# Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.1.91.0

**First Published: November 8, 2011**
**OL-19342-07**

These release notes describe open and resolved caveats for release 7.1.91.0 for Cisco 2500, 5500, WiSM2, WLCM2, and Cisco Flex 7500 Series Wireless LAN Controllers. 7.1.91.0 is a special release to introduce the Cisco Aironet 3600 Access Points. Ongoing support for this release will not be provided and is not supported in any other 7.0 maintenance release.

The release 7.1.91.0 for the AP-3600 is a restricted lifetime release, with no planned maintenance images. For future fix and feature development, customers are encouraged to migrate to next major release for ongoing support and improvements.

**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:

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

# Cisco Unified Wireless Network Solution Components

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

- Software release 7.1.91.0 for all Cisco controllers and lightweight access points
- Cisco IOS version 12.4(23c)JY
- Cisco autonomous to lightweight mode upgrade tool release 3.0
- Cisco Wireless Control System (WCS) software release 7.0.220.0
- Cisco WCS Navigator 1.6.220.0
- Mobility services engine software release 7.0.220.0 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. See the *Release Notes for Cisco 3350 Mobility Services Engine for Software Release 7.0* for more information.

- Cisco 3350, 3310 Mobility Services Engines
- Cisco 2500 Series Wireless LAN Controllers
- Cisco 5500 Series Wireless LAN Controllers
- Cisco Flex 7500 Series Wireless LAN Controllers
- Cisco Wireless Services Module 2 (WiSM2) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers
- Cisco 3201 Wireless Mobile Interface Cards (WMICs)
- Cisco Aironet 1130AG, 1240AG, 1550, 1522, 1552S, and 1524 Mesh Access Points
- Cisco Aironet 1130, 1140, 1240, 1250, 1260, 3500, 1040, OEAP 600 Series Access Points, 1522, 1552S, 1524, 1550, 3500p, AP801, and AP802 Series Lightweight Access Points

**Note** Cisco Aironet 1100, 1200, 1300 Access Points; Cisco 2100, 4400 Series Wireless LAN Controllers, and Cisco WiSM are not supported in this release.

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/en/US/prod/collateral/routers/ps380/data_sheet_c78_461543.html
- AP880:
  - http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78_459542_ps380_Products_Data_Sheet.html
  - http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78-613481.html
  - http://www.cisco.com/en/US/prod/collateral/routers/ps380/ps10082/data_sheet_c78_498096.html
  - http://www.cisco.com/en/US/prod/collateral/routers/ps380/ps10082/data_sheet_c78-682548.html
- AP890:

  http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78-519930.html

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

# 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 6.0 SP1 (or later) or Mozilla Firefox 2.0.0.11 (or later)

# MIB Files

Cisco controllers support standard SNMP Management Information Base (MIB) files. MIBs can be downloaded from the Software Center on Cisco.com. Only one MIB is posted per major release (7.0.220.0, 7.0.116.0, 7.0.98.0, 6.0, 5.2, 5.1, and so on). If an updated MIB becomes available, the previous version is removed from the Software Center and replaced by the new version.

# New Features

Two new Access Point platforms (3600 Series) are supported in this Controller release (7.1.91.0).

There are no other new software features in this release.

# 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 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.

## 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 7.1.91.0

Before upgrading your controller to software release 7.1.91.0, you must comply with the following rules:

- 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 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.
- Make sure 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 7.1.91.0 is larger than 32 MB; therefore, you must make sure 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 7.1.91.0 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 7.1.91.0. Table 1-1 shows the upgrade path that you must follow before downloading software release 7.1.91.0.
- Before you use an AP802 series lightweight access point with controller software release 7.1.91.0, 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 joined to the controller are upgraded to the intermediate release before you install the 7.1.91.0 software. In large networks, it can take some time to download the software on each access point.

- If you upgrade to the controller software release 7.1.91.0 from an earlier release, you must also upgrade WCS to 7.0.220.0 and MSE to 7.0.220.0.
- It is not possible to upgrade or downgrade a new image if FIPS is enabled.
- 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.

