

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.0.252.0

First Published: March 23, 2015

Last Updated: March 30, 2015

These release notes describe open and resolved caveats for release 7.0.252.0 for the following hardware platforms:

- Cisco 2100, 2500, 4400, 5500, and Cisco Flex 7500 Series Wireless LAN Controllers
- Cisco Wireless Services Modules (WiSMs), Cisco Wireless Services Module (WiSM2), Cisco Wireless LAN Controller Network Modules
- Catalyst 3750G Integrated Wireless LAN Controller Switches, Cisco 3201 Wireless Mobile Interface Cards (WMICs)
- Cisco Aironet 1100, 1130, 1140, 1200, 1230AG, 1240, 1250, 1300, 1522, 1524, 1550, 1552S, AP3500, AP1260, AP1040, AP801, and AP 802 Series Lightweight Access Points; Cisco OEAP 600 Series Access Points; Cisco Aironet 1130AG, 1240AG, 1522, and 1524 Mesh Access Points, which are part of the Cisco Unified Wireless Network (UWN) Solution



Note

Unless otherwise noted, all of the Cisco Wireless LAN controllers are referred to as *controllers*, and all of the Cisco lightweight access points are referred to as *access points*.

Contents

These release notes contain the following sections:

- [Cisco Unified Wireless Network Solution Components, page 2](#)
- [Controller Requirements, page 4](#)
- [MIB Files, page 4](#)
- [What's New in This Release, page 4](#)



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

- [Software Release Information, page 5](#)
- [Upgrading to a New Software Release, page 15](#)
- [Information About Field Upgrade Software, page 18](#)
- [Installation Notes, page 18](#)
- [Using the Controller USB Console Port, page 21](#)
- [Important Notes for Controllers and Nonmesh Access Points, page 22](#)
- [Important Notes for Controllers and Mesh Access Points, page 42](#)
- [Caveats, page 43](#)
- [Service and Support, page 53](#)
- [Obtaining Documentation and Submitting a Service Request, page 54](#)

Cisco Unified Wireless Network Solution Components

The following components are part of the Cisco UWN Solution and are compatible in this release:

- Software release 7.0.252.0 for all Cisco controllers and lightweight access points
- Cisco IOS version 12.4(23c)JA10.
- Cisco autonomous to lightweight mode upgrade tool release 3.0
- Cisco Wireless Control System (WCS) software release 7.0.240.0
- Cisco WCS Navigator 1.6.240.0
- Mobility services engine software release 7.0.240.0 and Context-Aware Software



Note Client and tag licenses are required in order to retrieve contextual (such as location) information within the Context-Aware Software. For more information, see the *Release Notes for Cisco 3350 Mobility Services Engine for Software Release 7.0.116.0*.

- Cisco 3350, 3310 Mobility Services Engines
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 2500 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 5500 Series Wireless LAN Controllers
- Cisco Flex 7500 Series Wireless LAN Controllers
- Cisco Wireless Services Module (WiSM) for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- Cisco Wireless Services Module 2 (WiSM2) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers



Note The 7.0.252.0 release does not support the NM-AIR-WLC6 platform. The NME-AIR-WLC platform is supported.

Support for the NM-AIR-WLC6 platform ended with the 4.2.209.0 release.

- Catalyst 3750G Wireless LAN Controller Switches
- Cisco 3201 Wireless Mobile Interface Cards (WMICs)
- Cisco Aironet 1130AG, 1240AG, AP 1550, 1522, 1552S, and 1524 Mesh Access Points
- Cisco Aironet 1100, 1130, 1140, 1200, 1230AG, 1240, 1250, AP1260, 1300, AP3500, AP 1040, OEAP 600 Series Access Points, 1522, 1552S, 1524, 1550, 3500p, AP801, and AP802 Series Lightweight Access Points



Note Controller software release 5.0.148.0 or later is not compatible with Cisco Aironet 1010, 1020, 1030, and 1510 Series Access Points.

The AP801 is an integrated access point on the Cisco 800 Series Integrated Services Routers (ISRs). For more information on the SKUs for the access points and the ISRs, refer to the following data sheets:

- AP860:
 - http://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78_461543.html
- AP880:
 - http://www.cisco.com/c/en/us/products/collateral/routers/887-integrated-services-router-isr/data_sheet_c78_459542.html
 - http://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78-613481.html
 - http://www.cisco.com/c/en/us/products/collateral/routers/880-3g-integrated-services-router-isr/data_sheet_c78_498096.html
 - http://www.cisco.com/c/en/us/products/collateral/routers/880g-integrated-services-router-isr/data_sheet_c78-682548.html
- AP890:
 - http://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78-519930.html



Note The AP802 is an integrated access point on the Next Generation Cisco 880 Series Integrated Services Routers (ISRs).



Note Only Cisco Aironet 1200 Series Access Points that contain 802.11g (AIR-MP21G) or second-generation 802.11a radios (AIR-RM21A or AIR-RM22A) are supported for use with controller software releases. The AIR-RM20A radio, which was included in early 1200 series access point models, is not supported. To see the type of radio module installed in your access point, enter this command on the access point: **show controller dot11radio *n***, where *n* is the number of the radio (0 or 1).

Controller Requirements

The controller GUI requires the following operating system and web browser:

- Windows XP SP1 (or later) or Windows 2000 SP4 (or later)
- Internet Explorer 8.0 (or later) or Mozilla Firefox 16 (or later)

MIB Files

Cisco controllers support standard SNMP Management Information Base (MIB) files. MIBs can be downloaded from the Cisco Software Center at <https://software.cisco.com/download/navigator.html>. Only one MIB is posted per major release (7.0.252.0, 7.0.230.0, 7.0.220.0, 7.0.116.0, 7.0.98.0, 6.0, and so on). If an updated MIB is available, the previous version is removed from the Software Center and replaced by the new version.

What's New in This Release

For old hardware, Cisco Lightweight Access Points and Cisco Wireless Controllers may fail to create CAPWAP/LWAPP connection due to certificate expiration. From this release, you may configure to allow AP with Manufactured Installed Certificates beyond their expiration date to associate with the WLC.

Solution

The AP lifetime-check parameter is enabled by default. After upgrading to the fixed software, we recommend that you disable the AP lifetime-check by entering this command:

```
(Controller) >config ap lifetime-check {mic | ssc} enable
```

With the **config ap lifetime-check {mic | ssc} enable** command in effect, the WLC ignores the expiration date on the APs' MICs and SSCs, allowing APs with certificates that are more than 10 years old to associate with the WLC. The AP lifetime-check must remain enabled as long as APs with expired MIC or SSC certificates are being managed by this WLC.

You can see the configuration state by entering this command:

```
(Controller)>show certificate summary

Web Administration Certificate..... 3rd Party
Web Authentication Certificate..... Locally Generated
Certificate compatibility mode:..... off
Lifetime Check for MIC ..... Enable
Lifetime Check for SSC ..... Enable
```



Note

There are no new features or enhancements in this release. For updates in this release, see the [“Caveats” section on page 43](#).

Software Release Information

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

Guidelines and Limitations

- The Cisco WiSM requires software release SWISMK9-32 or later releases. The Supervisor 720 12.2(18)SXF2 supports the Cisco WiSM software release 3.2.78.4 or later, and the Supervisor 720 12.2(18)SXF5 (Cisco IOS Software Modularity) supports the Cisco WiSM software release 4.0.155.5 (with Cisco IOS Software Modularity).
- To use the Cisco WiSM in the Cisco 7609 and 7613 Series Routers, the routers must be installed with Cisco IOS Release 12.2(18)SXF5 or later.
- The Cisco Wireless LAN Controller Network Module is supported on Cisco 2800/3700/3800 Series Integrated Services Routers running Cisco IOS Release 12.4(15)T, 15.0(1)M or later, and on 2900/3900 ISRs running 15.0(1)M and later.

The Cisco Wireless LAN Controller Network Module is also supported on Cisco 1941/2900/3900/3900E Series Integrated Services Routers Generation 2 running Cisco IOS Release 15.1(3)T or later universal image.



Note

Use Cisco IOS Release 15.1(3)T.01 if you use the Cisco 2900 Series Integrated Services Routers Generation 2 with packet voice/data module (PVDM).

- To use the controller in the Catalyst 3750G Wireless LAN Controller Switch, the switch must be running Cisco IOS Release 12.2(25)FZ, 12.2(35)SE or later, 12.2(37)SE or later, 12.2(44)SE or later, or 12.2(46)SE or later. The following Cisco IOS Releases and any variants are not supported: 12.2(25)SEC, 12.2(25)SED, 12.2(25)SEE, 12.2(25)SEF, and 12.2(25)SEG. All Catalyst 3750 software feature sets (IP Base, IP Service, and Advanced IP Services) are supported for use with the controller.
- You can use the Cisco 2112 and 2125 Series Controllers only with software release 5.1.151.0 or later.
- The Cisco 526 Wireless Express Mobility Controller is supported only on the Cisco Wireless LAN Controller, Release 5.2.193.0 and earlier releases. The later releases do not support the Cisco 526 Wireless Express Mobility Controller.

Finding the Software Release

To find the software release running on your controller, click **Monitor** and look at the Software Version field under Controller Summary on the controller GUI, or enter **show sysinfo** on the controller CLI.

Special Rules for Upgrading to Controller Software Release 7.0.252.0

Before upgrading your controller to software release 7.0.252.0, you must comply with the following rules:

- Before you download a software image or an ER.aes file to a 2100 series controller or a controller network module, use the **show memory statistics CLI** command to see the current amount of free memory. If the controller has less than 90 MB of free memory, you must reboot it before downloading the file.
- Cisco 860 ISR is not supported as an access point in a unified wireless deployment.
- If you are using a Cisco 880 ISR, you must use Cisco IOS 12.4(20)T or later releases with an advanced IP services license.
- If you are using a Cisco 890 ISR, you must use Cisco IOS 12.4(22)YB. The advanced IP service license is enabled by default on Cisco 890 ISR.
- Ensure that you have a TFTP or FTP server available for the software upgrade. Follow these guidelines when setting up a TFTP or FTP server:
 - Controller software release 7.0.252.0 is larger than 32 MB; therefore, you must ensure that your TFTP server supports files that are larger than 32 MB. Some TFTP servers that support files of this size are tftpd and the TFTP server within the WCS. If you attempt to download the 7.0.252.0 controller 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 service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable; or you must create static routes on the controller.
 - If you are upgrading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
 - A third-party TFTP or FTP server cannot run on the same computer as WCS because the WCS built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.
- You can upgrade or downgrade the controller software only between certain releases. In some instances, you must first install an intermediate release prior to upgrading to software release 7.0.252.0. [Table 1](#) shows the upgrade path that you must follow before downloading software release 7.0.252.0.
- Before you use an AP802 series lightweight access point with controller software release 7.0.252.0, you must upgrade the software in the Next Generation Cisco 880 Series Integrated Services Routers (ISRs) to Cisco IOS 151-4.M or later releases.
- When you upgrade the controller to an intermediate software release, wait until all of the access points associated with the controller are upgraded to the intermediate release before you install the 7.0.252.0 software. In large networks, it can take some time to download the software on each access point.
- You cannot install the Cisco Unified Wireless Network Controller Boot Software 7.0.230.0 ER.aes file on the Cisco 5500 Controller platform.
- Field Upgrade Software (FUS) 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. FUS version 1.9.0.0 can be used for the 7.0.252.0 release. For more information about installing FUS, see <http://www.cisco.com/c/en/us/support/wireless/5500-series-wireless-controllers/products-release-notes-list.html>. On this page, from the **Choose Topic** drop-down list, choose **Other** to see the FUS release notes.

- The ER .aes files are independent from the controller software files. You can run any controller software file with any ER.aes file. However, installing the latest boot software file (7.0.116.0 ER.aes) ensures that the boot software modifications in all of the previous and current boot software ER.aes files are installed.
- Consider a network deployment scenario where an OfficeExtend Access Point is configured with the Least Latency Join option enabled and the controller is configured with NAT enabled. The Least Latency Join feature enables the access point to choose a controller with the least latency when joining, that is, when the feature is enabled, the access point calculates the time between the discovery request and the response and joins the controller that responds first. NAT enables a device such as a router to act as an agent between the Internet and the local network. NAT enables you to map the intranet IP address of a controller to a corresponding external address.

