td>8510 Simple Network Management Protocol (SNMP) Agent reverses octet order of clrRrmPakRssiNtp object</td>
</tr>
<tr>
<td>CSCut32955</td>
<td>a-mpdu tx priority command missing from backup config</td>
</tr>
<tr>
<td>CSCut59663</td>
<td>Add channels 100-140 as default in 11a</td>
</tr>
<tr>
<td>CSCuu43603</td>
<td>Channel assignment leader IPv4 address not showing.</td>
</tr>
<tr>
<td>CSCus79791</td>
<td>Client connected to 11n Access Point shows as 11ac client on Cisco WLC</td>
</tr>
<tr>
<td>CSCuu80383</td>
<td>Clients is denied association by neighbor Access Point during optimized roaming</td>
</tr>
<tr>
<td>CSCut23857</td>
<td>Issues of a Access Point in Radios 802.11a/n/ac from Global mode to Custom mode</td>
</tr>
<tr>
<td>CSCuu71487</td>
<td>Minimum users is sometimes selected incorrectly</td>
</tr>
<tr>
<td>CSCut59679</td>
<td>Modify output of sh run-config, to reduce duplicate info on Access Points</td>
</tr>
<tr>
<td>CSCuw56127</td>
<td>Need to re-evaluate Tunisia for –I radio types</td>
</tr>
<tr>
<td>CSCuv67144</td>
<td>Need to re-evaluate Algeria if in –E or –I</td>
</tr>
<tr>
<td>CSCuw27160</td>
<td>RF Grouping Algorithm &gt; update interval NOT synchronized on controllers</td>
</tr>
<tr>
<td>CSCuu14124</td>
<td>RF-profile losing the channel and coverage values after downloading configuration file</td>
</tr>
<tr>
<td>CSCuv96996</td>
<td>Radio Resource Management (RRM) setting 24 channel width to 40, leading to CleanAir crash</td>
</tr>
<tr>
<td>CSCuu42378</td>
<td>RX-SOP threshold not working correctly</td>
</tr>
<tr>
<td>CSCut27056</td>
<td>Traplog message for radar Clear event needs correction</td>
</tr>
<tr>
<td>CSCuw79951</td>
<td>Unable to disable Assisted Roaming or Load Balancing through CLI</td>
</tr>
<tr>
<td>CSCuw62850</td>
<td>WiSM2 8.0.120.5 unexpected reload. mwar_ms_deadlock.crash</td>
</tr>
<tr>
<td>CSCuw33715</td>
<td>Cisco WLC unexpected reload on 11k processing is seen</td>
</tr>
<tr>
<td>CSCuw66299</td>
<td>Cisco WLC msglog showing NMSP Transmit Failure even when there is no MSE</td>
</tr>
<tr>
<td>CSCur40006</td>
<td>Cisco WLC: Group size exceeded with static RF Group member add</td>
</tr>
<tr>
<td>CSCuv08631</td>
<td>“Failed to add new AP Group: test” misleading when max Access Point Group hit</td>
</tr>
<tr>
<td>CSCut10882</td>
<td>11r clients not moving L2authentication to Run state on Cisco WLC</td>
</tr>
</tbody>
</table>
### Table 12  Resolved Caveats (continued)