*Table 1-1 Upgrade Path to Controller Software Release 7.1.91.0*

| Current Software Release | Upgrade Path to 7.1.91.0 Software |
|---|---|
| 6.0.188.0 or later 6.0 release | You can upgrade directly to 7.1.91.0. |
| 6.0.196.0 or later 6.0 release | You can upgrade directly to 7.1.91.0. |
| 7.0.98.0 | You can upgrade directly to 7.1.91.0. |
| 7.0.98.218 | You can upgrade directly to 7.1.91.0. |

## Software Release Support for Access Points

Table 1-2 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 1-2 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 | |
| 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 | — |

*Table 1-2 Software Support for Access Points (continued)*

| Access Points | | First Support | Last Support |
|---|---|---|---|
| 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 1-2 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 | |
| 3600e | AIR-CAP3602E-x-K9 | 7.1.91.0 | |
| 3600i | AIR-CAP3602I-x-K9 | 7.1.91.0 | |

[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 7.1.91.0

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

Table 1-3 describes the configuration used for testing the clients.

*Table 1-3 Test Bed Configuration for Interoperability*

| Hardware/Software Parameter | Hardware/Software Configuration Type |
|---|---|
| Release | 7.1.91.0 |
| Controller | Cisco 5500 Series Controller |
| Access points | 1142, 1242, 1252, AP 3500e and AP3500i, AP3600e and AP3600i |
| Radio | 802.11a, 802.11g, 802.11n |
| 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 1-4 lists the versions of the clients. The traffic tests included data or voice. The clients included laptops, handheld devices, phones, and printers.

*Table 1-4 Client Type*

| 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 |
| Intermec CN3/Windows Mobile 5.0 | 3.25.15.0065 |

*Table 1-4 Client Type (continued)*

| Client Type and Name | Version |
|---|---|
| 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 |

# 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 7.1.91.0 software to 500 access points simultaneously.
- 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.
- Do not install the 7.0.116.0 controller software file and the 7.0.116.0 ER.aes boot software file at the same time. Install one file and reboot the controller; then install the other file and reboot the controller.
- If you want to downgrade from 7.1.91.0 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 7.1.91.0 and if you have configured multicast interfaces, do not use the same configuration file for the 7.0.98.0 release. Using the 7.1.91.0 configuration file with multicast interfaces in the 7.0.98.0 release might cause the controller to be unresponsive.

To upgrade the controller software using the controller GUI, follow these steps.

**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 7.1.91.0 controller software from the Software Center on Cisco.com:

**a.** Click this URL to go to the Software Center:

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875243

**b.** Click **Wireless Software**.

**c.** Click **Wireless LAN Controllers**.

**d.** Click **Standalone Controllers** or **Integrated Controllers and Controller Modules**.

**e.** Click a controller series.

**f.** If necessary, click a controller model.

**g.** If you chose Standalone Controllers in Step d., click **Wireless LAN Controller Software**.

**h.** 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.

**i.** Click a software release number.

**j.** Click the filename (*filename*.aes).

**k.** Click **Download**.

**l.** Read Cisco's End User Software License Agreement and then click **Agree**.

**m.** Save the file to your hard drive.

**n.** Repeat steps a. through m. to download the remaining file (either the 7.1.91.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 7.0.116.0 ER.aes file).

**Step 3** Copy the controller software file (*filename*.aes) and the Cisco Unified Wireless Network Controller Boot Software 7.0.116.0 ER.aes file to the default directory on your TFTP or FTP server.

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

**Note** For busy networks, controllers on high utilization, or small controller platforms it is advisable to disable the 802.11a/b/g networks as a precautionary measure.

**Step 5** Disable any WLANs on the controller.

**Step 6** Click **Commands** > **Download File** to open the Download File to Controller page.

**Step 7** From the File Type drop-down list, choose **Code**.

**Step 8** From the Transfer Mode drop-down list, choose **TFTP** or **FTP.**

**Step 9** In the IP Address text box, enter the IP address of the TFTP or FTP server.

**Step 10** 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 11** In the File Path text box, enter the directory path of the software.

**Step 12** In the File Name text box, enter the name of the software file (*filename*.aes).

**Step 13** 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 14** Click **Download** to download the software to the controller. A message appears indicating the status of the download.

