Chapter 4

Upgrade Procedures

This chapter details software and hardware upgrade procedures. Aruba best practices recommend that you schedule a maintenance window when upgrading your controllers.

Read all the information in this chapter before upgrading your controllers.

Topics in this chapter include:

All version assume that you have upgraded to the most recent version as posted on the Aruba download site. For instance, 3.3.x assumes you have upgraded to the most recent version of 3.3.

Important Points to Remember

Upgrading your Aruba infrastructure can be confusing. To optimize your upgrade procedure, take the actions listed below to ensure your upgrade is successful. You should create a permanent list of this information for future use.

- Best practices recommends upgrading during a maintenance window. This will limit the troubleshooting variables.
- Verify your current ArubaOS version (execute the **show version** or the **show image version** command).
- Verify which services you are using for each controller (for example, Employee Wireless, Guest Access, Remote AP, Wireless Voice).
- Verify the exact number of access points (APs) you have assigned to each controller.
- List which method each AP uses to discover each controller (DNS, DHCP Option, broadcast), and verify that those methods are operating as expected.
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- List the devices in your infrastructure that are used to provide your wireless users with connectivity (Core switches, radius servers, DHCP servers, firewall, for example).

Technical Upgrading Best Practices

- Know your topology. The most important path is the connectivity between your APs and their controllers. Connectivity issues will interfere with a successful upgrade. You must have the ability to test and make connectivity changes (routing, switching, DHCP, authentication) to ensure your traffic path is functioning.
- Avoid combining a software upgrade with other upgrades; this will limit your troubleshooting variables.
- Avoid making configuration changes during your upgrade.
- Notify your community, well in advance, of your intention to upgrade.
- Verify that all of your controllers are running the same software version in a master-local relationship. The same software version assures consistent behavior in a multi-controller environment.
- Use FTP to upload software images to the controller. FTP is much faster then TFTP and also offers more resilience over slower links.

If you must use TFTP, ensure that your TFTP servers can send more then 30 MB of data.

- Always upgrade the non-boot partition first. If something happens during upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.

Basic Upgrade Sequence

Testing your clients and ensuring performance and connectivity is probably the most time-consuming part of the upgrade. Best practices recommends that you enlist users in different locations to assist with the validation before you begin the upgrade. The list below is an overview of the upgrade and validation procedures.

If you manage your controllers via the AirWave Wireless Management Suite, the AirWave upgrade process automates most of these steps.

1. Upload the same version of the new software image onto all controllers.
2. Reboot all controllers simultaneously.
3. Execute the **ping -t** command to verify all your controllers are up after the reboot.
4. Open a Secure Shell session (SSH) on your Master Controller.
5. Execute the **show ap database** command to determine if your APs are up and read to accept clients.
6. Execute the **show ap active** to view the up and running APs.
7. Cycle between step 5 and step 6 until a sufficient amount of APs are confirmed up and running.

   The **show ap database** command displays all of the APs, up or down. If some access points are down, execute the **show datapath session table** <*access point ip address*> command and verify traffic is passing. If not, attempt to ping them. If they still do not respond, execute a **show ap database long** command to view the wired mac address of the AP; locate it in your infrastructure.
8. Verify that the number of access points and clients are what you would expected.
9. Test a different type of client for each access method (802.1x, VPN, Remote AP, Captive Portal, Voice) and in different locations when possible.

Managing Flash Memory

All Aruba controllers store critical configuration data on an onboard compact flash memory module. To maintain the reliability of your WLAN network, Aruba recommends the following compact flash memory best practices:

- Do not exceed the size of the flash file system. For example, loading multiple large building JPEGs for RF Plan can consume flash space quickly.

  Warning messages alert you that the file system is running out of space if there is a write attempt to flash and 5 Mbytes or less of space remains.

Other tasks which are sensitive to insufficient flash file system space include:

- DHCP lease and renew information is stored in flash. If the file system is full, DHCP addresses can not be distributed or renewed.
- If a controller encounters a problem and it needs to write a log file, it will not be able to do so if the file system is full and critical troubleshooting information will be lost

In certain situations, a reboot or a shutdown could cause the controller to lose the information stored in its compact flash card. To avoid such issues, it is recommended that you issue the **halt** command before rebooting.

Before you upgrade

You should ensure the following before installing a new image on the controller:

- Make sure you have at least 10 MB of free compact flash space (**show storage** command).
- Run the **tar crash** command to ensure there are no "process died" files clogging up memory and FTP/TFTP the files to another storage device.
- Remove all unnecessary saved files from flash (**delete filename** command).

