ArubaOS 2.4.8.11-FIPS
Release Notes

ArubaOS 2.4.8.11-FIPS is a software release for the Aruba 800-Series, Aruba 5000, and Aruba 6000 Mobility Controllers that support FIPS 140-2 Level 2 certification.

These release notes describe the differences between standard versions of ArubaOS and the ArubaOS 2.4.8.11-FIPS software and other information pertinent to installing and using this release.

ArubaOS 2.4.8.11-FIPS Differences

The following are differences between standard versions of ArubaOS software and the ArubaOS 2.4.8.11-FIPS software.

Upgrading to This Release

- Prior to upgrading to ArubaOS 2.4.8.11-FIPS, you must execute the **write erase all** command. Otherwise, the SHA-1 hash will fail and the controller will not boot.

- A new CLI command, **fips enable/disable**, places the controller into FIPS mode or non-FIPS mode. The **fips enable** command causes DES encryption in 802.1X and disables WEP. The **show dot1x config** command shows whether or not FIPS mode is enabled.

NOTE: ArubaOS 2.4.8.11-FIPS does not support non-FIPS configurations. See "Upgrading to ArubaOS 2.4.8.11-FIPS" on page 11 for information on upgrading the configuration.

Default Configuration

- The Setup dialog is disabled. The default configuration is as follows:
  - The controller is a master controller
  - Country code is US
  - IP address is 172.16.0.254/24

- The controller boots up using the default IP address 172.16.0.254/24 with no default route. To configure a controller running ArubaOS 2.4.8.11-FIPS prior to deployment, you must connect the controller to a PC configured for the 172.16.0.0/24 subnetwork.

- The default admin password is **fipsadmin** and the default password for entering enable mode is **fipsenable**.

Admin Access

- Only SSH access is allowed to the controller; Telnet access is disallowed. SSH acceps only SHA-1 hashes, 3DES, and AES algorithms. Valid ciphers are aes128-cbc, aes192-cbc, aes256-cbc, and 3des-cbc.

- The WebUI accepts HTTPS connections only on port 4343; HTTP access is disallowed. Connections must use Transport Layer Security (TLS) version 1; SSL version 2 and 3 are rejected. You cannot connect via an Internet Explorer browser using TLS version 1 unless all SSL variants are disabled. Valid ciphers are 3DES-CBC-SHA, AES-128-SHA, and AES-256-SHA.

NOTE: You must configure your browser to use TLS to connect to an Aruba Mobility Controller that is running ArubaOS 2.4.8.11-FIPS. Internet Explorer (IE) uses SSL v2 and v3 by default and you must explicitly enable TLS version 1. To do this:

I. In the IE browser window, select Tools > Internet Options.

II. Select the Advanced tab.

III. Scroll to the bottom of the window.

IV. Select (check) the **Use TLS 1.0** option *and* deselect (uncheck) the **Use SSL 2.0** and **Use SSL 3.0** options.

If you configured Microsoft Windows to run in FIPS mode, then Internet Explorer uses TLS version 1.

NOTE: Firefox TLS version 1 sends a handshake in SSL v3 and cannot connect to an Aruba Mobility Controller that is running ArubaOS 2.4.8.11-FIPS.

Passwords

- All passwords must be at least six characters in length.
- Passwords in the local user database can be up to 128 characters in length. Passwords are stored in 3DES encrypted form.

Configuration

- Whenever the configuration on the controller is saved, including at initial setup, a SHA-1 hash is generated. This hash is verified whenever the configuration is loaded and the system will fail to reboot if the verification fails.

CLI

- A new CLI command **wipe out flash** can be used to overwrite the compact flash, destroying its contents.
- The following CLI commands are not allowed:
  - telnet soe
  - telnet cli

Other

- A new application, cryptoPOST, monitors encryption subsystems and reboots the controller if any subsystem fails.

For more information, see the *FIPS 140-2 Level 2 Release Supplement for Aruba 800, 5000 and 6000 Mobility Controller with ArubaOS 2.4.8.0-FIPS Software*.