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuw48488</td>
<td>4-way handshake fails on 11r+11w (FT+PMF) Wireless Local Area Network (WLAN)</td>
</tr>
<tr>
<td>CSCuv36505</td>
<td>8.0 Cisco WLC messages flooding CLI after debug client</td>
</tr>
<tr>
<td>CSCut90276</td>
<td>AireOS Traceback: APF-4-PROC_ACTION_FAILED</td>
</tr>
<tr>
<td>CSCut86986</td>
<td>Audit-session-id not learned correctly during L3 roam-Radius Network Access Control (NAC0 disable)</td>
</tr>
<tr>
<td>CSCut71612</td>
<td>OUI string should be synced across High Availability (HA)</td>
</tr>
<tr>
<td>CSCuv40033</td>
<td>Cisco WLC IPv6 IAPP WIPS Report Vulnerability</td>
</tr>
<tr>
<td>CSCuw62172</td>
<td>Unexpected reload seen on High Availability (HA) standby while setting Auth-priority order from Prime Infrastructure in 7.6</td>
</tr>
<tr>
<td>CSCut02524</td>
<td>Default NAS-ID value at the AP-Groups should be empty or “none”</td>
</tr>
<tr>
<td>CSCus61445</td>
<td>Domain Name System (DNS) Access Control List (ACL) on WLC is not working - Access Point not Send DTLS to Cisco WLC</td>
</tr>
<tr>
<td>CSCuu07700</td>
<td>Extensible Authentication Protocol (EAP) Packet does not get encrypted in Re-Auth request from client</td>
</tr>
<tr>
<td>CSCuw91763</td>
<td>Feature “AES Key Wrap” does not work</td>
</tr>
<tr>
<td>CSCus92667</td>
<td>GET on Access Point groups Table after set - response missing</td>
</tr>
<tr>
<td>CSCuw35341</td>
<td>IP address lost on AAA override+multiple subnetworks per vlan+DHCP req</td>
</tr>
<tr>
<td>CSCut45010</td>
<td>Issue with installing certs in Universal Time (UTC)</td>
</tr>
<tr>
<td>CSCuu66675</td>
<td>Lock unexpected reload is seen on RADIUS Transport Thread during CMCC External Auth</td>
</tr>
<tr>
<td>CSCut29535</td>
<td>Not able to remove domain name system, configured radius server.</td>
</tr>
<tr>
<td>CSCuv90333</td>
<td>afpmsConntask floods when running client console debug</td>
</tr>
<tr>
<td>CSCuu51713</td>
<td>RADIUS and Accounting Fall back does not work properly</td>
</tr>
<tr>
<td>CSCuu62544</td>
<td>RFC 3576 - Disconnect MSG not handled with WLC</td>
</tr>
<tr>
<td>CSCuu08752</td>
<td>Service Exchange Platform (SXP) unexpectedly reloads when running Trust Sec clients is seen</td>
</tr>
<tr>
<td>CSCuu15866</td>
<td>Unexpected Local Extensible Authentication Protocol (EAP) authentication termination.</td>
</tr>
<tr>
<td>CSCuu36172</td>
<td>Venue Name max takes 253 vs. CLI 200 characters for AP</td>
</tr>
<tr>
<td>CSCut92934</td>
<td>Cisco VWLC - Access Point with expire Mic not able to join with Ignore Mic settings</td>
</tr>
<tr>
<td>CSCuv97793</td>
<td>WiSM2 unexpected reload AP_DB_CREATE_ERR Message queue MFP-Q is nearing full</td>
</tr>
<tr>
<td>CSCuw82711</td>
<td>Cisco WLC 5508 8.1.111.0. RFC-3576 Disconnect-Request not heard from port 3799</td>
</tr>
<tr>
<td>CSCuq73590</td>
<td>Cisco WLC adds incorrect class attribute in accounting stop</td>
</tr>
<tr>
<td>CSCut08222</td>
<td>Cisco WLC local policy behavior is abnormal</td>
</tr>
<tr>
<td>CSCuw16295</td>
<td>Cisco WLC show boot shows backup image as Error failing to read linux.bak.img</td>
</tr>
</tbody>
</table>
### Caveats