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 external server or mass storage facility. At the very least, you should include the following files in these frequent backups:

- Configuration data
- WMS database
- Local user database
- Licensing database
- Floor plan JPEGs
- Customer captive portal pages
- Customer x.509 certificates

Backup and Restore Compact Flash on the WebUI

The WebUI provides the easiest way to back up and restore the entire compact flash file system. The following steps describe how to back up and restore the compact flash file system using the WebUI on the controller:

1. Navigate to the **Maintenance > File > Backup Flash** page.
2. Click **Create Backup** to back up the contents of the Compact Flash file system to the file flashbackup.tar.gz.
3. Click **Copy Backup** to copy the file to an external server.

You can later copy the backup file from the external server to the Compact Flash file system by navigating to the **Maintenance > File > Copy Files** page.

4. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > File > Restore Flash** page. Click **Restore**.

Backup and Restore Compact Flash on the CLI

The following steps describe the back up and restore procedure for the entire Compact Flash file system using the controller's command line:

1. Enter **enable** mode in the CLI on the controller. Use the **backup** command to back up the contents of the Compact Flash file system to the file flashbackup.tar.gz:

```
(host) # backup flash
Please wait while we tar relevant files from flash...
Please wait while we compress the tar file...
Checking for free space on flash...
Copying file to flash...
File flashbackup.tar.gz created successfully on flash.
```

2. Use the **copy** command to transfer the backup flash file to an external server:

```
(host) copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword>
<remote directory>
```

   You can later transfer the backup flash file from the external server to the Compact Flash file system with the copy command:

```
(host) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
```

3. Use the **restore** command to untar and extract the *flashbackup.tar.gz* file to the Compact Flash file system:

```
(host) # restore flash
```

License Mapping

License consolidation and even renaming of licenses occur over time. Figure 1 is an up-to-date illustration of the consolidated licenses effective with this release.

Licensing Change History

The following changes and/or consolidations were made to the ArubaOS licensing.

ArubaOS 5.0

- MAP was merged into base ArubaOS
- VPN was merged into base ArubaOS
- RAP was merged into AP license
- PEF (user basis) was converted to PEFNG (AP basis) with ArubaOS 5.0

ArubaOS 3.4.1

- VOC was merged into PEF. This merge happened with ArubaOS 3.4.1
- IMP was merged into base ArubaOS

ArubaOS 3.4.0

- ESI was merged into PEF

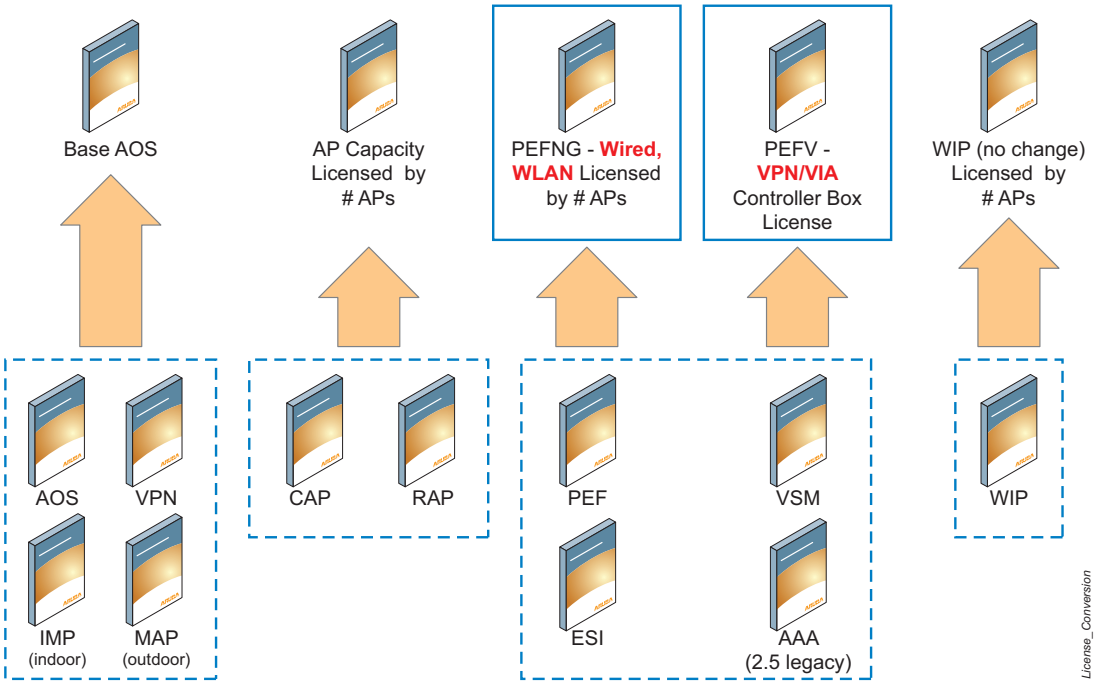
ArubaOS Legacy and End-of-Life

- AAA was merged into ESI with the release of ArubaOS 2.5.3.
- CIM is End-of-life

NOTE

Releases older than ArubaOS 2.5.4 have been End-of-Lifed.