Issues and Limitations Fixed in ArubaOS 2.4.8.11-FIPS

The following issues and limitations from ArubaOS 2.4.8.10-FIPS have been fixed in this release:

- Any ArubaOS 2.4.8.10-FIPS only deployment now operates in the defined channel (20210).

- A new CLI command **restore factory_default certificate** is available to select the factory default certificate (21265).

- AMs now correctly receive the AP configuration data (21806).

- Support for capturing encrypted packets from an AP is now disabled (5748).

Issues and Limitations Fixed in Previous Releases

The following issues and limitations have been fixed in the indicated release and included in this release.

Issues and Limitations Fixed in ArubaOS 2.4.8.10-FIPS

The following issues and limitations from ArubaOS 2.4.8.9-FIPS have been fixed in this release:

- To ensure compliance with FCC regulations, channels 52, 56, 60, and 64 are no longer available. Existing configurations using these channels automatically use a different available channel (20210).

- The spurious "Configuration upgrade failed" message is no longer displayed on the console when the controller reboots. There was no failure, and the message was harmless (18608).

- The SNMP community string is now updated properly so that the old string is no longer cached when the string is updated (18769).

- You can now enable dot1x termination from the CLI without the AAA license (18241).

Issues and Limitations Fixed in ArubaOS 2.4.8.9-FIPS

The following issues and limitations from ArubaOS 2.4.8.3-FIPS have been fixed in this release:

- A large amount of multicast traffic through the Ethernet port on an AP no longer occasionally causes the AP to reboot (10186).

- You can now change an AM to an AP for the B/G radio alone (12092, 12408, 12029).

- Database synchronization no longer fails when large images are used for the RF Plan background (12954, 14918).

- Several NTP problems were fixed so that: NTP no longer causes CPU utilization to be 100%; NTP commands no longer hang; the system clock is now properly updated via the NTP server; and NTP is no longer reported as having died with failure code 5H (13071).

- Monitored AP and station info is now correctly updated in WMS when an AP is continuously rebootstrapping (13113, 11758).

- Symbol-based scanners now associate properly during a VRRP fail-over (13165).

- Clients using DHCP can now successfully renew the IP address (13219).

- Provisioning a new AP or reprovisioning an existing AP no longer causes the SAPM process to crash (12913, 12953, 13424, 13625, 13888, 13932, 14206, 14281).

- Multicast traffic is now always forwarded properly after IGMP is enabled (13789).

- Broadcast and multicast traffic now always works over Port Channel trunk connections with IGMP snooping enabled (13970, 13397).

- The AP-80M now correctly negotiates speed and duplex settings (14976).

- When the controller is in a high-CPU condition, such as after a configuration change affecting all APs in the network, APs that reboot now receive their new configuration promptly (15386, 15511).

- ETSI DFS no longer causes an AP to prematurely move to a new channel (17370).

- Throughput is increased for large numbers of encrypted clients (17870).

- The controller no longer forwards RADIUS responses to clients that disconnect while authenticating (14253, 18611, 16088, 16090).

- The Report Polygon Bug button is no longer displayed in RF Plan (17692).

- APs no longer reboot when you change WEP keys for Virtual APs (13768, 13769, 13770).

- ADP is now disabled by default on Aruba 2E, Aruba 800-E, and Aruba 2400-E Access Multiplexers (17399).

- When the controller is in a high-CPU condition, such as after a configuration change affecting all APs in the network, APs that reboot now receive their new configuration promptly (15511).

- Various issues were fixed to improve AP stability in large configurations (14968, 15363, 15749, 17592).

- Clients using xSec no longer lose connectivity when they go into powersave mode (16314).