Table 12  
**Resolved Caveats (continued)**

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuw89581</td>
<td>Cisco WLC System unexpected reload on apfReceiveTask</td>
</tr>
<tr>
<td>CSCuv04058</td>
<td>Error is seen while trying to change the default trap receiver port.</td>
</tr>
<tr>
<td>CSCuw26629</td>
<td>Management Information Base (MIB) message of Power supply Status on 7500 is wrong</td>
</tr>
<tr>
<td>CSCut57471</td>
<td>Simple Network Management Protocol (SNMP) Interface Management Information Base (MIB) on 5520 is wrong</td>
</tr>
<tr>
<td>CSCuu64447</td>
<td>CleanAir device commands become disabled after restoring backup config</td>
</tr>
<tr>
<td>CSCuv43466</td>
<td>Garbage character are shown in CLI “show run-config startup-command”</td>
</tr>
<tr>
<td>CSCuu24064</td>
<td>Simple Network Management Protocol (SNMP): cLApUniversalPrimeStatus not returning for all APs</td>
</tr>
<tr>
<td>CSCuv55994</td>
<td>“Error in adding VLAN Map” popped up when VLAN ID is out of range</td>
</tr>
<tr>
<td>CSCuu97320</td>
<td>“Flex+Bridge&amp;SE-Connect” filtering back to uncheck after “Change Filter”</td>
</tr>
<tr>
<td>CSCuv65301</td>
<td>“WLAN SSID” popped up when invalid or unsupported IPv6 in server address</td>
</tr>
<tr>
<td>CSCuw34565</td>
<td>7500 Cisco WLC unexpected after deleting Access Point crash logs from GUI</td>
</tr>
<tr>
<td>CSCuv47252</td>
<td>Access point RF Troubleshoot legend issue is seen for channel</td>
</tr>
<tr>
<td>CSCuw97240</td>
<td>Access Control list (ACL) Rule: Adding Destination. port as HTTPS is not working</td>
</tr>
<tr>
<td>CSCuu08387</td>
<td>AQ graph shown twice in drop down of interference devices in Cisco WLC GUI</td>
</tr>
<tr>
<td>CSCut67169</td>
<td>Bridge data rates are not shown for 1572 Access Points in controller GUI</td>
</tr>
<tr>
<td>CSCuv79354</td>
<td>Cannot configure IP address x.x.x.255 or x.x.x.0 as gateway in GUI</td>
</tr>
<tr>
<td>CSCut81543</td>
<td>Click “Back” does not go back to filtered Access Points after going to an AP page for RADIUS</td>
</tr>
<tr>
<td>CSCut58777</td>
<td>Cisco WLC GUI does not have options to configure 2.4GHz HT Rates</td>
</tr>
<tr>
<td>CSCuw26377</td>
<td>Unexpected reload seen due to invalid form field validation on switch_cfg_rw.html</td>
</tr>
<tr>
<td>CSCur39649</td>
<td>Unexpected reload seen on /screens/base/tunnel_gtpv2Cfg.html</td>
</tr>
<tr>
<td>CSCuv18734</td>
<td>Dialogue message missing when Client “Removed” from Cisco WLC5500</td>
</tr>
<tr>
<td>CSCut15677</td>
<td>DS/US Channels are empty for CM Statistic on Cisco WLC GUI for AP/CM</td>
</tr>
<tr>
<td>CSCuw78528</td>
<td>Flex group name is missing when refresh flex Access Point’s wlan-acv mapping page</td>
</tr>
<tr>
<td>CSCus80870</td>
<td>GUI: Observed popup error message when disabling the Protected Management Frames (PMF) in WLAN</td>
</tr>
<tr>
<td>CSCut60950</td>
<td>Inconsistent errors seen during setup unsupported channel procedure on 40MHz/80MHz</td>
</tr>
<tr>
<td>CSCuu19563</td>
<td>Incorrect pop message seen in GUI 802.11 coverage</td>
</tr>
<tr>
<td>CSCuv44023</td>
<td>Local policy name with UTF-8 character is showing as junk in edit page</td>
</tr>
<tr>
<td>CSCuw51155</td>
<td>Mobility Express UI: Overwrites some Wireless Local Area Network (WLAN) config when edited from UI</td>
</tr>
<tr>
<td>CSCuv79155</td>
<td>Mismatch in config for Address Resolution Protocol (ARP) Timeout value in Cisco WLC CLI and GUI</td>
</tr>
<tr>
<td>CSCuv29025</td>
<td>Mobility domain name is displayed as Junk if created in UTF-8 character</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSCuu95889</td>