**Step 15** After the download is complete, click **Reboot**.

**Step 16** If prompted to save your changes, click **Save and Reboot**.

**Step 17** Click **OK** to confirm your decision to reboot the controller.

**Step 18** After the controller reboots, repeat Step 6 to Step 17 to install the remaining file (either the 7.1.91.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 7.0.116.0 ER.aes file).

**Step 19** Re-enable the WLANs.

**Step 20** For Cisco WiSM2, re-enable the controller port channel on the Catalyst switch.

**Step 21** If you have disabled the 802.11a/b/g networks in Step 4, re-enable them.

**Step 22** If desired, reload your latest configuration file to the controller.

**Step 23** To verify that the 7.1.91.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

**Step 24** To verify that the Cisco Unified Wireless Network Controller Boot Software 7.0.116.0 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 7.0.116.0 ER.aes file, the Emergency Image Version field shows “N/A.”

# Installation Notes

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

## Warnings

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

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

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

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

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

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

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

Warning **Do not operate the unit near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.** Statement 364

⚠ Warning **In order to comply with radio frequency (RF) exposure limits, the antennas for this product should be positioned no less than 6.56 ft. (2 m) from your body or nearby persons.** Statement 339

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

# Safety Information

Follow the guidelines in this section to ensure proper operation and safe use of the 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 Cisco 5500 Series Controller USB Console Port

The USB console port on the Cisco 5500 Series Controllers 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.

### USB Console OS Compatibility

- Microsoft Windows 2000, XP, Vista (Cisco Windows USB console driver required)
- Apple Mac OS X 10.5.2 (no driver required)
- Linux (no driver required)

To install the Cisco Windows USB console driver, follow these steps:

**Step 1** Follow these steps to download the USB_Console.inf driver file:

**a.** Click this URL to go to the Software Center:

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875243

**b.** Click **Wireless LAN Controllers**.

**c.** Click **Standalone Controllers**.

**d.** Click **Cisco 5500 Series Wireless LAN Controllers**.

**e.** Click **Cisco 5508 Wireless LAN Controller**.

**f.** Choose the USB driver file.

**g.** Save the file to your hard drive.

**Step 2** Connect the Type A connector to a USB port on your PC.

**Step 3** Connect the mini Type B connector to the USB console port on the controller.

**Step 4** When prompted for a driver, browse to the USB_Console.inf file on your PC. Follow the prompts to install the USB driver.

**Note** Some systems might also require an additional system file. You can download the Usbser.sys file from this URL:
http://support.microsoft.com/kb/918365

The USB driver is mapped to COM port 6. Some terminal emulation programs do not recognize a port higher than COM 4. If necessary, change the Cisco USB systems management console COM port to an unused port of COM 4 or lower. To do so, follow these steps:

**Step 1** From your Windows desktop, right-click **My Computer** and choose **Manage**.

**Step 2** From the list on the left side, choose **Device Manager**.

**Step 3** From the device list on the right side, double-click **Ports (COM & LPT)**.

**Step 4** Right-click **Cisco USB System Management Console 0108** and choose **Properties**.

**Step 5** Click the **Port Settings** tab and click the **Advanced** button.

**Step 6** From the COM Port Number drop-down list, choose an unused COM port of 4 or lower.

**Step 7** Click **OK** to save and then close the Advanced Settings dialog box.

**Step 8** Click **OK** to save and then close the Communications Port Properties dialog box.

# Important Notes for Controllers and Non-mesh Access Points

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

## Controllers Unreacheable from WCS when Upgrading from 7.0.116.0 to 7.0.220.0

When upgrading the controller software from release 7.0.116.0 to 7.0.220.0, it is found that the controllers that were previously reachable from WCS with SNMPv3 authentication were now unreachable.

Use any of the following workarounds to correct this:

- In WCS, momentarily 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 default value. If the SNMP engine ID is configured, it has to be reconfigured after applying the newly downloaded configuration.

## WPlus License Features Included in Base License

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 7.1.91.0, 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 7.1.91.0 to 6.0.196.0, 6.0.188 or 6.0.182, the license file in 7.1.91.0 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 7.1.91.0, 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 Wireless LAN Controller WPlus licenses remain in WCS and in the controller CLI and GUI in release 7.1.91.0. However, WLC WPlus license features have been included in the Base license, so you can ignore those references.