Issues and Limitations Fixed in ArubaOS 2.4.8.3-FIPS

The following issues and limitations from ArubaOS 2.4.8.2-FIPS have been fixed in this release:

- Odyssey Client re-connect now properly retrieves cached role information. (13393)
- Active IGMP members are no longer removed after the group membership interval expires (13295)
- Repeatedly saving the configuration no longer causes a crash in the AP. (13468)

Issues and Limitations Fixed in ArubaOS 2.4.8.2-FIPS

The following issues and limitations from ArubaOS 2.4.8.1-FIPS have been fixed in this release:

- Wired xSec clients connected to a trunk port with xSec enabled on a single VLAN can now properly pass data. (13255, 7684)
- The Aruba 41 AP is now fully supported. (12542)
- WMS no longer crashes continuously on an Aruba 800 Mobility Controller. (12731)

Issues and Limitations Fixed in ArubaOS 2.4.8.1-FIPS

The following issues and limitations from ArubaOS 2.4.8.0-FIPS have been fixed in this release:

- Provided workaround for interoperability with some legacy non-Aruba access points.

Feature-Specific Recommendations

To help ensure optimal ArubaOS operation, review the following recommendations and feature-specific tips:

- When configuring xSec point-to-point connections, note the MTU size in the xSec P2P command and verify that the intermediate L2 device is capable of handling jumbo frames that exceed the standard Ethernet MTU.
- To ensure successful synchronization of database events, you should set periodic synchronization of master-master redundancy to a minimum period of 20 minutes.

- Make sure that the native VLAN is included in the allowed VLAN list to ensure proper forwarding of Spanning Tree and other traffic which does not use tagging.

- Enabling NAT for source addresses on Aruba controllers is compatible with Nortel VPN clients, provided a rule is added before the src-nat rule. To support RSA token and time syncing, specify a rule on the client firewall.

- Access Points that are indirectly connected to Aruba Mobility Controllers through third-party switches may have problems processing IP packets larger than 1500 bytes. Aruba recommends setting the maximum transmission unit (MTU) on these Access Points to 1500 bytes. Do this by entering (from config mode) under the AP location:
  ap location 0.0.0 mtu 1500
  write memory

- Aruba supports directly connecting Aruba Mobility Controllers only with a cross-over cable. Connecting Aruba Mobility Controllers with straight-through cables is not recommended. Using the proper (cross-over) cable, ports on both sides of the connection can be configured to auto-negotiate or can be hard coded as long as they match.

- Devices that are idle for extended periods of time (for example, overnight) but need to maintain their connection to an Aruba controller must be able to respond to ICMP requests from the Aruba controller. However, the default settings of many personal firewalls (including XP SP2) deny incoming ICMP requests. This configuration results in the devices experiencing frequent disconnects and reconnects, as well as DHCP address problems. To eliminate connection problems, be sure to configure firewall settings to allow ICMP requests from the Aruba controller.

- Many personal firewalls and ad/pop-up blocker programs, (for example Google and Yahoo) block pop-up windows by default. This can cause Captive Portal logon/logout issues if the controller URL does not explicitly allow pop ups. To prevent this problem, allow pop ups for the controller's URL.
  To log-out from a Captive Portal session if the pop-up window is not available, point your web browser to:
  http://<controller ip address>/auth/logout.html

- In deployments with the Aruba dialer and RSA SecurID, new/next pin mode RSA token time syncing requires that the Aruba dialer be added into the firewall's application exception list. (For more information on configuring a firewall application exception list, refer to the Microsoft knowledge base, as this is typical for Microsoft applications.) This step is not required for normal operations.

- The Microsoft XP SP2 personal firewall already allows L2TP whereas Sygate needs this to be configured manually.

- If you are not doing any backend or local database authentication for administrative users, Aruba recommends that you disable this feature by using the **aaa mgmt-authentication mode disable** command.

The **Mobile Edge** Company

- To restore the correct syslog facility level from a saved configuration file, do a **write erase** before executing a **copy flash: <saved-cfg> flash: default.cfg**.

- If you have licensed features on a Supervisor Card and need to replace that card, be sure to restore the configuration from backup to the new card to restore your license information. For more information, refer to the *Managing Software Feature Licenses* document that ships with your controller.