When an OfficeExtend Access Point that is configured with the Least Latency Join option and is upgraded to the controller release 7.0.252.0 tries to associate to the controller with NAT enabled, the access point fails to join the controller. Due to an update to the software code of 7.0.252.0, the OEAP tries to join the non-NAT IP address, fails to join, and tries a rediscovery that fails again. The OEAP can never connect to the controller.

The issue can be resolved by setting the access point mode to local mode on the controller and let the access point join the controller. On joining, you must disable least latency join and upgrade to 7.0.252.0 release.

- If you require a downgrade from one release to another, you might lose the configuration from your current release. The workaround is to reload the previous controller configuration files saved on the backup server or to reconfigure the controller.
- Control which address(es) are sent in CAPWAP discovery responses when NAT is enabled on the Management Interface using the following command:

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

Where:

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



Note To avoid stranding 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.

- If you upgrade from 4.2.176.0 to 7.0.252.0, and if an old image is present in the `/mnt/images` directory in the controller, the upgrade fails for the first time. The upgrade completes successfully when you upgrade again. The upgrade failure could have occurred based on one of the following reasons:
 - If the image files are renamed manually in the controller.
 - The files `bzImage.bak`, `bzImage.pri`, `initrd.bak`, and `initrd.pri` are files that are shipped with the 4.2 release and over time these filenames have changed resulting in a failed upgrade.

Table 1 Upgrade Path to Controller Software Release 7.0.252.0

Current Software Release	Upgrade Path to 7.0.240.0 Software
3.2.78.0 or later 3.2 release	Upgrade to 4.0.206.0 or later 4.0 release, then upgrade to 4.2.176.0, before upgrading to 7.0.252.0.
4.0.155.5 or later 4.0 release	Upgrade to 4.2.176.0 or later 4.2 releases before upgrading to 7.0.252.0.
4.1.171.0 or later 4.1 release	Upgrade to 4.2.209.0 before upgrading to 7.0.252.0.
4.1.191.xM	Upgrade to 4.1.192.35M and then to 6.0.182.0 before upgrading to 7.0.252.0.
4.1.192.22M or 4.1.192.35M	Upgrade to 4.2.209.0 before upgrading to 7.0.252.0.
4.2.130.0 or earlier 4.2 release	Upgrade to 4.2.209.0 before upgrading to 7.0.252.0.
4.2.173.0 or later 4.2 release	You can upgrade directly to 7.0.252.0.
4.2.209.0 or later 4.2 release	You can upgrade directly to 7.0.252.0.
5.0.148.0 or later 5.0 release	You can upgrade directly to 7.0.252.0.
5.1.151.0 or later 5.1 release	Upgrade to a 5.2 or a 6.0 release and then upgrade to 7.0.252.0.
5.2.157.0 or later 5.2 release	You can upgrade directly to 7.0.252.0.
6.0.188.0 or later 6.0 release	You can upgrade directly to 7.0.252.0.
6.0.196.0 or later 6.0 release	You can upgrade directly to 7.0.252.0.
7.0.x releases	You can upgrade directly to 7.0.252.0.

Software Release Support for Access Points

Table 2 lists the controller software releases that support specific Cisco access points. The First Support column lists the earliest controller software release that supports the access point. For access points that are not supported in ongoing releases, the Last Support column lists the last release that supports the access point.

Table 2 Software Support for Access Points

Access Points	First Support	Last Support	
1000 Series	AIR-AP1010	3.0.100.0	4.2.207.0
	AIR-AP1020	3.0.100.0	4.2.207.0
	AIR-AP1030	3.0.100.0	4.2.207.0
	Airespace AS1200	—	4.0
	AIR-LAP1041N	7.0.98.0	
	AIR-LAP1042N	7.0.98.0	
1100 Series	AIR-LAP1121	4.0.155.0	7.0.x
	AIR-LAP1131	3.1.59.24	
	AIR-LAP1141N	5.2.157.0	
	AIR-LAP1142N	5.2.157.0	

Table 2 **Software Support for Access Points (continued)**

Access Points		First Support	Last Support
1220 Series	AIR-AP1220A	3.1.59.24	7.0.x
	AIR-AP1220B	3.1.59.24	7.0.x
1230 Series	AIR-AP1230A	3.1.59.24	7.0.x
	AIR-AP1230B	3.1.59.24	7.0.x
	AIR-LAP1231G	3.1.59.24	7.0.x
	AIR-LAP1232AG	3.1.59.24	7.0.x
1240 Series	AIR-LAP1242G	3.1.59.24	—
	AIR-LAP1242AG	3.1.59.24	—
1250 Series	AIR-LAP1250	4.2.61.0	—
	AIR-LAP1252G	4.2.61.0	—
	AIR-LAP1252AG	4.2.61.0	—
1260 Series	AIR-LAP1261N	7.0.116.0	
	AIR-LAP1262N	7.0.98.0	
1300 Series	AIR-BR1310G	4.0.155.0	7.0.x
1400 Series	Standalone Only	N/A	—
3500 Series	AIR-CAP3501E	7.0.98.0	
	AIR-CAP3501I	7.0.98.0	
	AIR-CAP3502E	7.0.98.0	
	AIR-CAP3502I	7.0.98.0	
	AIR-CAP3502P	7.0.116.0	
1500 Mesh Series	AIR-LAP-1505	3.1.59.24	4.2.207.54M
	AIR-LAP-1510	3.1.59.24	4.2.207.54M

Table 2 Software Support for Access Points (continued)

Access Points		First Support	Last Support	
1520 Mesh Series	AIR-LAP1522AG	-A and N: 4.1.190.1 or 5.2 or later ¹	—	
		All other reg. domains: 4.1.191.24M or 5.2 or later ¹	—	
	AIR-LAP1522HZ	-A and N: 4.1.190.1 or 5.2 or later ¹	—	
		All other reg. domains: 4.1.191.24M or 5.2 or later ¹	—	
	AIR-LAP1522PC	-A and N: 4.1.190.1 or 5.2 or later ¹	—	
		All other reg. domains: 4.1.191.24M or 5.2 or later ¹	—	
	AIR-LAP1523CM	7.0.116.0 or later.		
	AIR-LAP1524SB	-A, C and N: 6.0 or later	—	
		All other reg. domains: 7.0.116.0 or later.		
	AIR-LAP1524PS	-A: 4.1.192.22M or 5.2 or later ¹	—	
	1550	AIR-CAP1552I-x-K9	7.0.116.0	
		AIR-CAP1552E-x-K9	7.0.116.0	
AIR-CAP1552C-x-K9		7.0.116.0		
AIR-CAP1552H-x-K9		7.0.116.0		
1552S	AIR-CAP1552SA-x-K9	7.0.220.0		
	AIR-cAP1552SD-x-K9	7.0.220.0		

1. These access points are supported in the separate 4.1.19x.x mesh software release or with release 5.2 or later releases. These access points are not supported in the 4.2, 5.0, or 5.1 Releases.

Interoperability With Other Clients in 7.0.252.0

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

[Table 3](#) describes the configuration used for testing the clients.

Table 3 *Test Bed Configuration for Interoperability*

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	7.0.252.0
Controller	Cisco 4400 Series Controller and Cisco 5500 Series Controller
Access points	1131, 1142, 1242, 1252, AP 3500e and AP3500i
Radio	802.11a, 802.11g, 802.11n2, 802.11n5
Security	Open, WEP, PSK (WPA and WPA2), 802.1X (WPA-TKIP and WPA2-AES) (LEAP, PEAP, EAP-FAST, EAP-TLS)
RADIUS	ACS 4.2
Types of tests	Connectivity, traffic, and roaming between two access points

[Table 4](#) lists the versions of the clients. The traffic tests included data or voice. The clients included laptops, handheld devices, phones, and printers.

Table 4 *Client Type and their Versions*

Client Type and Name	Version
Laptop	
Intel 3945/4965	11.5.1.15 or 12.4.4.5
Intel 5100/5300/6200/6300	13.1.1.1
Dell 1395/1397/Broadcom 4312HMG(L)	XP/Vista: 5.60.18.8 Win7: 5.30.21.0
Dell 1505/1510/Broadcom 4321MCAG/4322HM	5.60.18.8
Dell 1520/Broadcom 43224HMS	5.60.48.18
Atheros HB92/HB97	8.0.0.320
Atheros HB95	7.7.0.358
MacBook Pro (Broadcom)	5.10.91.26
Handheld Devices	
Falcon 4200/WinCE 4.2	5.60.21
Intermec CK31/WinCE 4.2:	3.00.19.0748

Table 4 **Client Type and their Versions (continued)**

Client Type and Name	Version
Intermec CN3/Windows Mobile 5.0	3.25.15.0065
Psion 7535/Wince 5.0	1.02.09
Psion WAP/Wince 5.0	1.02.42
Symbol 8846/Pocket PC 4.20	2.4.2273
Symbol MC70 /Windows Mobile 5.0	3.0.0.226
Symbol MC9060/Pocket PC 4.2	3.1.7
Symbol MC9090/Wince 5.0	3.1.7
Phones and Printers	
Ascom i75	1.4.25
Nokia e61	3.0633.09.04
Spectralink 8030	104.025
Spectralink e340/PTE110	110.036/091.047/104.025
Spectralink i640/PTX110	110.036/091.047/104.025
Vocera B1000A	4.1.0.2817
Vocera B2000	4.0.0.269
Zebra QL320	HTNVK49s
Monarch 9855	3.2AB
Cisco 7921G	CP7921G-1.3.4.LOADS
Cisco 7925G	CP7925G-1.3.4.LOADS

Special Rules for Upgrading to Controller Software 7.0.252.0 in Mesh Networks

Before upgrading your controller to software release 7.0.252.0 in a mesh network, you must comply with the following rules.

Upgrade Compatibility Matrix

Table 5 outlines the upgrade compatibility of controller mesh and nonmesh releases and indicates the intermediate software releases required as part of the upgrade path.

Software Upgrade Notes

The software upgrade notes are as follows:

- You can upgrade from 4.1.192.22M and 4.1.192.135M to 6.0.182.0 without any configuration file loss. See Table 5 for the available upgrade paths.



Note If you downgrade to a mesh release, you must then reconfigure the controller. We recommend that you save the configuration from the mesh release before upgrading to release 7.0.252.0 for the first time. Then, you can reapply the configuration if you need to downgrade.

- It is not possible to downgrade from controller software release 7.0.252.0 to a mesh release (for example, 4.1.190.5, 4.1.191.22M, or 4.1.192.xM) without losing your configuration settings.
- Configuration files are in the binary state immediately after an upgrade from a mesh release to controller software release 7.0.252.0. After a reset, the XML configuration file is selected.
- Do not edit XML files.
- Any field with an invalid value is filtered out and set to default by the XML validation engine. Validation occurs during bootup.
- If you upgrade the controller from software release 4.1.191.xM to 4.1.192.xM and then to software release 6.0.182.0, the controller might reboot without a crash file. To work around this problem, manually reset the controller without saving the configuration after you upgrade the controller to software release 7.0.252.0. Also, make sure to check the RRM configuration settings after the reset to verify that they are correct (CSCsv50357).