## Additive Licenses Available for 5500 Series Controllers

You can now purchase licenses to support additional access points on Cisco 5500 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 500 AP Groups on 5500 Series Controllers.

## 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 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 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/en/US/docs/wireless/controller/5500/tech_notes/Wireless_Software_Compatibility_Matrix.html#wp80877.

## 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.

## 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, 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)
```

## 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 7.0.220.0, 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 non-multicast 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 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 ( 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.

## 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 higher provide the passive client feature for Cisco 2500, and 5500 Series Controllers 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.

## 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.

## 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.

## 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 an Access Point's Prestandard Power Setting

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 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

## 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

This version of the controller software release 7.1.91.0 is compatible with the Gateway Load Balancing Protocol (GLBP).

## 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 CAPWAP Access Point Password

Cisco IOS Control and Provisioning of Wireless Access Points Protocol (CAPWAP) access points have a default password of *Cisco*, and the pre-stage configuration for CAPWAP 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 pre-stage configuration for CAPWAP access points is disabled and the access point displays the following error message when the CLI commands are applied:

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

## Exclusion List (Blacklist) 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.

## 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 to the *Cisco Wireless LAN Controller Configuration Guide, Release 7.0,* 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 to the *Cisco Wireless LAN Controller Configuration Guide, Release 7.0.116.0,* for configuration instructions.

**Note** SNMP v3 is time sensitive. Make sure 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.

## Features Not Supported on Cisco 5500 Series Controllers

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

- Static AP-manager interface

  **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)

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

**Note** Make sure 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;</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;<input type="TEXT" name="username"
SIZE="25" MAXLENGTH="63" VALUE=""> </td> </tr> <tr align="center" > <td colspan="2">
Password &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 controller's dynamic AP-manager interface must be configured with the external NAT IP address so that the controller can send the correct IP address in the Discovery Response.

# 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 controllers and lightweight access points for version 7.1.91.0. For your convenience in locating caveats in Cisco's 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.

Note

If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

http://tools.cisco.com/Support/BugToolKit/

To become a registered cisco.com user, go to the following website:

http://tools.cisco.com/RPF/register/register.do

## Open Caveats

Table 1-5 lists open caveats in controller software release 7.1.91.0.

*Table 1-5 Open Caveats*

| ID Number | Description |
|---|---|
| CSCtt96370 | RIFS Rx gets disabled when changing MCS rates through the Controller User Interface<br>**Symptom**: When modifying the supported MCS rates in the Controller User Interface, RIFS reception always gets disabled.<br>**Conditions**: Modifying MCS rates using the Controller User Interface.<br>**Workaround**:<br>1. Use the Command Line to modify the MCS rates.<br>2. Re-enable RIFS Rx after modifying the MCS rates with the Controller User Interface by issuing the following CLI command:<br>**config 802.11a\|b 11n-support rifs rx enable** |