- Using A60/61 APs with Cisco 3550 PoE switches requires that the Cisco switches run IOS 12.1 (19) or later. Aruba recommends that you also make the following configuration settings on the Cisco 3550 (INLINE POWER) port:
  - power inline delay shutdown 15 initial 25
  - (config-if) spanning-tree portfast

- Funk-Odyssey clients may experience delays in getting authenticated when using WPA encryption and server derivation roles where the VLAN of the client is set by matching a particular attribute. Aruba recommends that these users set the WPA Key Timeout and WPA Retry Count to 5.

- When using some legacy Cisco Access Points (for example the Cisco AP 1200), be aware of the following condition when using PoE:
  - The Cisco AP is connected to an Aruba mobility controller.
  - Cisco mode is enabled (**poe cisco**).
  - PoE is turned off (**no poe**).
  - PoE is turned back on (**poe**).
  - Cisco mode is re-enabled (**poe cisco**)

- Sygate SODA users should note that upload file names cannot contain spaces.

Known Issues and Limitations in This Release

The following are issues for the ArubaOS 2.4.8.11-FIPS release. Where bug IDs are applicable, they are included in the description of the issue.

- IP spoofing detection across controllers does not work when the new-user-mobility flag is turned off. (12404)

- xSec P2P does not become active if commands are not entered in the correct order. (12330)

  For example, if you configure the xSec VLAN on a port *before* configuring xSec point-to-point, the configuration will not take effect on the controller. Delete the xSec point-to-point configuration, then enter the commands in the correct order. An example of the correct order that the configuration commands should be entered is as follows:

```
interface fastethernet 2/22
    xsec vlan 192
    xsec point-to-point 00:0b:86:00:17:00 50002xsc50001xsec allowed vlan 52-55 1420
    spanning-tree portfast
!
```

- After you configure the LDAP server in the WebUI, values in the Admin-DN and Admin-Passwd fields of the provisioned server may not be editable from the CLI. (They are editable from the WebUI.) If you need to change these values in the CLI, delete the LDAP server entry and create it again. (12191)

- Downgrading from this release to a previous release changes the installation date of evaluation licenses and, accordingly, the licenses are marked as expired. Reapply the evaluation license key after the downgrade and reboot the system. (12188)

- When using the WebUI basic configuration pages, you may see an error message when configuring the EAP offload feature to use the internal database as the authentication server. The workaround is to enable dot1x termination using the CLI or the WebUI advanced configuration pages. (12174)

- When upgrading from an earlier version of ArubaOS software, the IP addresses of L3 tunnel interfaces may disappear if there are no L2 tunnels configured within the system. You need to reconfigure L3 tunnel interfaces after upgrading the system. (12172)

- In complex VRRP scenarios, the selection of HA for a new user may not work correctly. (12140)

- After upgrading your system to ArubaOS 2.4.8.11-FIPS, verify the operational state of all APs/AMs in the network by issuing the 'show ap global-list' command. If any of the APs are in down state several minutes after other APs/AMs are up, execute the 'apboot ipaddr <ap_ip>' command to resolve the issue. (12049)

- TACACS accounting does not log WebUI commands. (11937)

- The TACACS accounting feature does not work reliably on local controllers until the controllers are rebooted. (11934)

- The EAP offload feature does not work with wired clients. (11585, 11570)

- In some configurations, ports may not be reset to their original states after deleting them from a port-channel (Link Aggregation) group and this could affect forwarding of data on those ports. (10957,10101)

- Occasionally users cannot delete a virtual AP from the WebUI. The workaround is to go to phytype mode in the CLI and then delete it. (9198)

- Some VPN sessions on the remote AP controller are not timing out. (9343)

- Occasionally, a heat map may display a polygon error. A retry should solve the problem. (9445, 7070)

- If a line card is removed and the controller is rebooted before the line card is replaced, the VLAN configuration reverts to default values. (6226)

- The user entry created on the Home Agent (HA) may not display the correct Location, Roaming, ESSID/BSSID/Phy values. (This is a display-only issue.) (6151)

- User entries showing wrong Location and Roaming Status may occur after a failover and recovery. The HA shows the correct information but the FA may not. (6858)

- While moving a station, if 802.1x authentication is delayed, the **show user global-user-map** command output is not displayed correctly. (6557)

- Wired clients who fail authentication are blacklisted, but they can still try to login. (6802)

- Session mirroring does not update for sessions that are already active. (6829)

- All PPTP connections to Aruba (or any PPTP server) for users with Windows XP Service Pack 2 firewall enabled, experience a one minute wait before being able to reconnect.