<td>Mobility Group without MAC “Error in creating Member” improperly popped</td>
</tr>
<tr>
<td>CSCuv07657</td>
<td>Monitor page does not support Session timeout in VWLC</td>
</tr>
<tr>
<td>CSCut62786</td>
<td>Native VLAN id textbox missing in webUI</td>
</tr>
<tr>
<td>CSCuu61286</td>
<td>No error displayed but silently quit for “Power Injector State” is seen.</td>
</tr>
<tr>
<td>CSCuur50538</td>
<td>No pop-up shown when affected channels field is selected without any i/p</td>
</tr>
<tr>
<td>CSCuu42415</td>
<td>Non-realistic 102% or 120% displayed for Interference Impact</td>
</tr>
<tr>
<td>CSCux03140</td>
<td>Not able to add valid Phase-Shift Keying (PSK) key from GUI</td>
</tr>
<tr>
<td>CSCuu23237</td>
<td>Parameters got expanded when clicking back button in Best Practices page</td>
</tr>
<tr>
<td>CSCuv96333</td>
<td>Read only user able to change “Telnet Capability” setting</td>
</tr>
<tr>
<td>CSCuw73215</td>
<td>RF profile&gt; coverage, exception clients range differs in Cisco WLC GUI and CLI</td>
</tr>
<tr>
<td>CSCuu14734</td>
<td>RFDB: Client Performance: client connections: size and position of donuts vary</td>
</tr>
<tr>
<td>CSCuw02258</td>
<td>Severity Filter for Monitoring CleanAir Interferer's does not work</td>
</tr>
<tr>
<td>CSCut95326</td>
<td>Showing access-VLAN when client is in Quarantine state in GUI-flexmodeAP</td>
</tr>
<tr>
<td>CSCuu11129</td>
<td>Switching from 2.4 G to 5G, the proposed high-chart disappeared on Safari</td>
</tr>
<tr>
<td>CSCuu88339</td>
<td>Unable to configure Central DHCP Flex+Mesh/Flexconnect WLAN from WLC GUI</td>
</tr>
<tr>
<td>CSCut63507</td>
<td>Cisco VWLC showing application ID instead of application name</td>
</tr>
<tr>
<td>CSCuv79867</td>
<td>WLAN GUI: WLAN edit can't accept 20 characters password for Phase-Shift Keying (PSK)</td>
</tr>
<tr>
<td>CSCuu33740</td>
<td>Cisco WLC unexpectedly reloads while editing SNMP community - waFormSubmit_snmp_comm_list</td>
</tr>
<tr>
<td>CSCut79304</td>
<td>Cisco WLC GUI is throwing error for DSCP marking</td>
</tr>
<tr>
<td>CSCuv12875</td>
<td>Cisco WLC Spartan: 802.11ac Max Capability issue for all Access Point</td>
</tr>
<tr>
<td>CSCut44986</td>
<td>Cisco WLC is throwing error when accounting is disabled on WLAN</td>
</tr>
<tr>
<td>CSCus77368</td>
<td>Cisco WLC: Unexpected reload ewaFormSubmit_cell_edit</td>
</tr>
<tr>
<td>CSCuu66484</td>
<td>Cisco WLC: GUI 'downloaded AVP' page just keeps reloading</td>
</tr>
<tr>
<td>CSCut81459</td>
<td>Cisco WLC: Noise of OFF Access Points shows as blank or as ()</td>
</tr>
<tr>
<td>CSCux03108</td>
<td>8510 Unexpected reload on Task Name:portalMsgTask.</td>
</tr>
<tr>
<td>CSCur94843</td>
<td>External web Auth URL goes through loop and never gets to the Login page</td>
</tr>
<tr>
<td>CSCuv25826</td>
<td>Disabling, mDNS profile on all wireless local area networks (WLAN) throws wrong error msg</td>
</tr>
<tr>
<td>CSCuu51728</td>
<td>Enabled UniversalAPAdminMode in wireless local area network (WLAN) gets disabled after config transfer</td>
</tr>
<tr>
<td>CSCur88123</td>
<td>Invalid Phase-Shift Keying (PSK) for layer 2 security after controller reboot</td>
</tr>
<tr>
<td>CSCuu39294</td>
<td>mDNS snooping is not disabling when flex local switching is enabled</td>
</tr>
<tr>
<td>CSCut62944</td>
<td>Mismatch between show run-config commands and device configurations for Cisco WLC</td>
</tr>
<tr>
<td>CSCuu16348</td>
<td>Oeap600 RLAN 'quiet' wired clients timing out</td>
</tr>
</tbody>
</table>
### Resolved Caveats (continued)