Table 5 Upgrade Compatibility Matrix for Controller Mesh and Nonmesh Releases from 4.0.206.0 Release and Later Releases

Upgrade to	7.0.252.0	7.0.235.0	7.0.230.0	7.0.220.0	7.0.116.0	7.0.98.218	7.0.98.0	6.0.199.0	6.0.196.0	6.0.188.0	6.0.182.0	5.2	4.2.207.54M	4.2.176.51M	4.1.192.35M	4.1.191.24M	4.1.190.5	4.1.185.0	4.1.171.0	4.0.219.0	4.0.217.204	4.0.217.0	
Upgrade from																							
7.0.116.0	Y	Y	Y	Y																			
7.0.98.218	Y	Y	Y	Y	Y																		
7.0.98.0	Y	Y	Y	Y	Y	Y																	

Table 5 Upgrade Compatibility Matrix for Controller Mesh and Nonmesh Releases from 4.0.206.0 Release and Later Releases (continued)

	Upgrade to	7.0.252.0	7.0.235.0	7.0.230.0	7.0.220.0	7.0.116.0	7.0.98.218	7.0.98.0	6.0.199.0	6.0.196.0	6.0.188.0	6.0.182.0	5.2	4.2.207.54M	4.2.176.51M	4.1.192.35M	4.1.191.24M	4.1.190.5	4.1.185.0	4.1.171.0	4.0.219.0	4.0.217.204	4.0.217.0	
6.0.199.0		Y	Y	Y	Y	Y	Y	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
6.0.196.0		Y	Y	Y	Y	Y	Y	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
6.0.188.0		Y	Y	Y	Y	Y	Y	Y	Y	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-
6.0.182.0		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	-	-	-	-	-	-	-	-	-	-	-	-
5.2		Y	Y	Y	Y	Y	Y	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
4.2.207.54M		Y	Y	Y	Y	Y	Y	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
4.2.176.51M		Y	Y	Y	Y	Y	Y	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
4.1.192.35M		-	-	-	-	-	-	-	-	-	-	Y	Y	-	-	-	-	-	-	-	-	-	-	-
4.1.192.22M		-	-	-	-	-	-	-	-	-	-	Y	Y	-	-	Y	-	-	-	-	-	-	-	-
4.1.191.24M		-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-
4.1.190.5		-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y ₁	Y	-	-	-	-	-	-	-
4.1.185.0		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y ₂	-	-	-	-	-	-
4.1.181.0		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y ₂	Y ²	-	-	-	-	-
4.1.171.0		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y ₂	Y ²	-	-	-	-	-
4.0.219.0		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y ²	Y ₂	-	-	-	-
4.0.217.204		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y ₂	-	Y ²	Y ₂	Y ²	-	-	-
4.0.217.0		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y ²	Y ₂	Y ²	Y ³	-	-
4.0.216.0		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y ²	Y ₂	Y ²	Y ³	Y	-
4.0.206.0		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y ²	Y ₂	Y ²	Y ³	Y	-

1. You can upgrade directly from software release 4.1.190.5 to 4.1.192.35M; however, upgrading to 4.1.191.24M before upgrading to 4.1.192.35M is highly recommended.
2. Customers who require dynamic frequency selection (DFS) functionality should not use this release. This release does not provide DFS functionality fixes found in release 4.0.217.204. Additionally, this release is not supported in ETSI-compliant countries or Singapore.
3. Release 4.0.217.204 provides fixes for DFS on 1510 series access points. This functionality is needed only in countries where DFS rules apply.

Upgrading to a New Software Release

When you upgrade to the latest software release, the software on the access points associated with the controller is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession. Up to 10 access points can be concurrently upgraded from the controller.

Guidelines and Limitations

- The Cisco 5500 Series Controllers can download the 7.0.252.0 software to 500 access points simultaneously.
- Multicast mode is not supported on the Cisco 600 Series OfficeExtend access points.
- Do not power down the controller or any access point during the upgrade process; otherwise, you might corrupt the software image. Upgrading a controller 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 in software release 4.0.206.0 and later, the upgrade time should be significantly reduced. The access points must remain powered, and the controller must not be reset during this time.
- In controller software release 5.2 or later, the WLAN override feature has been removed from both the controller GUI and CLI. If your controller is configured for WLAN override and you upgrade to controller software release 7.0.252.0, the controller deletes the WLAN configuration and broadcasts all WLANs. You can specify that only certain WLANs be transmitted by configuring access point groups. Each access point advertises only the enabled WLANs that belong to its access point group.
- If a WiSM controller is heavily loaded with access points and clients and is running heavy traffic, a software upgrade sometimes causes an Ethernet receive-path lockup and the hardware watchdog sometimes trips. You might need to reset the controller to return to normal operation.
- Do not install the 7.0.252.0 controller software file and the 7.0.230.0 ER.aes boot software file at the same time. Install one file and reboot the controller and install the other file and reboot the controller.
- When upgrading from 5.2.193.0 to 7.0.252.0 release, access points with names that contain spaces will lose their configured name. For example, if an access point was named “APT testName 12,” after upgrade, when the access point rejoins the controller, the name is truncated to “APT testName.”
- If you want to downgrade from 7.0.252.0 release to a previous release, do either of the following:
 - Delete all WLANs that are mapped to interface groups and create new ones.
 - Ensure that all WLANs are mapped to interfaces rather than interface groups.
- If you are using controller software release 7.0.252.0 and if you have configured multicast interfaces, do not use the same configuration file for the 7.0.98.0 release. Using the 7.0.252.0 configuration file with multicast interfaces in the 7.0.98.0 release might cause the controller to be unresponsive.
- When upgrading the controller software from release an earlier release to 7.0.252.0, the controllers that were previously reachable from WCS with SNMPv3 authentication are now unreachable.

Use any of the following workarounds to correct this issue:

- In WCS, change the SNMP credentials for this controller to v2C and then back to V3.
- Stop and start the WCS.
- Add the controller to the WCS.



Note When a config XML is downloaded, the SNMP engine ID is reset to the default value. If the SNMP engine ID is configured, you must configure it again after you apply the newly downloaded configuration.

- When you upgrade a mesh network to the 7.0.252.0 release and select a certain channel number during the upgrade process, the MAP might be unable to join its parent. The workaround to this issue is as follows:

For AP1552 operating in the U.S. domain, when upgrading the mesh network from 7.0.116.0 or 7.0.220.0 release to the 7.0.252.0 release, select channel (149, 153) or (157, 161) if you choose 40-MHz bandwidth for backhaul. After the upgrade is propagated to the whole of the mesh network, then you can change to the other channel selection.

Upgrading the Controller Software (GUI)


Step 1 Upload your controller configuration files to a server to back them up.



Note We highly recommend that you back up your controller's configuration files prior to upgrading the controller software. Otherwise, you must manually reconfigure the controller.

Step 2 Follow these steps to obtain the 7.0.252.0 controller software and the Cisco Unified Wireless Network Controller Boot Software 7.0.240.0 ER.aes file from the Software Center on Cisco.com:

- Click this URL to go to the Software Center:
<http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875243>
- Click **Wireless Software**.
- Click **Wireless LAN Controllers**.
- Click **Standalone Controllers** or **Integrated Controllers and Controller Modules**.
- Click a controller series.
- If necessary, click a controller model.
- If you chose Standalone Controllers in Step **d.**, click **Wireless LAN Controller Software**.
- If you chose Cisco Catalyst 6500 Series/7600 Series Wireless Services Module (WiSM) in Step **e.**, click **Wireless Services Modules (WiSM) Software**.
- Click a controller software release. The software releases are labeled as follows to help you determine which release to download:
 - **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.
- Click a software release number.
- Click the filename (*filename.aes*).

- l. Click **Download**.
 - m. Read Cisco's End User Software License Agreement and then click **Agree**.
 - n. Save the file to your hard drive.
 - o. Repeat steps a. through n. to download the remaining file (either the 7.0.252.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 7.0.240.0 ER.aes file).
- Step 3** Copy the controller software file (*filename.aes*) and the Cisco Unified Wireless Network Controller Boot Software 7.0.230.0 ER.aes file to the default directory on your TFTP or FTP server.
- Step 4** (Optional) Disable the controller 802.11a/n and 802.11b/g/n networks.
-
-  **Note** For busy networks, controllers on high utilization, or small controller platforms it is advisable to disable the 802.11a/b/g/n networks as a precautionary measure.
-
- Step 5** Click **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** or **FTP**.
- Step 8** In the IP Address text box, enter the IP address of the TFTP or FTP server.
- Step 9** If you are using a TFTP server, the default values of 10 retries for the Maximum Retries text field, and 6 seconds for the Timeout text field should work fine 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) that 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, follow these steps:
- a. In the Server Login Username text box, enter the username to log on to the FTP server.
 - b. In the Server Login Password text box, enter the password 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 controller. A message appears indicating the status of the download.
- Step 14** After the download is complete, click **Reboot**.
- Step 15** If prompted to save your changes, click **Save and Reboot**.
- Step 16** Click **OK** to confirm your decision to reboot the controller.
- Step 17** After the controller reboots, repeat [Step 5](#) to [Step 16](#) to install the remaining file (either the 7.0.252.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 7.0.240.0 ER.aes file).
- Step 18** For Cisco WiSMs, reenable the controller port channel on the Catalyst switch.
- Step 19** If you have disabled the 802.11a/b/g networks in [Step 4](#), reenable them.
- Step 20** If desired, reload your latest configuration file to the controller.
- Step 21** To verify that the 7.0.252.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

- Step 22** To verify that the Cisco Unified Wireless Network Controller Boot Software 7.0.240.0 ER.aes file is installed on your controller, enter the **show sysinfo** command on the controller CLI and look at the Emergency Image Version field.



Note If you do not install the 7.0.240.0 ER.aes file, the Emergency Image Version field shows “N/A.”

Information About Field Upgrade Software

Field Upgrade Software (FUS) is a special AES package that performs various system-related component upgrades. We recommend that you perform an FUS upgrade (if needed) to upgrade components such as the bootloader, field recovery image, FPGA/MCU, and other firmware to their latest respective versions.

For more information about installing FUS, see <http://www.cisco.com/c/en/us/support/wireless/5500-series-wireless-controllers/products-release-notes-list.html>. On this page, from the **Choose Topic** drop-down list, choose **Other** to see the FUS release notes.

Installation Notes

This section contains important information to keep in mind when installing controllers and access points:

- [Warnings, page 18](#)
- [Safety Information, page 19](#)
- [Installation Instructions, page 20](#)

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 controllers 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!

1. 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.
2. 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.
3. 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.
4. 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.
5. When installing an antenna, remember:
 - a. Do not use a metal ladder.
 - b. Do not work on a wet or windy day.
 - c. Do dress properly—shoes with rubber soles and heels, rubber gloves, long-sleeved shirt or jacket.
6. 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!**
7. 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.
8. If an accident should occur with the power lines, call for qualified emergency help immediately.

Installation Instructions

Refer to the appropriate quick start guide or hardware installation guide for instructions on installing controllers and access points.

**Note**

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

Personnel installing the controllers and access points must understand wireless techniques and grounding methods. Access points with internal antennas can be installed by an experienced IT professional.

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

Using the Controller USB Console Port

The USB console port on the Cisco 5500 Series Controllers and the Cisco WiSM2 connects directly to the USB connector of a PC using a USB Type A-to-5-pin mini Type B cable.



Note

The 4-pin mini Type B connector is easily confused with the 5-pin mini Type B connector. They are not compatible. Only the 5-pin mini Type B connector can be used.

For operation with Microsoft Windows, the Cisco Windows USB console driver must be installed on any PC connected to the console port. With this driver, you can plug and unplug the USB cable into and from the console port without affecting Windows HyperTerminal operations.



Note

Only one console port can be active at a time. When a cable is plugged into the USB console port, the RJ-45 port becomes inactive. Conversely, when the USB cable is removed from the USB port, the RJ-45 port becomes active.

You can now remove your console cable and plug it back in again without having to quit the terminal program and restarting it.

USB Console OS Compatibility

The USB console drivers are available for Microsoft Windows (both 32 and 64-bit architectures), Apple Mac OS, and Linux. See the README PDF files in the USB Console Driver.zip package for installation instructions.

To download and configure the Cisco Windows USB console driver, follow these steps.

-
- Step 1** Go to the Cisco Software Center at:
<https://software.cisco.com/download/navigator.html>
 - Step 2** Choose **Products > Wireless > Wireless LAN Controller > Standalone Controllers > Cisco 5500 Series Wireless Controllers**.
 - Step 3** Click **USB Console Port Driver Software**.



Note

The USB Console Port Driver Software is also applicable to the Cisco WiSM2.

- Step 4** Click **Download Now**.
- Step 5** Save the file to your hard drive.
- Step 6** Extract the .zip file and install the driver depending on the operating system you are using.