- If trim-fqdn is enabled for 802.1x server, the domainname portion for the FQDN is still passed to the RADIUS server by the client internal EAP module. (6898)

- If the username is in the format of domain\username, trim-fqdn does not remove the domain portion before sending request to the server. (6804)

- There is a BW contract granularity limitation. The effective bandwidth enforced is not accurate for contracts less than 300 Kbits. (6838)

- The wired-dot1x role-based VLAN is not supported for SecureJack. (7464)

- WiFiMUX wired 802.1x is not supported in this release. (6310)

- Changes in the NTP Servers list on master controllers are not being propagated to local controllers. (4944)

- ESI can be used within a multi-controller topology with master and local controllers and full redundancy. However, the following limitations apply in this release.:

  - On the WebUI, using the **Back** button to move back to previous browser pages occasionally causes incorrect data (blanks) to be filled in some fields. This can result in ESI misconfigurations being sent to the controller. (7618).

  - By design, in a multi-controller topology, client VLANs should not be shared across controllers. For example, client VLAN 100 cannot be configured on controller lms1 and lms2 as doing so would cause the AVF routes to be incorrect when the client moves between the controllers. Use separate VLANs instead on each controller and let mobility take care of preserving the IP addresses of the client when the client moves between controllers.

- After a role-based VLAN is disabled, the 802.1x client will not have connectivity for a few minutes. (7892)

- **Monitoring > Switch Summary** may not display the correct total of clients. The WLAN client summary may be smaller than the total of client entries because the per-controller display includes additional entries – which are not shown in the global user list. (7904)

- After restoring a configuration, verify that your logging levels are set properly as they may not be restored. (7542)

- Wired clients appear on All WLAN Clients pages in the WebUI. (7968)

- xSec cannot be enabled on uplink trunk ports doing dot1q tagging. (7704)

- When the Funk Odyssey xSec client is used, some client NICs (for example, Dlink, 3Com) may experience problems sending frames when the MTU size is changed to 1500 bytes (7963)

- The message: "Please reload the switch for the new service key to take effect" continues to display even after an existing temporary key is replaced with another temporary or permanent key. A reboot is not required if the associated feature is already enabled (as shown by the **show keys** CLI command or on the WebUI license management page). (7214)

- The message: "Reboot Cause: License Expired" displays with the **show switchinfo** CLI command output, but does not specify which of the licenses has expired and caused a scheduled system reboot. (7215)

- No SNMP traps are generated when software feature licenses are added, deleted, or expire. Syslog messages, however do report these events.(7450)

- Sygate SMS does not return MPPE keys when user authentication fails and host authentication is passed. (7736)

- When Sygate Virtual Desktop check is enabled, the first check always fails and the subsequent check passes. (7501)

- The Cisco AP does not power on. To resolve this condition, enter **no poe cisco**. The Cisco AP then functions normally as a PoE device. (8054, 7442)

Upgrading to ArubaOS 2.4.8.11-FIPS

If the software upgrade distributed with these release notes is on CD or some other static media, be sure to visit the Customer Support website to make sure you have the latest release of ArubaOS.

For information on upgrading to or downgrading from this release, refer to

Before Changing Your Mobility Controller's Image

Aruba Mobility Controllers store critical configuration data on an onboard Compact Flash memory module. In order to maintain the reliability of your Aruba Mobile Edge enabled WLAN network, Aruba recommends the following general best practices with respect to the use of your Aruba controller and its Compact Flash memory:

Backing Up Critical Data

It is important to frequently back up all critical configuration data and files on the Compact Flash file system to an off-controller external server or mass storage facility. At the very least, you should include the following files in these frequent off-controller backups:

- Configuration data
- WMS database
- Internal database
- Licensing database
- Floor Plan JPEGs
- Customer Captive Portal pages
- Customer x.509 certificates

NOTE: The internal format of the ArubaOS 2.4.8.11-FIPS configuration file is different from other ArubaOS configuration files. Therefore, you will not be able to restore the backed up configuration file after upgrading to ArubaOS 2.4.8.11-FIPS. You can copy and paste configuration commands from the saved file to the new configuration file.