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuw90458</td>
<td>Prime Infrastructure 3.0 does not properly push template for wireless local area network (WLAN) i</td>
</tr>
<tr>
<td>CSCuw31595</td>
<td>Bogus line in show run-config commands output is seen</td>
</tr>
<tr>
<td>CSCuu77738</td>
<td>Prime 3.0 Auto Provisioning is not working</td>
</tr>
<tr>
<td>CSCuw29532</td>
<td>CAPWAP to Mobility Express conversion: shows incomplete cmd when image download not required</td>
</tr>
<tr>
<td>CSCuw12525</td>
<td>Simple Network Management Protocol (SNMP) get on system Temperature attribute returns 5000 on Mobility Express Cisco WLC</td>
</tr>
<tr>
<td>CSCut40305</td>
<td>Console logs are creating during AP-GUI login session and PSE status</td>
</tr>
<tr>
<td>CSCuw03323</td>
<td>Cisco AP702w draws additional power (22.1 watts) when LAN port 4 is disabled</td>
</tr>
</tbody>
</table>
The Cisco Mobility Express wireless network solution is available starting from Cisco Wireless Release 8.1.122.0.

The Cisco Mobility Express wireless network solution provides a wireless LAN controller functionality bundled into, the Cisco Aironet 1850 and 1830 Series APs currently. This functionality provides a simplified Wi-Fi architecture with limited enterprise-level WLAN capability to small and medium deployments.

In the Cisco Mobility Express wireless network solution, one AP, which runs the Cisco Mobility Express wireless LAN controller, is designated as the primary AP. Other access points, referred to as Subordinate APs, associate to this primary AP.

The primary AP operates as a wireless LAN controller, to manage and control the subordinate APs. It also operates as an AP to serve clients. The subordinate APs behave as normal lightweight APs to serve clients.

For more information about the solution, including setup and configuration, see the Cisco Mobility Express User Guide for Release 8.2, at:


### Supported Cisco Aironet Access Points

<table>
<thead>
<tr>
<th>APs Supported as Primary (Support Integrated Wireless Controller Capability)</th>
<th>APs Supported as Subordinate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Aironet 1850 Series</td>
<td>In addition to the following, all the APs that are supported as primary APs are also supported as subordinate APs.</td>
</tr>
<tr>
<td>Cisco Aironet 1830 Series</td>
<td></td>
</tr>
<tr>
<td>Cisco Aironet 700i Series</td>
<td></td>
</tr>
<tr>
<td>Cisco Aironet 700w Series</td>
<td></td>
</tr>
<tr>
<td>Cisco Aironet 1600 Series</td>
<td></td>
</tr>
<tr>
<td>Cisco Aironet 1700 Series</td>
<td></td>
</tr>
<tr>
<td>Cisco Aironet 2600 Series</td>
<td></td>
</tr>
<tr>
<td>Cisco Aironet 2700 Series</td>
<td></td>
</tr>
<tr>
<td>Cisco Aironet 3500 Series</td>
<td></td>
</tr>
<tr>
<td>Cisco Aironet 3600 Series</td>
<td></td>
</tr>
<tr>
<td>Cisco Aironet 3700 Series</td>
<td></td>
</tr>
</tbody>
</table>
Mobility Express Features

The following features and functionalities are present in this release:

- CLI-based Initial configuration wizard
- Up to three Network Time Protocol (NTP) servers, with support for FQDN names.
- Simple Network Management Protocol (SNMP) version 3 polling, supported via CLI only.
- IEEE 802.11r with support for Over-the-Air Fast BSS transition method, Over-the-DS Fast BSS transition method, and Fast Transition PSK authentication. Fast BSS transition methods are supported via CLI only.
- CCKM, supported via CLI only.
- Client ping test
- Changing the country code on the controller and APs on the network, via the controller GUI.
- Syslog messaging towards external server
- Software image download using HTTP for networks containing only AP 1850, AP 1830, or both kinds of access points.