Figure 1 *License Consolidation*



Upgrading from 3.4.x to 5.0

Read all the following information before you upgrade to ArubaOS 5.0.1. If you are upgrading from a version earlier than 3.4.x, see "Upgrading from 3.3.x to 5.0" on page 22 or "Upgrading from 2.5.x to 3.3.x to 5.0." on page 23.

Caveats

Before upgrading to ArubaOS 5.0 take note of these known upgrade caveats.

- If you have occasion to downgrade to a prior version, and your current ArubaOS 5.0 configuration has CPSec enabled, you must disable CPSec before you downgrade.

  For more information on configuring control plane security and auto-certificate provisioning, refer to the *ArubaOS 5.0 User Guide*.

Load New Licenses

Before you upgrade to ArubaOS 5.0, assess your software license requirements and load any new or expanded licenses you require prior to upgrading to ArubaOS 5.0.

Software licenses in ArubaOS 5.0 are consolidated and in some instances license names and modules are renamed to more accurately represent the modules supported by the licenses (see Figure 1).

For a detailed description of these new license modules, refer to the "Software Licenses" chapter in the user guide.

If you need to downgrade to ArubaOS 3.4.x, the previous licenses will be restored. However, once you upgrade again to ArubaOS 5.0 the licenses will no longer revert should you need to downgrade again.

Save your Configuration

Before upgrading, save your configuration and back up your controllers data files (see "Managing Flash Memory" on page 17). Saving your configuration saves the **admin** and **enable** passwords in the proper format.

Saving the Configuration on the WebUI

1. Click on the **Configuration** tab.
2. Click the **Save Configuration** button at the top of the screen.

Saving the Configuration on the CLI

Enter the following command in enable or config mode:

```
(host) #write memory
```

Install ArubaOS 5.0.1

Download the latest software image from the Aruba Customer Support website.

When upgrading the software in a multi-controller network (one that uses two or more Aruba controllers), special care must be taken to upgrade all the controllers in the network and to upgrade them in the proper sequence. (See "Upgrading in a Multi-Controller Network" on page 24.)

Install ArubaOS 5.0.1 on the WebUI

The following steps describe how to install the ArubaOS software image from a PC or workstation using the Web User Interface (WebUI) on the controller. You can also install the software image from a TFTP or FTP server using the same WebUI page.

1. Upload the new software image to a PC or workstation on your network.
2. Log in to the WebUI from the PC or workstation.
3. Navigate to the **Maintenance > Controller > Image Management** page. Select the Upload Local File option, then click the **Browse** button to navigate to the image file on your PC or workstation.
4. Determine which memory partition will be used to hold the new software image. Best practices is to load the new image onto the backup partition. To see the current boot partition, navigate to the **Maintenance > Controller > Boot Parameters** page.
5. Select **Yes** for Reboot Controller After Upgrade.
6. Click **Upgrade**.
7. When the software image is uploaded to the controller, a popup appears. Click **OK** in the popup window. The boot process starts automatically within a few seconds (unless you cancel it).

8. When the boot process is complete, log in to the WebUI and navigate to the **Monitoring > Controller > Controller Summary** page to verify the upgrade, including country code. The Country field displays the country code configured on the controller.

Install ArubaOS 5.0.1 on the CLI

The following steps describe how to install the ArubaOS software image using the CLI on the controller. You need a FTP/TFTP server on the same network controller you are upgrading.

1. Upload the new software image to your FTP/TFTP server on your network.
2. Execute the ping command to verify the network connection from the target controller to the FTP/TFTP server:

```
(host) # ping <ftphost>
or
(host) # ping <tftphost>
```

A valid IP route must exist between the FTP/TFTP server and the controller. A placeholder file with the destination filename and proper write permissions must exist on the FTP/TFTP server prior to executing the **copy** command.