All the above files reside on the Compact Flash file system on the Aruba Mobility Controller. If supported on your current ArubaOS image, the WebUI provides the easiest way to back up and restore the entire Compact Flash file system: navigate to Maintenance > File > Backup Flash. Click Create Backup to back up the contents of the Compact Flash file system to the file flashbackup.tar.gz. Then click Copy Backup to copy the file to an external server.

NOTE: Prior to upgrading to ArubaOS 2.4.8.11-FIPS, you must execute the **write erase all** command. Otherwise, the SHA-1 hash will fail and the controller will not boot.

Managing Flash Memory

Be careful not to exceed the size of the Compact Flash file system. For example, loading multiple large building JPEGs for RF Plan can consume flash space quickly. If a write attempt to flash occurs when there is 5 MB or less of flash space, warning messages will alert you that the file system is running out of space.

Other tasks which are sensitive to insufficient flash space include:

- Using the internal database: DHCP lease and renew. is also stored in the Compact Flash file system. If the file system is full, DHCP addresses will not be distributed or renewed.

- If an Aruba controller encounters a bug where it needs to write a core file, it will not be able to do so if the file system is full, and critical troubleshooting information will be lost.

Powering the System Down or Power Cycling the System

Compact Flash devices can be corrupted if power is lost during a write event (for example. **write mem**). To reduce the exposure of the Compact Flash system to corruption, be sure to follow these procedures:

To power down:

1. From the CLI, type: halt.

2. The controller responds with the message: system halted.

3. Now the controller is ready to be powered down or reset (at this point will automatically reset after approximately 90 seconds).

Installing ArubaOS 2.4.8.11-FIPS— Prerequisites

- Make sure you have at least 10 MB flash space available.

- Back up the WMS database and TFTP it off the controller.

- Remove all unnecessary saved files from flash.

- Run the tar crash command to make sure that there are no "process died" files clogging up flash and TFTP the files off the controller.

- Prior to upgrading to ArubaOS 2.4.8.11-FIPS, you must execute the **write erase all** command. Otherwise, the SHA-1 hash will fail and the controller will not boot.

Upgrading to ArubaOS 2.4.8.11-FIPS

The ArubaOS software can be upgraded as new releases become available.

> ⚠️ **CAUTION:** When upgrading the software in a multi-controller network (one that uses two or more Aruba Mobility Controllers), special care must be taken to upgrade all the mobility controllers in the network and to upgrade them in the proper sequence (see "Upgrading Multi-Controller Networks" on page 17).

1. Obtain the latest valid Aruba Mobility Controller software image from Aruba Customer Support.

   NOTE: The most current Aruba Mobility Controller software image may be newer than that available at the time these release notes were written. Aruba recommends that you always download the latest software image from Aruba Customer Support before proceeding with these installation instructions.

2. Upload the new software image to a TFTP server on your network.

3. Verify the network connection between from the target controller to the TFTP server:

   ```
   (aruba) # ping <TFTP server IP address>
   ```

4. Back up your current controller configuration.

   Use the following command to determine the name of your configuration file:

   ```
   (aruba) # show boot
   Config File: default.cfg
   Boot Partition: PARTITION 0
   ```

   In this example, `default.cfg` is the configuration filename. To copy the configuration file to an external TFTP server, use the following command:

   ```
   (aruba) # copy flash: default.cfg tftp: <TFTP server IP address>
   <dest. filename>
   ```

   NOTE: A valid IP route must exist between the TFTP server and the Mobility Controller. Also required, a placeholder file with the destination filename and proper write permissions must exist on the TFTP server prior to executing the copy command.