The following are existing features, with continued support in the current release:

Note: Even if the Cisco AP is 802.3ad (LACP)-compliant, link aggregation groups (LAG) are not supported on the AP while it has a Cisco Mobility Express software image.

- Scalability:
  - Up to 25 APs
  - Up to 500 clients
  - Up to 16 WLANs
  - Up to 100 rogue APs
  - Up to 1000 rogue clients
- License—Does not require any licenses (Cisco Right-To-Use License or Swift) for APs.
- Operation—The primary AP can concurrently function as controller (to manage APs) and as an AP (to serve clients).
- Initial configuration wizard.
- Priming at distribution site.
- Default Service Set Identifier (SSID), set from factory. Available for initial provisioning only.
- Management—Through a web interface Monitoring Dashboard.
- Cisco Wireless Controller Best Practices.
- Quality of Service (QoS).
- Multicast with default settings.
- Application Visibility and Control (AVC)—Limited HTTP, with only Application Visibility and not Control. Deep Packet inspection with 1,500+ signatures.
- WLAN access control lists (ACLs).
- Roaming—Layer 2 roaming without mobility groups.
- IPv6—for client bridging only.
- High Density Experience (HDX)—Supported when managing APs that support HDX.
- Radio Resource Management (RRM)—Supported within AP group only.
- WPA2 Security.
- WLAN-VLAN mapping.
- Guest WLAN login with Web Authorization.
- Local EAP Authentication (local RADIUS server).
- Local profile.
- Network Time Protocol (NTP) Server.
- Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP).
- Clean Air.
- Simple Network Management Protocol (SNMP).
- Management—SSH, Telnet, Admin users.
- Reset to factory defaults.
- Serviceability—Core file and core options, Logging and syslog.
- Cisco Prime Infrastructure.
- Cisco CMX 10.x—Only CMX Presence is supported. CMX Connect, Location and Analytics are not supported.
- BYOD—Onboarding only.
- UX regulatory domain.
- Authentication, Authorization, Accounting (AAA) Override.
- IEEE 802.11k
- IEEE 802.11r
  - Supported—Over-the-Air Fast BSS transition method
  - Not Supported—Over-the-DS Fast BSS transition and Fast Transition PSK authentication
- Passive Client
- Voice with Call Admission Control (CAC), with Traffic Specification (TSpec)
- Fast SSID
- Terminal Access Controller Access Control System (TACACS)
- Management over wireless
- High Availability and Redundancy—Built-in redundancy mechanism to self-select a primary AP and to select a new AP as primary in case of a failure. Supported using VRRP.
- Software upgrade with preimage download
- Migration to controller-based deployment.

New Features and Functionalities

The following new features and functionalities have been introduced in this release.
Compatibility with Other Cisco Wireless Solutions

See the Cisco Wireless Solutions Software Compatibility Matrix, at:

Software Release Information

Cisco Mobility Express software for Cisco Wireless Release 8.2.100.0, is as follows:

<table>
<thead>
<tr>
<th>Software Pype and purpose</th>
<th>For AP 1850</th>
<th>For AP 1830</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software to be used only for conversion from Unified Wireless Network Lightweight APs software to Cisco Mobility Express software.</td>
<td>AIR-AP1850-K9-8.2.100.0.tar</td>
<td>AIR-AP1830-K9-8.2.100.0.tar</td>
</tr>
<tr>
<td>AP software image bundle, to be used for software update, or supported access points images, or both.</td>
<td>AIR-AP1850-K9-ME-8-2-100-0.zip</td>
<td>AIR-AP1830-K9-ME-8-2-100-0.zip</td>
</tr>
</tbody>
</table>

Installing Mobility Express Software

See the “Getting Started” section in the Mobility Express User Guide at the following URL:

Caveats

The open caveats applicable to the Cisco Mobility Express solution are listed under the “Caveats” section on page 37. All caveats associated with the Cisco Mobility Express solution have Cisco Mobility Express specified in the headline.

Related Documentation

- Cisco Mobility Express User Guide
- Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide
Installation Notes

This section contains important information to keep in mind when installing Cisco WLCs and access points.