**Note**

Instructions for installing the USB console port software for Apple Mac OS and Linux are provided in the downloadable zip file.

- Step 7** Connect the mini Type B connector to the USB console port on the controller. Connect the Type A connector to a USB port on your PC.

Important Notes for Controllers and Nonmesh Access Points

This section describes important information about controllers and nonmesh lightweight access points.

WPlus License Features Included in Base License

All features included in a Wireless LAN Controller WPlus license are now included in the base license; this change is introduced in release 7.0.252.0. There are no changes to WCS BASE and PLUS licensing.

These WPlus license features are included in the base license:

- Office Extend AP
- Enterprise Mesh
- CAPWAP Data Encryption

The licensing change can affect features on your wireless LAN when you upgrade or downgrade software releases, so you should be aware of these guidelines:

- If you have a WPlus license and you upgrade from 6.0.18x to 7.0.252.0, your license file contains both Basic and WPlus license features. You will not see any disruption in feature availability and operation.
- If you have a WPlus license and you downgrade from 7.0.252.0 to 6.0.196.0, 6.0.188 or 6.0.182, the license file in 7.0.220.0 contains both Basic and WPlus license features, so you will not see any disruption in feature availability and operation.
- If you have a base license and you downgrade from 7.0.252.0, 7.0.240.0, 7.0.230.0, 7.0.220.0, 6.0.196.0, 6.0.188.0 or 6.0.182.0, you lose all WPlus features.

**Note**

Some references to the Wireless LAN Controller WPlus licenses remain in WCS and in the controller CLI and GUI in release 7.0.252.0. However, WLC WPlus license features have been included in the Base license, so you can ignore those references.

Additive Licenses Available for Controllers

You can now purchase licenses to support additional access points on Cisco 5500 Series and Cisco Flex 7500 Series Controllers. The new additive licenses (for 25, 50, or 100 access points) can be upgraded from all license tiers (12, 25, 50, 100, and 250 access points). The additive licenses are supported through both rehosting and RMAs.

One-Time Password (OTP) Support

One Time Passwords (OTPs) are supported on the Wireless Lan Controller (WLC) using TACACS and RADIUS. In this configuration, the controller acts as a transparent passthrough device. The controller forwards all client requests to the TACACS/RADIUS server without inspecting the client behavior. When using OTP, the client must establish a single connection to the controller to function properly. The controller currently does not have any intelligence or checks to correct a client that is trying to establish multiple connections.

RADIUS Called-station-id and Calling-station-id Attributes

In software releases prior to 6.0, the controller sends uppercase alphabetic characters in the MAC address. In software release 6.0 or later, the controller sends lowercase alphabetic characters in the MAC address for the RADIUS called-station-id and calling-station-id attributes. If you enabled these attributes for 802.1X authentication in previous releases and upgrade to software release 6.0, client authentication fails. Therefore, you must change the MAC addresses to lowercase characters on the RADIUS server before upgrading to software release 6.0.

Access Point Groups

You can create up to 50 access point groups for Cisco 2100 Series Controllers and controller network modules and up to 300 access point groups for Cisco 4400 Series Controllers, 500 AP Groups on 5500 Series Controllers, and 192 access point groups for the Cisco WiSM, and the 3750G wireless LAN controller switch.

Using Access Points in Sniffer Mode

You must disable IP-MAC address binding in order to use an access point in sniffer mode if the access point is joined to a 5500 series controller, a 2100 series controller, or a controller network module running software release 6.0. To disable IP-MAC address binding, enter this command using the controller CLI: **config network ip-mac-binding disable**.

WLAN 1 must be enabled in order to use an access point in sniffer mode if the access point is joined to a 5500 series controller, a 2100 series controller, or a controller network module running software release 6.0. If WLAN 1 is disabled, the access point cannot send packets.

Inter-Release Controller Mobility

Learn more about inter-release controller mobility compatibility across releases at this URL:

<http://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html#pgfId-149658>

RLDP Limitations

The Rogue Location Discovery Protocol (RLDP) is a controller feature that detects the presence of rogue access points that are connected to your wired network. RLDP operates with these limitations:

- RLDP detects rogue access points that are configured for open authentication.
- RLDP detects rogue access points that use a broadcast BSSID (that is, the access point broadcasts its SSID in beacons).
- RLDP detects only rogue access points that are on the same network. In other words, if an access list in the network prevents the sending of RLDP traffic from the rogue access point to the controller, RLDP does not work.
- RLDP does not work on 5-GHz dynamic frequency selection (DFS) channels. However, RLDP works when the managed access point is a monitor mode AP on a DFS channel.

Internal DHCP Server

When clients use the internal DHCP server of the controller, IP addresses are not preserved across reboots. As a result, multiple clients can be assigned with the same IP address. To resolve any IP address conflicts, clients must release their existing IP address and request a new one.

Bootloader Menu

When you plug a controller into an AC power source, the bootup script and power-on self-test run to initialize the system. During this time, you can press **Esc** to display the bootloader Boot Options Menu. The menu options for the 5500 and Flex 7500 series controllers are different than for other controller platforms.

Bootloader Menu for 5500 Series Controllers:

```

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 Controller 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, or enter **4** (on a 5500 series controller) or **5** (on another controller platform) to run the current software and set the controller configuration to factory defaults. Do not choose the other options unless directed to do so.



Note

See the Installation Guide or Quick Start Guide for your controller for more details on running the bootup script and power-on self-test.

Fragmented Pings

Cisco 5500 series controllers do not support fragmented pings on any interface. Similarly, Cisco 4400 series controllers, the Cisco WiSM, and the Catalyst 3750G Integrated Wireless LAN Controller Switch do not support fragmented pings on the AP-manager interface.

802.11g Controller and 802.11b Clients

When a controller is configured to allow only 802.11g traffic, 802.11b client devices are able to successfully connect to an access point but cannot pass traffic. When you configure the controller for 802.11g traffic only, you must mark 11g rates as mandatory.

CAPWAP Problems with Firewalls and ACLs

If you have a firewall or Access Control List (ACL) between the controller and its access points that allows LWAPP traffic, before upgrading to software release 5.2 or later and CAPWAP, you should allow CAPWAP traffic from the access points to the controller by opening the following destination ports:

- UDP 5246
- UDP 5247

The access points use a random UDP source port to reach these destination ports on the controller. In controller software release 5.2, LWAPP was removed and replaced by CAPWAP, but if you have a new out-of-the-box access point, it could try to use LWAPP to contact the controller before downloading the CAPWAP image from the controller. Once the access point downloads the CAPWAP image from the controller, it uses only CAPWAP to communicate with the controller.



Note

After 60 seconds of trying to join a controller with CAPWAP, the access point falls back to using LWAPP. If it cannot find a controller using LWAPP within 60 seconds, it tries again to join a controller using CAPWAP. The access point repeats this cycle of switching from CAPWAP to LWAPP and back again every 60 seconds until it joins a controller.



Note

An access point with the LWAPP recovery image (an access point converted from autonomous mode or an out-of-the-box access point) uses only LWAPP to try to join a controller before downloading the CAPWAP image from the controller.

Messages Appearing Upon Controller Bootup

Several messages might flood the message logs when the controller boots up. These messages appear because of a failure to read or delete several different configuration files. These are low-severity messages that can safely be ignored. They do not affect controller functionality. These are some examples:

```
Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Failed to delete the file :
sshpmInitParms.cfg. file removal failed.
-Process: Name:fp_main_task, Id:11ca7618
Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Failed to delete the file :
bcastInitParms.cfg. file removal failed.
```

-Process: Name:fp_main_task, Id:11ca7618

Web Authentication Redirects

The controller supports web authentication redirects only to HTTP (HTTP over TCP) servers. It does not support web authentication redirects to HTTPS (HTTP over SSL) servers.



Note

For Cisco 5500 Series Controllers, Cisco 2100 Series Controllers, and controller network modules, you must configure a preauthentication access control list (ACL) on the WLAN for the external web server and then choose this ACL as the WLAN preauthentication ACL under Security Policies > Web Policy on the WLANs > Edit page.

Crash Files for Cisco Aironet 1250 Series Access Points

The 1250 series access points might contain a bootloader older than version 12.4(10b)JA. Units with old bootloaders do not generate a crash log when a crash occurs. The crash log is disabled so that a crash does not corrupt the flash file system. Units with bootloader versions 12.4(10b)JA or later generate a crash log if the access point is associated to a controller running software release 4.2.112.0 or later.

New 1250 series access points shipped from the factory contain new bootloader images, which fix the flash file system after it is corrupted during a crash (without losing files). This new bootloader automatically sets a new CRASH_LOG environment variable to "yes," which enables a crash log to be generated following a crash but only on controllers running software release 4.2.112.0 or later. Therefore, no user configuration is needed to enable a crash log on new 1250 series access points shipped from the factory.

These examples show the output from the CLI commands (in bold) that you use to check the bootloader version on lightweight and autonomous 1250 series access points:

Commands entered on the controller CLI:

```
debug ap enable AP001b.d513.1754
debug ap command "show version | include BOOTLDR" AP001b.d513.1754
```

```
Thu Apr 23 09:31:38 2009: AP001b.d513.1754: BOOTLDR: C1250 Boot Loader
(C1250-BOOT-M) Version 12.4(10b)JA, RELEASE SOFTWARE (fc1)
```

Command entered on the access point CLI:

```
show version | include BOOTLDR
BOOTLDR: C1250 Boot Loader (C1250-BOOT-M) Version 12.4(10b)JA, RELEASE SOFTWARE (fc1)
```

Configuration File Stored in XML

In controller software release 4.2.61.0 and later, the bootup configuration file of the controller is stored in an Extensible Markup Language (XML) format rather than in binary format. When you upgrade a controller to 4.2.61.0 or a later software release, the binary configuration file is migrated and converted to XML.

**Note**

You cannot download a binary configuration file onto a controller running software release 7.0.252.0. Also, do not attempt to make changes to the configuration file. If you do so and then download the file to a controller, the controller displays a cyclic redundancy checksum (CRC) error while it is rebooting and returns the configuration parameters to their default values.

**Note**

You cannot modify the configuration files for 2000, 4000, and 4100 series controllers. The ability to modify configuration files is available in controller software release 5.2 or later, and these controllers support only earlier software releases (up to the 4.2 release for 2000 series controllers and up to the 3.2 release for 4000 and 4100 series controllers).

LWAPP Mode Changes

When you upgrade to controller software release 5.0.148.0 or later, the LWAPP mode changes to Layer 3 if it was previously configured for Layer 2.

If you downgrade from controller software release 7.0.252.0, 7.0.220.0, 6.0.196.0, 6.0.188.0, 5.2.178.0, 5.2.157.0, 5.1.151.0, or 5.0.148.0 to 4.2.61.0 or an earlier release, the LWAPP mode changes from Layer 3 to Layer 2. Access points might not join the controller, and you must manually reset the controller to Layer 3 to resolve this issue.

Issues with APs That Transmit Multicast Frames at Highest Configured Basic Rate and Management Frames with Lowest Basic Rates

Access points running recent Cisco IOS versions transmit multicast frames at the highest configured basic rate and management frames at the lowest basic mandatory rates, can cause reliability problems. Access points running LWAPP or autonomous Cisco IOS should transmit multicast and management frames at the lowest configured basic rate. Such behavior is necessary to provide good coverage at the cell's edge, especially for unacknowledged multicast transmissions where multicast wireless transmissions might fail to be received.

Because multicast frames are not retransmitted at the MAC layer, clients at the edge of the cell might fail to receive them successfully. If reliable reception is a goal, multicast frames should be transmitted at a low data rate. If support for high data rate multicast frames is required, it might be useful to shrink the cell size and disable all lower data rates.

Depending on your specific requirements, you can take the following actions:

- If you need to transmit multicast data with the greatest reliability and if there is no need for great multicast bandwidth, then configure a single basic rate, that is low enough to reach the edges of the wireless cells.
- If you need to transmit multicast data at a certain data rate in order to achieve a certain throughput, you can configure that rate as the highest basic rate. You can also set a lower basic rate for coverage of nonmulticast clients.

Disabling Radio Bands

The controller disables the radio bands that are not permitted by the configured country of operation (CSCsi48220).

802.11a Channels 120, 124, and 128 Disabled

802.11a channels 120, 124, and 128 are disabled to achieve compliance with draft EN 301 893 version 1.5.1 on the following -E regulatory domain products: AP1131AG, AP1242AG, and AP1252AG.

Impact of External Antenna Gain on Transmit Power

In controller software release 4.2 or later, external antenna gain is factored into the maximum transmit power of the access point. Therefore, when you upgrade from an earlier software release to 4.2 or later, you might see a decrease in transmit power output.

**Note**

The Transmit Power level can range between -1 dBm to 30 dBm.

Supporting Oversized Access Point Images

Controller software release 4.2 or later enables you to upgrade to an oversized access point image by deleting the recovery image to create sufficient space. This feature affects only access points with 8 MB of flash (the 1100, 1200, and 1310 series access points). All newer access points have a larger flash size than 8 MB.



Note

As of August 2007, there are no oversized access point images, but as new features are added, the access point image size will continue to grow.

The recovery image provides a backup image that can be used if an access point power-cycles during an image upgrade. The best way to avoid the need for access point recovery is to prevent an access point from power-cycling during a system upgrade. If a power-cycle occurs during an upgrade to an oversized access point image, you can recover the access point using the TFTP recovery procedure.

To recover the access point using the TFTP recovery procedure, follow these steps:

-
- Step 1** Download the required recovery image from Cisco.com (c1100-rcvk9w8-mx, c1200-rcvk9w8-mx, or c1310-rcvk9w8-mx) and install it in the root directory of your TFTP server.
 - Step 2** Connect the TFTP server to the same subnet as the target access point and power-cycle the access point. The access point boots from the TFTP image and then joins the controller to download the oversized access point image and complete the upgrade procedure.
 - Step 3** After the access point has been recovered, you might remove the TFTP server.
-

Multicast Queue Depth

The multicast queue depth is 512 packets on all controller platforms. However, the following message might appear on 2106 controllers: “Rx Multicast Queue is full on Controller.” This message does not appear on 4400 series controllers because the 4400 NPU filters ARP packets while controllers forwarding (multicast or otherwise) and multicast replication is done in the software on the 2106.

This message appears when too many multicast messages are sent to the CPU. In controller software releases prior to 5.1, multicast, CDP, and ARP packets share the same queue. However, in software releases 5.1 and later, these packets are separated into different queues. There are currently no controller commands that can be entered to determine if the multicast receive queue is full. When the queue is full, some packets are randomly discarded.

MAC Filtering for WGB Wired Clients

Controller software release 4.1.178.0 or later enables you to configure a MAC-filtering IP address for a workgroup bridge (WGB) wired client to allow passive WGB wired clients, such as terminal servers or printers with static IP addresses, to be added and remain in the controller’s client table while the WGB is associated to a controller in the mobility group. This feature, activated by the **config macfilter ipaddress MAC_address IP_address** CLI command, can be used with any passive device that does not initiate any traffic but waits for another device to start communication.

This feature enables the controller to learn the IP address of a passive WGB wired client when the WGB sends an IAPP message to the controller that contains only the WGB wired client's MAC address. Upon receiving this message from the WGB, the controller checks the local MAC filter list (or the anchor controller's MAC filter list if the WGB has roamed) for the client's MAC address. If an entry is found and it contains an IP address for the client, the controller adds the client to the controller's client table.



Note

Unlike the existing MAC filtering feature for wireless clients, you are not required to enable MAC filtering on the WLAN for WGB wired clients.



Note

WGB wired clients that use MAC filtering do not need to obtain an IP address through DHCP to be added to the controller's client table.

Controller software releases 7.0.116.0 and later provide the passive client feature for Cisco 2100, 2500, 5500 Series Controllers and Cisco WiSM2 that enable devices like printers connected to WGB to hear ARP requests, answer and move to run state. That is a dynamic alternative that replaces the MAC filter. The MAC filter feature is required for Cisco 4400 Series Controller and WiSM for passive clients.

CKIP Not Supported with Dynamic WEP

In controller software release 4.1.185.0 or later, CKIP is supported for use only with static WEP. It is not supported for use with dynamic WEP. Therefore, a wireless client that is configured to use CKIP with dynamic WEP is unable to associate to a wireless LAN that is configured for CKIP. We recommend that you use either dynamic WEP without CKIP (which is less secure) or WPA/WPA2 with TKIP or AES (which are more secure).

Setting the Date and Time on the Controller

Cisco Aironet lightweight access points do not connect to the controller if the date and time are not set properly. Set the current date and time on the controller before allowing the access points to connect to it.

Synchronizing the Controller and Location Appliance

For controller software release 4.2 or later, if a location appliance (release 3.1 or later) is installed on your network, the time zone must be set on the controller to ensure proper synchronization between the two systems. Also, we highly recommend that the time be set for networks that do not have location appliances. See Chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide, Release 7.0.116.0*, for instructions to set the time and date on the controller.



Note

The time zone can be different for the controller and the location appliance, but the time zone delta must be configured accordingly, based on Greenwich Mean Time (GMT).

FCC DFS Support on 1130 Series Access Points

Federal Communications Commission (FCC) dynamic frequency selection (DFS) is supported only on 1130 series access points in the United States, Canada, and the Philippines that have a new FCC ID. Access points use DFS to detect radar signals such as military and weather sources and then switch channels to avoid interfering with them. 1130 series access points with FCC DFS support have an FCC ID *LDK102054E* sticker. 1130 series access points without FCC DFS support have an *LDK102054* (no *E* suffix) sticker. 1130 series access points that are operating in the United States, Canada, or the Philippines; have an FCC ID *E* sticker; and are running the 4.1.171.0 software release or later can use channels 100 through 140 in the UNII-2 band.

Inaccurate Transmit Power Display

After you change the position of the 802.11a radio antenna for a lightweight 1200 or 1230 series access point, the power setting is not updated in the controller GUI and CLI. Regardless of the user display, the internal data is updated, and the transmit power output is changed accordingly. To see the correct transmit power display values, reboot the access point after changing the antenna's position. (CSCsf02280)

Setting the Retransmit Timeout Value for TACACS+ Servers

We recommend that the retransmit timeout value for TACACS+ authentication, authorization, and accounting servers be increased if you experience repeated reauthentication attempts or the controller falls back to the backup server when the primary server is active and reachable. The default retransmit timeout value is 2 seconds and can be increased to a maximum of 30 seconds.

Configuring Prestandard Power Setting of an Access Point

An access point can be powered by a Cisco prestandard 15-W switch with Power over Ethernet (PoE) by entering this command:

```
config ap power pre-standard {enable | disable} {all | Cisco_AP}
```

A Cisco prestandard 15-W switch does not support intelligent power management (IPM) but does have sufficient power for a standard access point. The following Cisco prestandard 15-W switches are available:

- AIR-WLC2106-K9
- WS-C3550, WS-C3560, WS-C3750
- C1880
- 2600, 2610, 2611, 2621, 2650, 2651
- 2610XM, 2611XM, 2621XM, 2650XM, 2651XM, 2691
- 2811, 2821, 2851
- 3631-telco, 3620, 3640, 3660
- 3725, 3745
- 3825, 3845

The **enable** version of this command is required for full functionality when the access point is powered by a Cisco prestandard 15-W switch. It is safe to use if the access point is powered by either an IPM switch or a power injector or if the access point is not using one of the 15-W switches listed above.

You might need this command if your radio operational status is “Down” when you expect it to be “Up.” Enter the **show msglog** command to look for this error message, which indicates a PoE problem:

```
Apr 13 09:08:24.986 spam_lrad.c:2262 LWAPP-3-MSGTAG041: AP 00:14:f1:af:f3:40 is unable to
verify sufficient in-line power. Radio slot 0 disabled.
```

Controller Functions that Require a Reboot

After you perform these functions on the controller, you must reboot the controller for the changes to take effect:

- Enable or disable link aggregation (LAG)
- Enable or disable long preambles to optimize the operation of SpectraLink NetLink phones on your wireless LAN
- Enable a feature that is dependent on certificates (such as HTTPS and web authentication)
- Install a license, change the license feature set, or change the priority of an AP-count evaluation license on a 5500 series controller

2106 Controller LEDs

The Status LED and AP LED of 2106 controllers do not flash amber when software is being uploaded to the controller or downloaded to an access point, respectively.



Note

Some versions of the *Cisco 2106 Wireless LAN Controller Quick Start Guide* might incorrectly state that these LEDs flash amber during a software upload or download.

Rate-Limiting on the Controller

Rate-limiting is applicable to all traffic destined to the CPU from either direction (wireless or wired). We recommend that you always run the controller with the default **config advanced rate enable** command in effect in order to rate limit traffic to the controller and protect against denial-of-service (DoS) attacks. You can use the **config advanced rate disable** command to stop rate-limiting of Internet Control Message Protocol (ICMP) echo responses for testing purposes. However, we recommend that you reapply the **config advanced rate enable** command after testing is complete.

Pings Supported to the Management Interface of the Controller

Controller software release 4.1.185.0 or later is designed to support ICMP pings to the management interface either from a wireless client or a wired host. ICMP pings to other interfaces configured on the controller are not supported.

Pinging from a Network Device to a Controller Dynamic Interface

Pinging from a network device to a controller dynamic interface might not work in some configurations. When pinging does operate successfully, the controller places Internet Control Message Protocol (ICMP) traffic in a low-priority queue, and the reply to ping is by best effort. Pinging does not pose a security threat to the network. The controller rate limits any traffic to the CPU, and flooding the controller is prevented. Clients on the WLAN associated with the interface pass traffic normally.

GLBP Support

The controller software 7.0.220.0 and later releases are compatible with the Gateway Load Balancing Protocol (GLBP).

4400 Series Controllers Do Not Forward Subnet Broadcasts through the Guest Tunnel

As designed, 4400 series controllers do not forward IP subnet broadcasts from the wired network to wireless clients across the EoIP guest tunnel.

Connecting 1100 and 1300 Series Access Points

You must install software release 4.0.179.8 or later on the controller before connecting 1100 and 1300 series access points to the controller.

Preventing Clients from Accessing the Management Network on a Controller

To prevent or block a wired or wireless client from accessing the management network on a controller (from the wireless client dynamic interface or VLAN), the network administrator must ensure that only authorized clients gain access to the management network through proper CPU ACLs, or use a firewall between the client dynamic interface and the management network.

Voice Wireless LAN Configuration

We recommend that aggressive load balancing always be turned off either through the controller GUI or CLI in any wireless network that is supporting voice, regardless of vendor. When aggressive load balancing is turned on, voice clients can hear an audible artifact when roaming, if the handset is refused at its first reassociation attempt.

Enabling/Disabling Band Selection and Client Load Balancing

It is not possible to enable or disable band selection and client load balancing globally through the controller GUI or CLI. You can, however, enable or disable band selection and client load balancing for a particular WLAN. Band selection and client load balancing are enabled globally by default.

Changing the IOS LWAPP Access Point Password

Cisco IOS Lightweight Access Point Protocol (LWAPP) access points have a default password of *Cisco*, and the prestage configuration for LWAPP access points is disabled by default. To enable it, you must configure the access point with a new username and password when it joins the controller. Enter this command using the controller CLI to push a new username and password to the access point:

```
config ap mgmtuser add user-id password password {Cisco_AP | all}
```

- The *Cisco_AP* parameter configures the username and password on the specified access point.
- The **all** parameter configures the username and password on all the access points registered to the controller.

The password pushed from the controller is configured as “enable password” on the access point.

There are some cases where the prestage configuration for LWAPP access points is disabled and the access point displays the following error message when the CLI commands are applied:

```
"ERROR!!! Command is disabled."
```

For more information, see *Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode* at http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80/b_cg80_chapter_01101010.html

Exclusion List Client Feature

If a client is not able to connect to an access point, and the security policy for the WLAN and client are correct, the client has probably been disabled. In the controller GUI, you can view the client’s status on the Monitor > Summary page under Client Summary. If the client is disabled, click **Remove** to clear the disabled state for that client. The client automatically comes back and, if necessary, reattempts authentication.

Automatic disabling happens as a result of too many failed authentications. Clients disabled due to failed authorization do not appear on the permanent disable display. This display is only for those MACs that are set as permanently disabled by the administrator.

Client exclusion can happen both statically and dynamically. In a static exclusion, the client is disabled permanently. In dynamic exclusion, the client is excluded until the configured exclusion timeout is reached in the WLAN.

The following client exclusion policies are available:

- Excessive 802.11 association failure
- Excessive 802.11 authentication failure
- Excessive 802.1X authentication failure
- IP theft or reuse
- Excessive web authentication failure

RADIUS Servers and the Management VLAN

If a RADIUS server is on a directly connected subnet (with respect to the controller), then that subnet must be the management VLAN subnet. If you use RADIUS interface override (using the command `config wlan radius_server overwrite-interface`), you can connect to the dynamic interface to the server.

TACACS+ and NMS Servers and the Management VLAN

If a TACACS+, or an NMS (like WCS or NCS) server is on a directly connected subnet (with respect to the controller), then that subnet must be the management VLAN subnet.

RADIUS Servers

This product has been tested with CiscoSecure ACS 4.2 and later and works with any RFC-compliant RADIUS server.

Management Usernames and Local Netuser Names

Management usernames and local netuser names must be unique because they are stored in the same database. That is, you cannot assign the same name to a management user and a local netuser.

Using the Backup Image

The controller 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, be sure to 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 controller.

Home Page Retains Web Authentication Login with IE 5.x

Because of a caching problem in the Internet Explorer 5.x browser, the home page retains the web authentication login. To correct this problem, clear the history or upgrade your workstation to Internet Explorer 6.x.

Ad-Hoc Rogue Containment

Client card implementations might mitigate the effectiveness of ad-hoc containment.

Changing the Default Values of SNMP Community Strings

The controller has commonly known default values of “public” and “private” for the read-only and read-write SNMP community strings. Using these standard values presents a security risk. Therefore, We strongly advise that you change these values. See the *Cisco Wireless LAN Controller Configuration Guide, Release 7.0.116.0*, for configuration instructions.

Changing the Default Values for SNMP v3 Users

The controller uses a default value of “default” for the username, authentication password, and privacy password for SNMP v3 users. Using these standard values presents a security risk. Therefore, we strongly advise that you change these values. See the *Cisco Wireless LAN Controller Configuration Guide, Release 7.0.116.0*, for configuration instructions.

**Note**

SNMP v3 is time sensitive. Ensure that you have configured the correct time and time zone on your controller.

DirectStream Feature Is Not Supported With WGB

The DirectStream feature from the controller does not work for clients behind workgroup bridges and the stream is denied.

No Support for Jumbo Frames

The controller does not support transmitting of jumbo frames. To avoid having the controller transmit CAPWAP packets to the AP that necessitates fragmentation and reassembly, reduce the MTU/MSS on the client side.

Enforce a minimum configured data rate

24Mbps is always enabled even if you select OFDM rates that are less than 24Mbps.

Features Not Supported on Cisco 2100 Series Controllers

This hardware feature is not supported on 2100 series controllers:

- Service port (separate out-of-band management 10/100-Mbps Ethernet interface)
- The Cisco 2100 Series Controllers do not support AP801 and AP802 access points.

These software features are not supported on 2100 series controllers:

- VPN termination (such as IPsec and L2TP)
- VPN passthrough option



Note You can replicate this functionality on a 2100 series controller by creating an open WLAN using an ACL.

- Termination of guest controller tunnels (origination of guest controller tunnels is supported)
- External web authentication web server list
- Spanning Tree Protocol (STP)
- Port mirroring
- AppleTalk
- QoS per-user bandwidth contracts
- IPv6 pass-through
- Link aggregation (LAG)
- Multicast-unicast mode

Features Not Supported on Cisco 2500 Series Controllers

These software features are not supported on Cisco 2500 Series Controllers:

- Support for wired guest access.
- Cisco 2500 Series Controller cannot be configured as an auto anchor controller. However you can configure it as a foreign controller.
- Supports only multicast-multicast mode.
- Bandwidth Contract feature is unsupported.
- Access points in direct connect mode is unsupported
- Service port support
- Apple Talk Bridging
- LAG
- Wired Guest

Features Not Supported on Cisco 5500 Series Controllers

These software features are not supported on Cisco 5500 Series Controllers:

- Static AP-manager interface—this interface is not required for the Cisco 5500 Series controllers.



Note For 5500 series controllers, you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default, and the access points can join on this interface.

- Asymmetric mobility tunneling
- Spanning Tree Protocol (STP)
- Port mirroring

- Layer 2 access control list (ACL) support
- VPN termination (such as IPsec and L2TP)
- VPN passthrough option



Note You can replicate this functionality on a 5500 series controller by creating an open WLAN using an ACL.

- Configuration of 802.3 bridging, AppleTalk, and Point-to-Point Protocol over Ethernet (PPPoE)

Features Not Supported on Cisco Flex 7500 Series Controllers

These software features are not supported on Cisco Flex 7500 Series Controllers:

- Static AP-manager interface



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

- L3 Roaming
- VideoStream
- WGB
- Client rate limiting for centrally switched clients
- Access points in local mode



Note AP associated with the controller in local mode should be converted to H-REAP mode or Monitor mode.

- Mesh
- LAG
- Spanning Tree Protocol (STP)
- Cisco Flex 7500 Controller as a guest controller
- Multicast
- ACLs
- P2P Blocking

Some Clients See Only 64 Access Point MAC Addresses (BSSIDs) at a Time

In a crowded RF environment, clients might not be able to detect the desired SSID because of internal table limitations. Sometimes disabling and then enabling the client interface forces a rescan. Your RF environment needs to be controlled. Cisco UWN rogue access point detection and containment can help you to enforce RF policies in your buildings and campuses.

Upgrading External Web Authentication

When upgrading a controller from operating system release 2.0 or 2.2.127.4 to release 3.2.116.21 or later, update the external web authentication configuration as follows:

1. For Cisco 5500 Series Controllers, 2100 Series Controllers, and controller network modules, you must configure a preauthentication access control list (ACL) on the WLAN for the external web server and then choose this ACL as the WLAN preauthentication ACL under **Security Policies > Web Policy** on the WLANs > Edit page.
2. For Cisco 4400 Series Controllers and the Cisco WiSM, instead of using a preauthentication ACL, the network manager must configure the external web server IP address using this command:

```
config custom-web ext-webserver add index IP-address
```



Note *IP-address* is the address of any web server that performs external web authentication.

3. The network manager must use the new `login_template` shown here as follows:



Note Ensure to format the script to avoid any extra characters or spaces before using the web authentication template.

```
<html>
<head>
<meta http-equiv="Pragma" content="no-cache"> <meta HTTP-EQUIV="Content-Type"
CONTENT="text/html; charset=iso-8859-1"> <title>Web Authentication</title> <script>

function submitAction(){
    var link = document.location.href;
    var searchString = "redirect=";
    var equalIndex = link.indexOf(searchString);
    var redirectUrl = "";
    var urlStr = "";
    if(equalIndex > 0) {
        equalIndex += searchString.length;
        urlStr = link.substring(equalIndex);
        if(urlStr.length > 0){
            redirectUrl += urlStr;
            if(redirectUrl.length > 255)
                redirectUrl = redirectUrl.substring(0,255);
            document.forms[0].redirect_url.value = redirectUrl;
        }
    }

    document.forms[0].buttonClicked.value = 4;
    document.forms[0].submit();
}

function loadAction(){
    var url = window.location.href;
    var args = new Object();
    var query = location.search.substring(1);
    var pairs = query.split("&");
    for(var i=0;i<pairs.length;i++){
        var pos = pairs[i].indexOf('=');
        if(pos == -1) continue;
        var argname = pairs[i].substring(0,pos);
        var value = pairs[i].substring(pos+1);
```

```
        args[argname] = unescape(value);
    }
    //alert( "AP MAC Address is " + args.ap_mac);
    //alert( "The Switch URL is " + args.switch_url);
    document.forms[0].action = args.switch_url;

    // This is the status code returned from webauth login action
    // Any value of status code from 1 to 5 is error condition and user
    // should be shown error as below or modify the message as it suits
    // the customer
    if(args.statusCode == 1){
        alert("You are already logged in. No further action is required on your
part.");
    }
    else if(args.statusCode == 2){
        alert("You are not configured to authenticate against web portal. No further
action is required on your part.");
    }
    else if(args.statusCode == 3){
        alert("The username specified cannot be used at this time. Perhaps the user is
already logged into the system?");
    }
    else if(args.statusCode == 4){
        alert("Wrong username and password. Please try again.");
    }
    else if(args.statusCode == 5){
        alert("The User Name and Password combination you have entered is invalid.
Please try again.");
    }
}

</script>
</head>
<body topmargin="50" marginheight="50" onload="loadAction();" ><form method="post">
<input TYPE="hidden" NAME="buttonClicked" SIZE="16" MAXLENGTH="15" value="0">
<input TYPE="hidden" NAME="redirect_url" SIZE="255" MAXLENGTH="255" VALUE="">
<input TYPE="hidden" NAME="err_flag" SIZE="16" MAXLENGTH="15" value="0">

<div align="center">
<table border="0" cellspacing="0" cellpadding="0"> <tr> <td>&nbsp;&nbsp;&nbsp;</td></tr>

<tr align="center"> <td colspan="2"><font size="10" color="#336699">
Web Authentication</font></td></tr>

<tr align="center">

<td colspan="2"> User Name &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<input type="TEXT" name="username"
SIZE="25" MAXLENGTH="63" VALUE=""> </td> </tr> <tr align="center" > <td colspan="2">
Password &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<input type="Password" name="password"
SIZE="25" MAXLENGTH="24"> </td> </tr>

<tr align="center">
<td colspan="2"><input type="button" name="Submit" value="Submit" class="button"
onclick="submitAction();"> </td> </tr> </table> </div>