5. Back up your current WMS and internal databases.

Use the following commands to export the Mobility Controller's internal databases to an internal file with the filename of your choice, and then to an external TFTP server:

```
(aruba) # wms export-db <filename for WMS db>
(aruba) # copy flash: <filename for db> tftp: <TFTP server IP address>
<dest. filename>
(aruba) # local-userdb export <filename for local user db>
(aruba) # copy flash: <filename for db> tftp: <TFTP server IP address>
<dest. filename>
```

NOTE: A valid IP route must exist between the TFTP server and the Mobility Controller. A placeholder file with the proper write permissions for each destination filename must exist on the TFTP server prior to executing the copy commands.

6. Determine which memory partition will be used to hold the new software image.

   Use the following command to check the memory partitions:

```
(aruba) # show image version
----------------------------------
Partition                  : 0:0 (/dev/hda1) **Default boot**
Software Version           : 2.4.8.9-FIPS
Build number               : Axxx_2.4.8.9-FIPS_12149
Built on                   : Mon Dec 19 05:52:19 PDT 2005
----------------------------------
Partition                  : 0:1 (/dev/hda2)
/dev/hda2: Image not present
----------------------------------
Partition                  : 1:0 (/dev/hdc1)
Not plugged in.
----------------------------------
Partition                  : 1:1 (/dev/hdc2)
Not plugged in.
```

   It is recommended that you load the new image into the backup partition. In the above example, partition 0 contains the active image. Partition 1 is empty (image not present) and can be used for loading the new software.

7. Use the **copy** command to load the new image into the Aruba Mobility Controller:

   # **copy tftp: <server address> <image filename> system: partition {0|1}**

> **NOTE:** When using the copy command to load a software image, the specified partition automatically becomes active the next time the controller is rebooted. There is no need to manually select the partition.

8. Verify that the new image is loaded:

   # **show image version**

   Information about the newly loaded software image should be displayed for the appropriate partition.

9. Reboot the controller:

   # **reload**

10. When the boot process is complete, use the **show version** command to verify the upgrade.

```
(aruba) #show version
Aruba Wireless Operating System Software.
ArubaOS (MODEL: Aruba5000), Version 2.4.8.9-FIPS
Website: http://www.arubanetworks.com
Copyright (c) 2003-2005 by Aruba Wireless Networks, Inc.
Compiled on 2005-1-1 at 15:02:41 PDT (build 8xxx) by p4build


ROM: System Bootstrap, Version CPBoot 1.0.6 (Aug 13 2003 - 16:17:05)


Switch uptime is 3 days 46 minutes 47 seconds
Reboot Cause: User reboot.
Aruba Supervisor Card
Aruba Processor (revision 16.20 (pvr 8081 1014)) with 256M bytes of
memory.
32K bytes of non-volatile configuration memory.
128M bytes of Supervisor Card System flash (model=TOSHIBA
THNCF128MBA).



(aruba) #
```

   In this example, version 2.4.8.9-FIPS is loaded and running, indicating that the upgrade is complete.

11. Log in as the administrator and set the proper time zone for your location.

(config) # **clock timezone <name of timezone> <UTC offset>**

Upgrading Multi-Controller Networks

In a multi-controller network (one with two or more Mobility Controllers), special care must be taken to upgrade all controllers in the proper sequence based on the controller type (master or local). Be sure to back up all controllers being upgraded.

1. Make sure you have at least 10MB of free flash.

2. Back up the WMS database and TFTP it off the controller.

3. Remove all unnecessary saved files from flash.

4. Run the tar crash command to make sure that there are no "process died" files cluttering memory and TFTP the files off the controller.

Upgrading to ArubaOS 2.4.8.11-FIPS

Upgrading an Existing Network

To upgrade an existing multi-controller system to ArubaOS 2.4.8.11-FIPS:

1. Upgrade the master Mobility Controller first.

2. Upgrade all local Mobility Controllers last.

NOTE: For proper operation, all Mobility Controllers in the network must be upgraded to use the same version of ArubaOS software.