Warnings

⚠️ Warning
This warning means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.
Statement 1071

⚠️ Warning
Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
Statement 1030

⚠️ Warning
Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death. For proper installation and grounding of the antenna, please refer to national and local codes (e.g. U.S.: NFPA 70, National Electrical Code, Article 810, Canada: Canadian Electrical Code, Section 54).
Statement 280

⚠️ Warning
This product relies on the building’s installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).
Statement 13

⚠️ Warning
This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground connector. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.
Statement 1024

⚠️ Warning
Read the installation instructions before you connect the system to its power source.
Statement 10

⚠️ Warning
Do not work on the system or connect or disconnect any cables (Ethernet, cable, or power) during periods of lightning activity. The possibility of serious physical injury exists if lightning should strike and travel through those cables. In addition, the equipment could be damaged by the higher levels of static electricity present in the atmosphere.
Statement 276

⚠️ Warning
Do not operate the unit near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.
Statement 364
Warning  In order to comply with radio frequency (RF) exposure limits, the antennas for this product should be positioned no less than 6.56 ft. (2 m) from your body or nearby persons. Statement 339

Warning  This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security. Statement 1017

Safety Information

Follow the guidelines in this section to ensure proper operation and safe use of the Cisco WLCs and access points.

FCC Safety Compliance Statement

FCC Compliance with its action in ET Docket 96-8, has adopted a safety standard for human exposure to RF electromagnetic energy emitted by FCC-certified equipment. When used with approved Cisco Aironet antennas, Cisco Aironet products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper operation of this radio device according to the instructions in this publication results in user exposure substantially below the FCC recommended limits.

Safety Precautions

For your safety, and to help you achieve a good installation, read and follow these safety precautions. They might save your life.

- If you are installing an antenna for the first time, for your own safety as well as others’, seek professional assistance. Your Cisco sales representative can explain which mounting method to use for the size and type of antenna you are about to install.
- Select your installation site with safety as well as performance in mind. Electric power lines and phone lines look alike. For your safety, assume that any overhead line can kill you.
- Call your electric power company. Tell them your plans and ask them to come look at your proposed installation. This is a small inconvenience considering your life is at stake.
- Plan your installation carefully and completely before you begin. Successfully raising a mast or tower is largely a matter of coordination. Each person should be assigned to a specific task and should know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.
- When installing an antenna, remember:
  - Do not use a metal ladder.
  - Do not work on a wet or windy day.
  - Do dress properly—shoes with rubber soles and heels, rubber gloves, long-sleeved shirt or jacket.
- If the assembly starts to drop, get away from it and let it fall. Remember that the antenna, mast, cable, and metal guy wires are all excellent conductors of electrical current. Even the slightest touch of any of these parts to a power line completes an electrical path through the antenna and the installer: you!
• If any part of an antenna system should come in contact with a power line, do not touch it or try to remove it yourself. Call your local power company. They will remove it safely.
• If an accident should occur with the power lines, call for qualified emergency help immediately.

### Installation Instructions

See the appropriate quick start guide or hardware installation guide for instructions on installing Cisco Wireless Controllers and APs.

**Note**

To meet regulatory restrictions, all external antenna configurations must be installed by experts.

Personnel installing the Cisco WLCs and APs must understand wireless techniques and grounding methods. APs with internal antennas can be installed by an experienced IT professional.

The Cisco WLC must be installed by a network administrator or qualified IT professional, and the proper country code must be selected. After the installation, access to the Cisco WLC should be password protected by the installer to maintain compliance with regulatory requirements and ensure proper unit functionality.

### Service and Support

#### Troubleshooting

**Step 1** For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at: [http://www.cisco.com/c/en/us/support/index.html](http://www.cisco.com/c/en/us/support/index.html)

**Step 2** Choose **Product Support > Wireless**.

**Step 3** Choose your product and click **Troubleshooting** to find information about the problem you are experiencing.

### Related Documentation

For more information about the Cisco WLCs, lightweight access points, and mesh access points, see these documents:

• The quick start guide or installation guide for your particular Cisco WLC or access point
• *Cisco Wireless Controller Configuration Guide*
• *Cisco Wireless Controller Command Reference*
• *Cisco Wireless Controller System Message Guide*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation at:

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