</form>
</body>
</html>
```


Switch Port and Controller Port

When the port status on the controller changes, the switch status does not get changed. This is a known issue. For example, when the controller port goes down, the switch port is still in the administrable state. This has been resolved in Cisco 5500 Series Controllers.

Unsupported mac-address Command for Unified and Autonomous Access Points

The unified and autonomous access point do not support the **mac-address** command for the wireless interfaces. When invoked, the command executes but can cause the access point to fail.

Fast Roaming and Authentication/Key Management for CCKM Clients

CCKM Fast-roaming clients in hybrid REAP mode works only with the following authentication or key management combinations:

- WPA2+AES
- WPA+TKIP

CCKM Fast-roaming clients in hybrid REAP mode is not supported with the following authentication or key management combinations:

- WPA+AES
- WPA2+TKIP

Errors When Using AAA with an Active RADIUS Fallback

Consider a scenario where you configured the active RADIUS fallback feature using AAA for a controller. When using this feature, the controller sends the accounting request probes without the session ID during a fallback, which might be dropped by the RADIUS Server. The controller cannot send accounting information with the session ID because during the fallback the controller does not have the context of the client. Some RADIUS Servers like ISE might report errors for accounting probes that are sent to ISE. If your Authentication and Accounting servers are the same, ignore the errors that are logged in ISE.

Roaming Clients When Access Points are in Standalone Mode

When access points are in standalone mode, they are not aware the states and status of the clients associated with the access points. For example, consider a scenario where two clients (Client 1 and Client 2) are communicating with each other. Also, assume that both the clients are associated with same access point (say, AP1). Let us also assume that both AP1 and AP2 are in standalone mode. Now, if Client 1 roams to AP2, the packets sent from Client 2 do not reach Client 1.

Using Lightweight Access Points with NAT

You can place a lightweight access point under NAT. On the access point side, you can have any type of NAT configured. However, when you configure the controller, you can have only 1:1 (Static NAT) configured and the external NAT IP address configured on the dynamic AP management interface. This situation is applicable only for Cisco 5500 Series Controllers. NAT cannot be configured on the controller because LAPs cannot respond to controllers if the ports are translated to ports other than 5246 or 5247, which are meant for control and data messages.



Note

Select the Enable NAT Address check box and enter the external NAT IP address if you want to be able to deploy your Cisco 5500 Series Controller behind a router or other gateway device that is using one-to-one mapping network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a local network (private). In this case, it maps the controller's intranet IP addresses to a corresponding external address. The dynamic AP-manager interface of the controller must be configured with the external NAT IP address so that the controller can send the correct IP address in the Discovery Response.



Note

With CAPWAP, a controller behind NAT is not supported with the Cisco 4400 Series, 2100 Series Wireless LAN Controllers, and the WiSM.

Default A-MPDU settings

By default, Aggregated MAC Protocol Data Unit (A-MPDU) is enabled for priority level 0, 4 and 5 and the rest are disabled. In releases prior to 6.0 release, only priority 0 was enabled by default. The video performance is enhanced when priorities 4 and 5 are enabled for A-MPDU aggregation.

Important Notes for Controllers and Mesh Access Points

This section describes important information about controllers and mesh access points.

Features Not Supported on Mesh Networks

The following controller features are not supported on mesh networks:

- Multi-country support
- Load-based CAC (mesh networks support only bandwidth-based, or static, CAC)
- High availability (fast heartbeat and primary discovery join timer)
- EAP-FASTv1 and 802.1X authentication
- Access point join priority (mesh access points have a fixed priority)
- Locally significant certificate
- Location-based services

Caveats

The following sections lists [Open Caveats](#) and [Resolved Caveats](#) for Cisco WLCs and lightweight access points for Release 7.0.252.0. To enable you to locate caveats in the Cisco Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms might be standardized.
- Spelling errors and typos might be corrected.

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

<https://tools.cisco.com/bugsearch/search>



Note

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

Open Caveats

Table 6 lists open caveats in controller software release 7.0.252.0.

Table 6 Open Caveats

ID	Description
CSCts55071	<p>Symptom: A WLC may unexpectedly reload with a failure in the crashfile similar to the following:</p> <pre>Software was stopped by the reaper for the following reason: Reaper Reset: Task "spamReceiveTask" missed software watchdog Just prior to the crash, the msglog is full of messages like these: *spamApTask0: May 30 00:42:13.648: %LWAPP-3-MSG_SEND_ERR2: spam_api.c:10804 Unable to send MFP key set message to LWAPP *spamApTask0: May 30 00:42:13.648: %OSAPI-4-MSGQ_SEND_FAILED: osapi_msgq.c:518 Failed to send a message to the message queue object: SPAM-Q . enqueue failed.</pre> <p>Condition: Infrastructure MFP enabled.</p> <p>Workaround: Disable infrastructure MFP.</p>
CSCui25170	<p>Symptom 1: A WLC's management interface is not reachable via IP. Msglog reports messages similar to this:</p> <pre>*broffu_SocketReceive: Oct 20 07:31:15.291: #BROFFU-0-DP_BUFFER_POOL_LOW_DETECTED: broffu_fp_dapi_cmd.c:5060 Warning: DP Early PacketBuffer low detected. DP1 PacketBuffer=26105 (<?26200) WQE=102318 (<?26200)</pre> <p>Symptom 2: An AP is unable to join the WLC. The AP sends CAPWAP DISCOVERY REQUEST IPv4 broadcasts, but the WLC ignores them.</p> <p>Condition: In the symptom 1 case, there are PMIPv6 (IPv4, UDP port 5346) packets in the network that are addressed to wireless clients. The WLC generates a forwarding loop for these packets.</p> <p>In the symptom 2 case, the AP relies on CAPWAP broadcast to discover the WLC (i.e., the AP is on the WLC's management interface's subnet, or an IP helper-address is used on the AP's subnet.)</p> <p>Workaround: For Symptom 1, configure a CPU ACL (switch ACL or WLC CPU ACL) to block the PMIPv6 packets from reaching the WLC.</p>
CSCud84109	<p>Symptom: When adding a new Dual Band AP to a controller with multiple countries, the AP may select a country in a different regulatory domain than that of the AP.</p> <p>Condition: With a new dual band Access Point joining a controller with countries in regulatory domains for -A and -N. The AP will select the country in the -N regulatory domain.</p> <p>Dual Band AP examples: 3600, 3500, 1140, 1240, etc.</p> <p>Workaround: Select the correct country and enable the AP admin state.</p>

Table 6 **Open Caveats (continued)**

ID	Description
CSCug42330	<p>Symptom: Interface ACL on WLC may incorrectly apply on all the interfaces even on the one it is not applied on.</p> <p>Condition: WLC running software codes 7.0 to 7.3.</p> <p>Workaround: None.</p>
CSCsv54436	<p>Symptom: While doing SSH to the controller, it is sometimes denied with the “Sorry, telnet is not allowed on this port” message.</p> <p>If the same PC, the same controller, retries immediately, the SSH connection is accepted. No changes in between.</p> <p>Condition: SSH connection is performed from a different L3 network; issue found both in Cisco 2100 and 4400 series controllers.</p> <p>This is breaking monitoring tools through SSH.</p> <p>Workaround: Retry SSH connection.</p>
CSCta77755	<p>Symptom: Third-party certificate is missing on a WLC.</p> <p>Conditions: This can occur after transferring a configuration file from a Cisco WLC that has a third-party certificate installed on a new Cisco WLC. Another condition might be if the Cisco WLC was restored to factory defaults and the old configuration was transferred back to the WLC.</p> <p>Workaround: None.</p> <p>Further Problem Description: The configuration file does not contain any third-party certificates. If a third-party certificate is required on the new WLC, you must install the certificate through the TFTP transfer of the .pem file and provide the corresponding certificate password.</p>
CSCtb77395	<p>Symptom: Syslog entries appear on the server.</p> <p>Conditions: Normal.</p> <p>Workaround: None.</p>

Table 6 Open Caveats (continued)

ID	Description
CSCtj06944	<p>Symptom: A Cisco 5500 Series controller or Cisco WiSM2 might stop working with messages similar to the following displayed on the console log:</p> <pre>Kernel panic - not syncing: Failed to allocate skb for hardware pool 0 LKCD:Dumping from interrupt handler! 262144 pages of RAM 0 pages of HIGHMEM 10968 reserved pages 5010 pages shared 0 pages swap cached swapper: page allocation failure. order:0, mode:0x20 Call Trace: [<ffffffff81126b28>] dump_stack 0x8/0x48 [<ffffffff81196de4>] __alloc_pages 0x32c/0x3c0 [<ffffffff811b56a8>] cache_alloc_refill 0x398/0x6e8 [<ffffffff811b5b50>] __kmalloc 0x158/0x168 [<c0000000003f758c>] ssh_kernel_alloc 0x5c/0x1b0 [sshquicksec] [<c0000000003faec>] ssh_interceptor_packet_alloc_header 0x64c/0x708 [sshquicksec] [<c0000000004947e0>] ssh_interceptor_packet_in 0xe8/0x750 [sshquicksec]</pre> <p>Conditions:</p> <ul style="list-style-type: none"> • The service port on the Cisco WLC is plugged into a VLAN, which is also present on one of the Cisco WLC's uplink interfaces. • Service port plugged to a VLAN carrying heavy broadcast/multicast traffic. <p>Workaround: Options include the following:</p> <ul style="list-style-type: none"> • Unplug the service port, or connect the service port to a VLAN, which is not switched to the Cisco WLC's uplink interfaces. • Plug the service port to a VLAN with low broadcast/multicast traffic. <p>Further Problem Description: If the service port is connected to the switched network, you must configure the service port into a VLAN that is not connected to the Cisco WLC's distribution ports. The service port in a VLAN that is in use by the Cisco WLC's management, AP-Manager or dynamic interfaces is not a valid configuration.</p>
CSCtk65207	<p>Symptom: MFP anomalies are reported due to invalid MIC violations.</p> <p>Conditions: Both the detector and the generator AP are part of the same mobility group.</p> <p>Workaround: Disable MFP globally.</p>

Table 6 *Open Caveats (continued)*

ID	Description
CSCtn52995	<p>Symptom: H-REAP—Reached the limit on the association ID for AP or messages similar to the following is displayed in the message log:</p> <pre>*apfMsConnTask_6: May 29 10:15:57.758: #APF-3-AID_UPDATE_FAILED: apf_80211.c:9041 Error updating Association ID for REAP AP Client00:ac:fd:00:8f:00 - AID 41 *apfMsConnTask_6: May 29 10:15:57.758: #LWAPP-3-INVALID_AID2: spam_api.c:1357 Association identifier 41 for client 00:d2:d1:01:11:f2 is already in use by 00:d2:d1:01:10:29 At this time, clients are unable to associate on the given BSSID on the given AP.</pre> <p>Conditions:</p> <ol style="list-style-type: none"> 1. H-REAP. 2. Client 1 is associated with the controller with AID=1 on SSID X. 3. Client 1 sends 802.11 authentication frame on SSID Y; at this point, AID=1 is freed at the AP. Authentication frames are not honored at the controller; therefore, the controller is not informed 4. No association frame arrives from client 1 at SSID 2. 5. Client 2 associates with the AP and gets AID=1. 6. AP updates the controller about client 2 and AID=1; at this point, the controller adds duplicate entries and increments the count (controller already has client 1 AID=1). Counter gets incremented and is reaching 256. It is due to the network conditions at the customer site in which the 802.11 authentication frames are sent (sometimes on different WLANs), but is not followed by association frames. <p>Workaround: None.</p>
CSCto61773	<p>Symptom: Auto contain and auto RLDP commands do not work independently.</p> <p>Conditions: Using CLI, if auto contain is enabled for 'rogue on wire' and an attempt is made to enable auto RLDP for only the monitor mode APs, then auto contain configuration gets disabled. The same issue can be seen if the commands are tried in the reverse order.</p> <p>Workaround: Use the GUI to configure auto contain 'rogue on wire' and auto RLDP using only the monitor mode APs.</p>
CSCto95594	<p>Symptom: This issue is based on the XML configuration file. There is no command found XML file. Thus, when the configuration file is downloaded to the controller, the rogue on wire is disabled.</p> <p>Conditions: Uploaded the configuration file from the TFTP server.</p> <p>Workaround: There is no specific command to enable the rogue on wire. This needs to be enabled.</p>
CSCtq91516	<p>Symptom: Unable to configure LAG when there is an untagged interface.</p> <p>Conditions: If untagged interface is present on the controller and mapped to an interface group, then when you enable LAG, the controller tries to delete untagged interface, which is expected but the interface is not deleted because it is mapped to an interface group.</p> <p>Workaround: Remove interface for interface group.</p>