Upgrading Redundant Controllers

When configuring master/local controllers in a redundant (VRRP) environment, the redundant controllers should be the same class of controller (5000, 6000, or 800) or better, running the same revision of ArubaOS.

Aruba recommends upgrading in the following order:

1. Upgrade the Master controller to the new software.

2. Reboot the Master controller.

3. Upgrade the Local controllers to the new software.

4. Do not reboot the Local controllers yet.

5. From the Master CLI, enter
   `apboot location 0.0.0`

6. Now reboot the Local controllers.

The APs should now have the new version of ArubaOS since they were rebooted and not failed over through VRRP.

Troubleshooting

If there is trouble with the controller (for example, insufficient – less than 10MB – flash space), do the following:

1. Disconnect the link to the APs.

2. Remove all unnecessary files from flash, including the db_dump.sql type files.

3. Remove any crash files.

4. Import the old wms DB file and reboot.

5. Reconnect the link for the APs.

Before You Call Technical Support

Before you place a call to Technical Support, please follow these steps:

1. Provide a detailed network topology (including all the devices in the network between the user and the Aruba WLAN controller with IP addresses and interface numbers if possible).

   The diagram can be a Visio, PowerPoint, JPEG, TIF, etc. file, or it can even be handwritten and faxed to support at 1-408-227-4550.

2. Provide the Aruba WLAN controller logs and output of the **show tech-support** command via the GUI Maintenance tab or via the CLI (**tar logs tech-support**).

3. Provide the Syslog server file of the Aruba WLAN controller at the time of the problem.

   If you do not have a Syslog server capturing logs of the Aruba WLAN controller, Aruba strongly recommends that you consider adding one.

4. Let the support person taking your call know if this is a new or existing installation.(This helps the support team to take different troubleshooting approaches depending on whether you have had:

   ● An outage in the network that worked in the past.

   ● A network configuration that has never worked.

   ● A brand new install.

5. Let the support person know if anything has recently changed in your network (external to Aruba) or if anything has recently been changed in the Aruba WLAN controller or AP configuration.

6. If there was a configuration change, please list the exact configuration steps and commands used.

7. Provide the date and time (if possible) when the problem first occurred

8. Is the problem reproducible? (If the problem is reproducible, please list the exact steps taken to recreate the problem.)

9. Please provide any wired or wireless Sniffer traces taken during the time of the problem.

10. Please provide the wireless device's make & model #, its OS version, including any service packs or patches, its wireless NIC make & model #, its wireless NIC's driver date & version, and its wireless NIC's configuration.

11. Please provide the Aruba WLAN controller site access information if possible.

   Aruba recommends that access to your site access should only be enabled when a problem occurs (or if Aruba support is monitoring the device), that access be restricted to a VPN (PPTP, L2TP, SSL) connection that limits the support person to only have IP access to the Aruba WLAN controller.

Documents Related to This Release

The following documents are included in this release:

- 0510281-04   *ArubaOS 2.4.8.11-FIPS Release Notes* (this document)
- 0510142-02   *FIPS 140-2 Level 2 Release Supplement for Aruba 800, 5000 and 6000 Mobility Controller with ArubaOS 2.4.8.0-FIPS Software*
- 0510237-01   *ArubaOS 2.4.8 User Guide*
- 0500024-03   *Aruba 5000/6000 Mobility Controller Installation Guide*
- 0500147-02   *Aruba 800-Series Mobility Controller Installation Guide*
- Aruba AP Installation Guide

This documentation library is updated continuously. You can download the latest version of any of these documents from:

https://support.arubanetworks.com

For More Information

To contact Aruba Wireless Networks, refer to the information below:

Web Site	
■ **Main Site**	http://www.arubanetworks.com
■ **Support Site**	http://www.arubanetworks.com/support
Telephone Numbers	
■ **Aruba Corporate**	408-227-4500
■ **FAX**	408-227-4550
■ **Support**	
● United States	800-WI-FI-LAN (800-943-4526)
● France	+33 (0) 170725559
● United Kingdom	+44 (0) 2071275989
● Germany	+49 (0) 69380977228
● All other countries	+00 1-408-754-1200