| CSCtr41297 | Unsupported 1200 and 1100 AP models wait in IMAGE state with 7.1.91.0 controller<br>**Symptom**: The AP models AP1310, AP1200 and AP1100 are no longer officially supported in this software release. Though, the APs are still able to join the controller and will go into the imaging download state but there are no images for these models. Without the AP image, the APs will reboot and continuously join the controller.<br>**Conditions**:<br>This happens because there are no AP images for these models due to support being dropped for these APs in this release.<br>**Workaround**:<br>Since the APs are not supported by this release, the only workaround is to place a controller version which supports these models on the network. The APs should join that controller. |

*Table 1-5 Open Caveats*

| ID Number | Description |
|---|---|
| CSCtr94418 | Small upstream throughput degradation may be observed with short guard interval enabled.<br>**Symptom**:<br>Higher packet retry counts may occur when a 802.11n 3 spatial-stream client is transmitting data to the access point. This may prevent the client from achieving maximum theoretical throughput. This is not expected to degrade maximum possible (upstream) throughput by more than 5%.<br>**Conditions**:<br>In most environments, this condition will not be observable. It is most likely to occur in extremely clean RF environments, where there is very little interference or traffic from other cells.<br>**Workaround**: None |
| CSCtr94572 | Certain microwave oven models may be classified as jammers by CleanAir.<br>**Symptom**:<br>Some microwave oven models may be classified and reported as a "Jammer" by CleanAir.<br>**Conditions**:<br>The classification of a microwave oven as a jammer by CleanAir is unique to certain microwave models. Cisco does not maintain a list of each such model.<br>**Workaround**: None |
| CSCts56505 | Radio may reset with console message "CleanAir error: No CleanAir msmts".<br>**Symptom**:<br>Under very rare, specific, circumstances, CleanAir reporting may halt and be restarted automatically, also causing a brief disruption to clients being served by the same radio.<br>The AP's console will display the message, "CleanAir error: No CleanAir msmts" when this occurs.<br>**Conditions**:<br>This condition has only been observed when rogue containment has identified and is actively containing a rogue access point simultaneously with very high traffic loading.<br>**Workaround**: Disable the rogue containment feature. |

*Table 1-5 Open Caveats*

| ID Number | Description |
|---|---|
| CSCtt44826 | Radio may reset with console message "CleanAir error".<br>**Symptom**:<br>In very rare circumstances, in very busy RF environments, CleanAir may stop functioning on one or both of the AP's radios, resulting in a immediate reset of the radio interface. The following message is displayed on the AP's console when this condition occurs: "CleanAir error count exceeded".<br>**Conditions**:<br>This condition requires CleanAir to be enabled in an environment with nearly constant 100% channel utilization.<br>**Workaround**: Disable CleanAir. |
| CSCud20593 | **Symptom**: The Cisco TrustSec SXP feature is not supported.<br>**Conditions**: 7.0.x controller software releases.<br>**Workaround**: None. |

## Resolved Caveats

Table 1-6 lists caveats resolved in controller software release 7.1.91.0.

*Table 1-6 Resolved Caveats*

| ID Number | Caveat Title |
|---|---|
| | |
| CSCtr65620 | Cisco Aironet 1142 or 3502 Access Points falsely report high channel utilization. |
| CSCtj38889 | Cisco Flex 7500 Series Controller- Locally authenticated PMK cache info gets deleted after the controller reboots. |
| CSCtn04229 | Signal strength increases for a while though TxPower is static. |
| CSCto59770 | OfficeExtend Access Points with least latency join are stranded. |
| CSCtb78072 | SNMPv3 communication breaks with NAC appliance CAM. |
| CSCtl98942 | CleanAir Trap types go back to default after configuration is restored. |
| CSCtn16281 | Mesh access point is unresponsive on a BVI restart by DHCP. |
| CSCtn16347 | A controller does not rewrite DHCP ACK packets correctly for DHCP information. |
| CSCtn37462 | The `show net user summary` command does not show users when the local database has more than 256 entries |
| CSCto06084 | The access point summary report does not show any data for the Cisco Aironet 602 OfficeExtend access point. |

*Table 1-6 Resolved Caveats (continued)*

| ID Number | Caveat Title |
|---|---|
| CSCto11060 | A Remote LAN fails to apply to Cisco 2500 Series Controller through WCS. |
| CSCto11157 | An access point does not send an association response to a client. |
| CSCto50248 | Cisco Flex 7500 Series Controller-OKC fast roam fails in standalone mode while using EAPfast/PEAP EAP. |
| CSCsl11129 | A Cisco IOS device configured with Cisco IOS Gateway for T.37 On-Ramp Fax Support might not respond and display a bus error. |
| CSCto63711 | A Cisco IOS DHCP client does not parse option 43 if preceded by option 33 data. |
| CSCtc39367 | An access point processes a CDP packet addressed to a bogus multicast address. |
| CSCtj06528 | WCS displays wrong channels for WIPs alarms. |