Table 6 **Open Caveats (continued)**

ID	Description
CSCtq91573	<p>Symptom:</p> <ul style="list-style-type: none"> • User is unable to configure LAG. • User is unable to disable NAC on a WLAN mapped to an interface group. • Incorrect error message is displayed: “NAC OOB can not be disabled as AP Groups have NAC enabled on this WLAN/Guest-Lan/remote-lan.” <p>Conditions: WLAN is configured with NAC in enabled state and mapped to an interface group.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. Remove the interface group from the WLAN, and replace with a single interface (with a quarantine VLAN assigned). 2. Remove the WLAN, and re-create.
CSCtr22540	<p>Symptom: Removing an entry from an ACL, which is applied on CPU has no effect; the modifications are not applied.</p> <p>Conditions: Not applicable.</p> <p>Workaround: Reapply the ACL on the CPU.</p>
CSCts14535	<p>Symptom: Client entry on the Cisco WLC is not updated by H-REAP when the AP is in standalone mode.</p> <p>Conditions: Client roams on standalone mode APs, which then connect back to the controller in connected mode. Cisco 5508 WLC using Release 7.0.116.0.</p> <p>Workaround: None.</p>
CSCts23174	<p>Symptom: In AIR-CT7510 controller, the AP-Manager interface cannot be removed using the GUI.</p> <p>Conditions: Only AIR-CT7510 is affected.</p> <p>Workaround: Remove the AP-manager interface using CLI by entering this command:</p> <pre>(Cisco Controller) >config interface delete interface-name</pre>
CSCts54424	<p>Symptom: Web authentication on MAC filter failure does not correctly bypass web authentication for valid MAC address clients on an anchored WLAN.</p> <p>Conditions: Release 7.0.116.0; using web authentication on MAC filter failure and WLAN anchor.</p> <p>Workaround: If possible, do not anchor the WLAN in question. Use two separate WLANs (one MAC filter, one web-auth).</p>

Table 6 *Open Caveats (continued)*

ID	Description
CSCtt00022	<p>Symptom: Cisco WLC SNMP walk output are inconsistent. From Cisco 5508 WLC:</p> <pre data-bbox="589 394 1521 632">[5508WLC]\$ snmpwalk -v 2c -c xxxxxxxxxx 10.19.x.x IF-MIB::ifSpeed IF-MIB::ifSpeed.1 = Gauge32: 1000000000 IF-MIB::ifSpeed.2 = Gauge32: 1000000000 [5508WLC]\$ snmpwalk -v 2c -c xxxxxxxxxx 10.19.x.x IF-MIB::ifHighSpeed IF-MIB::ifHighSpeed.1 = Gauge32: 100 IF-MIB::ifHighSpeed.2 = Gauge32: 100 WiSM2 output [root@utnetnms ~]# snmpwalk -v 2c -c xxxxxxxxxx 10.19.5.22 IF-MIB::ifSpeed IF-MIB::ifSpeed.1 = Gauge32: 0 IF-MIB::ifSpeed.2 = Gauge32: 0 [root@utnetnms ~]# snmpwalk -v 2c -c xxxxxxxxxx 10.19.5.22 IF-MIB::ifHighSpeed IF-MIB::ifHighSpeed.1 = Gauge32: 100 IF-MIB::ifHighSpeed.2 = Gauge32: 100</pre> <p>Conditions: Customer is monitoring WiSM2 interface using a monitoring tool system developed by themselves based on Cisco MIBs—SNMP walk. They are reporting back at 100 Mbps interfaces when the SNMP description shows that the interfaces are 1 Gbps. The WiSM2 interface is supposed to be 10Gbps.</p> <p>Workaround: None.</p>
CSCtt94557	<p>Symptom: Tags using CCX format had to compulsorily use the CCX multicast address 01:40:96:00:00:03. Tags using other multicast addresses were interpreted as non-CCX address.</p> <p>Conditions: Tags using the multicast address 01:0C:CC:00:00:00 were interpreted as non-CCX tags even though they were using CCX tag format.</p> <p>Workaround: Configure the tags to use the CCX multicast address 01:40:96:00:00:03. Tags will be detected as CCX tags.</p> <p>Further Problem Description: According to the CCX specifications, for a tag to be interpreted as a CCX tag, the tag has to use the multicast address 01:40:96:00:00:03. However, customers might have configured CCX tags with other multicast address.</p>
CSCtu39166	<p>Symptom: AP rebooted with information about the problem created during normal operation.</p> <p>Conditions: Normal operation.</p> <p>Workaround: None.</p>
CSCtw69980	<p>Symptom: Configuring a few multiple WLC country codes seems to insert invalid channels 17 & 21 on the 2.4 GHz 802.11b/g/n DCA list.</p> <p>Conditions: Configure WLC multiple country codes where at least one of the following is included as well as a country code not in this list (for example, US): BY Belarus EG Egypt ILO Israel (Outdoor) MK Macedonia TR Turkey.</p> <p>Workaround: None.</p>
CSCtw84572	<p>Symptom: Cannot search based on the Ethernet MAC address and supporting OEAP users, they only would have access to the AP itself, and this is where the MAC address of the Ethernet interface is printed on the bottom of the AP.</p> <p>Conditions: When APs cannot join, it is difficult to look up the AP's join statistics.</p> <p>Workaround: Look up in NCS/WCS.</p>

Table 6 Open Caveats (continued)

ID	Description
CSCty40179	<p>Symptom: Cannot change H-REAP VLAN mapping. The following error message is displayed:</p> <pre>WLAN ID 3 cannot be altered</pre> <p>Conditions: The issue is that the SSID “SAW_Voice_Authorised_Access_only” exceeds 31 bytes. While it is possible to create an SSID profile with 32 bytes, as part of profile payload, you can store only 31 bytes, which leads to mismatch and therefore the controller does not allow you to change the VLAN, which is the reason why only this particular WLAN causes issues.</p> <p>Workaround: Do not exceed the 31 bytes when you create SSID profile.</p>
CSCub07050	<p>Symptom: Interface port mapping configuration can be lost on Cisco 2500 WLC.</p> <p>Conditions: If LAG is enabled on 7.4 or later releases and downgrade is performed to 7.3 or lower on Cisco 2500 WLC, interface port mapping configuration will be lost after downgrade and will have to be redone.</p> <p>Workaround: Configuration for interface port mapping will have to be redone and saved after downgrade.</p>
CSCuc98178	<p>Symptom: Unconfiguring HSRP will lead CAPWAP APs to keep sending data traffic to the old HSRP MAC while the control traffic is sent to the new correct gateway MAC.</p> <p>Conditions: Release 7.2, 3500 APs, and HSRP gateway.</p> <p>Workaround: Reboot the AP.</p>
CSCud57784	<p>Symptom: With Cisco 5508 WLC using MAC filtering authentication:</p> <ol style="list-style-type: none"> 1. On the WLC GUI, choose Security > AAA > RADIUS > Authentication, define more than one RADIUS server. 2. Choose Security > AAA > MAC Filtering, set “RADIUS Compatibility Mode” as “Free RADIUS”. 3. In the WLAN settings, check “MAC Filtering,” select Authentication server which is defined in step 1 and also has index number 1. In this situation, everything is normal. 4. Choose Security > AAA > RADIUS > Authentication, delete the RADIUS server which has index number 1. 5. In the WLAN settings, select Authentication server, which has an index number other than 1. In this scenario, client authentication fails. <p>Conditions: Unknown.</p> <p>Workaround: On the WLC GUI, choose Security > AAA > RADIUS > Authentication, define a dummy RADIUS server, which has an index as 1.</p>
CSCud84109	<p>Symptom: When adding a new dual band AP to a controller with multiple countries, the AP might select a country in a different regulatory domain than that of the AP.</p> <p>Conditions: With a new dual band AP associating with a controller with countries in regulatory domains for –A and –N. The AP selects the country in the –N regulatory domain. Dual band AP examples: 3600, 3500, 1140, 1240, and so on.</p> <p>Workaround: Select the correct country and enable the AP admin state.</p>

Table 6 **Open Caveats (continued)**

ID	Description
CSCue83738	<p>Symptom: The rogue AP, which is not connected to the network by cable, is contained as malicious by the Cisco WLC abnormally in certain conditions.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCui24995	<p>Symptom: It is seen on client authentication for an H-REAP in the standalone mode that the Called-Station-ID attributes do not contain the SSID information.</p> <p>Conditions: AP configured for local RADIUS support.</p> <p>Workaround: Use Cisco WLC for authentication.</p>
CSCui42023	<p>Symptom: Deauthenticate the RADIO MAC of MAP, it never joined back.</p> <p>Conditions: Let a mesh AP associate with the WLC. Deauthenticate the RADIO MAC of the MAP using the config client deauthenticate RADIO-MAC command and reboot the MAP.</p> <p>Workaround: Reboot the Cisco WLC.</p>
CSCui75794	<p>Symptom: The foreign WLC does not respond to ARP from foreign export client to a local client being on the same VLAN.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • Client1 associates with WLC1 (local) • Client1 does L3 roam to WLC2 (WLC2: foreign / WLC1: anchor) • Client2 associates with WLC2 (local) • Initiate traffic (i.e., ping from Client1 to Client2) <p>Workaround: None.</p> <p>More Information: This bug fix CSCui75794 is only a partial fix. To get the complete fix, run an image that also has the fix for CSCug80814.</p>
CSCul76414	<p>Symptom: Some APs showed 0 percent utilization when the show run command is entered on the Cisco WLC.</p> <p>Conditions:</p> <ol style="list-style-type: none"> 1. Cisco WLC Release 7.0 with AP 3500 2. Cisco WLC Release 7.2 with AP 3500 <p>Workaround: After a few seconds, use the same command again.</p>
CSCul85504	<p>Symptom: Wireless clients remain in an excluded state and cannot associate with the network although the client MAC address is not in the client exclusion list.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCum57354	<p>Symptom: DHCP option 7 for log server information does not work.</p> <p>Conditions: AP syslog server configured on Cisco WLC overrides DHCP option 7.</p> <p>Workaround: Configure AP syslog server in Cisco WLC.</p>

Table 6 **Open Caveats (continued)**

ID	Description
CSCum57384	<p>Symptom: Traceback in AP console.</p> <p>Conditions: Cisco 1524PS mesh AP with this release.</p> <p>Workaround: None.</p>
CSCum62697	<p>Symptom: Web authentication precedence is not uploaded to the configuration file.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCum74416	<p>Symptom: According to the GUI on the WLC, multicast video traffic shows a user priority of '0' even though it is actually prioritized as priority '4' in the VLAN and verified with a sniffer as having an actual priority of 4.</p> <p>Conditions: Cisco 5500 Series WLC; AP mode—H-REAP multicast traffic video streams.</p> <p>Workaround: None.</p>
CSCum89780	<p>Symptom: You must check the FPGA and other related components revision/version using the show sysinfo command before installing any Field Upgrade Software (FUS) images. There is a severe risk to install duplicated FUS image on top of the appliance which actually does not need FUS upgrade. In worst cases, the appliance could become unable to be booted or recovered. DoA/RMA is required if that is the case. This is not a bug but an enhancement to prevent users from installing unnecessary duplicated FUS image on the WLC appliances.</p> <p>Conditions: Installing FUS images on WLC appliances.</p> <p>Workaround: You must check if the box has been applied with necessary FUS image before installing any FUS images. The show sysinfo command shows the components revision/version, which are described in FUS image Release Notes.</p>
CSCum93363	<p>Symptom: Battery temperature of mesh CAP1552E shows abnormally high reading.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCum93754	<p>Symptom: The Bronze QoS profile does not experience translations; shows DSCP 0x02: Unknown sniffed at the ap switch port.</p> <p>Conditions: QoS profile mapped to WLAN>Bronze.</p> <p>Workaround: None.</p>
CSCut54330	<p>Symptom: WLC crashes on emWeb task.</p> <p>Conditions:</p> <p>The following commands are entered without passing any argument over Telnet or SSH:</p> <p>config ap lifetime-check mic</p> <p>config ap lifetime-check ssc</p> <p>Workaround: None needed.</p> <p>The trigger is incomplete command, not happening during normal code execution. Crash is not reproducible over console; only applies to Telnet/SSH connections.</p>

Resolved Caveats

Table 7 lists caveats resolved in controller software release 7.0.252.0.

Table 7 **Resolved Caveats**

ID	Title
CSCus42727	JANUARY 2015 OpenSSL Vulnerabilities
CSCus46861	LIZRD attack: Denial of Service
CSCuq19142	LAP/WLC MIC lifetime expiration causes DTLS failure
CSCus69513	WLC: Evaluation of glibc GHOST vulnerability - CVE-2015-0235

Service and Support

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at this URL: <http://www.cisco.com/c/en/us/support/index.html>

Click **Product Support** > **Wireless**. Then choose your product and **Troubleshooting** to find information on the problem you are experiencing.

Omissions

The Package Contents section in the *Quick Start Guide: Cisco 4400 Series Wireless LAN Controllers* should be updated to include this item, which is included with the 4400 series controller:

- DB-9-to-DB-9 null modem cable

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 LAN Controller Configuration Guide*
- *Cisco Wireless LAN Controller Command Reference*
- *Cisco Wireless LAN Controller System Message Guide*
- *Cisco Wireless Mesh Access Points, Design and Deployment Guide*

You can access these documents at this URL: <http://www.cisco.com/c/en/us/support/index.html>

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).

- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

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

© 2015 Cisco Systems, Inc. All rights reserved.