| CSCtn09749 | HREAP access points unresponsive on parser command interface configuration. |
| CSCtn14507 | Access Point radio is in a radio core dump (PAK stuck) on Cisco Aironet1140 Access Point. |
| CSCtn23202 | A Cisco Aironet 3500 Series Access Point longevity test failure has occurred; no client can communicate. |
| CSCtn38127 | Hybrid REAP radio interfaces reset with reason: `Radio reset due to 70`. |
| CSCtn42589 | An access point reboots while moving from connected to standalone if radio b/g is disabled. |
| CSCtn50229 | Cisco Aironet1240 Access Point coredump: `bad rx ring addr-0xACEDE421, 0xD0EDE421` |
| CSCtn84245 | Mesh: Bandwidth of 8ch/12ch in 4.9 GHz is changed to 5 MHz/10 MHz in -P (Japan). |
| CSCtn92381 | Cisco Aironet 600 Series OfficeExtend Access Point: Remote LAN commands get uploaded as WLAN commands. |
| CSCtn95179 | When CAPWAP data encryption is enabled, no DSCP marking are seen in the CAPWAP IP header. |
| CSCto06251 | An access point sends DHCP renew before a discovery when fast heartbeat is enabled. |
| CSCto32431 | AES CCM Replay messages appear on the Mesh AP CLI. |
| CSCto34834 | Cisco Aironet 1520 and 1550 Series Access Points might change the 2.4 GHz channel setting when reloaded. |
| CSCto44483 | Custom set TX Power Level Assignment is not preserved on an AP reboot in the Cisco Aironet 1040 Access Point. |
| CSCto62533 | DFS failure on Cisco Aironet 1550 Series Access Point for Japan 0.5uS pulse detection. |
| CSCto73361 | When a WGB roams between two access points, and the access point might have another client, an AID reuse occurs that causes a collision on the AP. |
| CSCto83294 | Access Point is unresponsive when performing the check Hybrid REAPs task. |

*Table 1-6 Resolved Caveats (continued)*

| ID Number | Caveat Title |
|---|---|
| CSCtq24098 | Radio core dump observed as a result of radio timeouts on access points: `FW: irq/mac stat=400/2, cmd=0x16 seq=6, @B96FF5.` |
| CSCtq32267 | Cisco Aironet 1552 Access Point longevity test fails with AES CCMP replays. |
| CSCtq53998 | Cisco Aironet 600 Series OfficeExtend Access Point: False warning message is thrown first time for a strong password. |
| CSCtq67940 | Cisco Aironet 1140 and 1040 Access Points: Bootloader fix for CHIP_21 erratum (only for newly manufactured Cisco Aironet 1140 Series Access Points). |
| CSCtq68744 | Access point unresponsive with the following message: `CAPWAP CLIENT; CPUvec 1400 dtls_shimbuf_data.` |
| CSCtq70348 | Large number of packets are dropped during the Cisco Aironet 1300 Series Access Point longevity test. |
| CSCtq77063 | Radio reset due to timing out of probes suppression command. |
| CSCtq85081 | When running a soft phone over laptop with priority 0, a 500ms delay is observed in an audio upstream from the client at least once a minute. |
| CSCtq87010 | Allow additional countries to be listed in the controller. |
| CSCtq93161 | Band Select client RSSI is always enabled regardless if Band Select being enabled or not. |
| CSCtq95499 | Cisco Aironet 1552 Series Controller: RAP convergence time is 5 minutes, which is too long. |
| CSCtr04517 | Degraded downstream throughput observed on Cisco Aironet 1142 Series Access Point for 1518 frame size on 5G radio. |
| CSCtr08208 | Controller unresponsive when executing `Virtual Exec CPUvector 700.` |
| CSCtr43679 | Intercontroller roaming does not work. |
| CSCsw68997 | Hybrid REAP VLAN mappings are mismatched. |
| CSCtn39497 | Identity Services Engine: Failed logs in ISE while switching between ISE in RUN time. |
| CSCtn77107 | WiSM-2 Data port down on VSS after multiple SSOs or standby switch resets. |
| CSCtq46316 | Some rogue classifications are not retained after reboot. |
| CSCtq64452 | WLAN with same SSID, different Layer 2 Security not allowed in AP Group. |

# If You Need More Information

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:

http://tools.cisco.com/Support/BugToolKit/

(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.)

# Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at

http://www.cisco.com/en/US/support/index.html

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

# Documentation Updates

This section lists updates to user documentation that has not yet been added to either printed or online documents.

# Related Documentation

For additional information on the Cisco controllers and lightweight access points, see these documents:

- *The quick start guide or installation guide for your particular controller or access point*
- *Cisco Wireless LAN Controller Configuration Guide*
- *Cisco Wireless LAN Controller Command Reference*
- *Cisco Wireless Control System Configuration Guide*

You can access these documents from this link:

http://www.cisco.com/cisco/web/support/index.html

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

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.