3. Determine which partition d to load the new software image. Use the following command to check the partitions:

```
#show image version
-----------------------------------
Partition               : 0:0 (/dev/hda1) **Default boot**
Software Version        : ArubaOS 3.3.1.23 (Digitally Signed - Production Build)
Build number            : 20219
Label                   : 20219
Built on                : 2009-05-11 20:51:46 PST
-----------------------------------
Partition               : 0:1 (/dev/hda2)
/dev/hda2: Image not present
```

Best practices is to load the new image onto the backup partition (the non-boot partition). In the above example, partition 0 is the boot partition. Partition 1 is empty (image not present) and can be used to load the new software.

4. Use the **copy** command to load the new image onto the controller:

```
(host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
or
host) # copy tftp: <tftphost> <image filename> system: partition 1
```

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

5. Execute the **show image version** command to verify the new image is loaded:

```
(host) #show image version
-----------------------------------
Partition               : 0:0 (/dev/hda1) **Default boot**
Software Version        : ArubaOS 4.3.0.0 (Digitally Signed - Production Build)
Build number            : 23623
Label                   : 23623
Built on                : Wed Mar 10 09:11:59 PST 2009
-----------------------------------
Partition               : 0:1 (/dev/hda2)
Software Version        : ArubaOS 5.0.0.0 (Digitally Signed - Production Build)
Build number            : 23711
Label                   : 23711
Built on                : Wed Mar 24 09:11:59 PST 2010
```

6. Reboot the controller:

```
(host) # reload
```

7. Execute the **show version** command to verify the reload and upgrade is complete.

```
(host) #show version
Aruba Operating System Software.
ArubaOS (MODEL: Aruba 3200-US), Version 5.0.0.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2010, Aruba Networks, Inc.
Compiled on 2010-04-25 at 15:18:56 PDT 5.0.0.0 (Digitally Signed - Production Build)
...
```

Upgrading from 3.3.x to 5.0

The following steps describe how to install the ArubaOS software image from a PC or workstation using the Web User Interface (WebUI) on the controller. You can also install the software image from a FTP/TFTP server using the same WebUI page.

Upgrading on the WebUI

1. Upload the new software image to a PC or workstation on your network.
2. Log in to the WebUI from the PC or workstation.
3. Navigate to the **Maintenance > Controller > Image Management** page. Select the Upload Local File option, then click the **Browse** button to navigate to the image file on your PC or workstation.
4. Determine which memory partition will be used to hold the new software image. Best practices is to load the new image into the backup partition. To view the current boot partition, navigate to the **Maintenance > Controller > Boot Parameters** page.
5. Select **Yes** for Reboot Controller After Upgrade.
6. Click **Upgrade**.
7. When the software image is uploaded to the controller, a popup appears. Click **OK** in the popup window. The boot process starts automatically within a few seconds (unless you cancel it).
8. When the boot process is complete, log in to the WebUI and navigate to the **Monitoring > Controller > Controller Summary** page to verify the upgrade, including country code. The Country field displays the country code configured on the controller.

Upgrading on the CLI

The following steps describe how to install the ArubaOS software image using the CLI on the controller. You need a FTP/TFTP server on the same network controller you are upgrading.

1. Upload the new software image to your FTP/TFTP server on your network.
2. Execute the ping command to verify the network connection from the target controller to the FTP/TFTP server:

```
(host) # ping <ftphost>
```

or

```
(host) # ping <tftphost>
```

A valid IP route must exist between the FTP/TFTP server and the controller. A placeholder file with the destination filename and proper write permissions must exist on the FTP/TFTP server prior to executing the **copy** command.

3. Determine which partition to load the new software image. Best practices are to load the new image onto the backup partition (the non-boot partition). In the above example, partition 0 is the boot partition. Partition 1 is empty (image not present) and can be used to load the new software.
4. Use the **copy** command to load the new image onto the controller:

```
(host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
```

or

```
host) # copy tftp: <tftphost> <image filename> system: partition 1
```

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

5. Verify that the new image is loaded:

```
(host) # show image version
```

6. Reboot the controller:

```
(host) # reload
```

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

Upgrading from 2.5.x to 3.3.x to 5.0.

Upgrading from ArubaOS 2.5.x to ArubaOS 5.0 requires an "upgrade hop". That is, you must upgrade from ArubaOS 2.5.x to ArubaOS 3.3.x first and then from ArubaOS 3.3.x to ArubaOS 5.0.

Once you have completed the upgrade to the latest version of 3.3.x, then follow the steps in "Upgrading from 3.3.x to 5.0" on page 22 to complete your last "upgrade hop".

To assist you with this migration, Aruba Networks, Inc. provides comprehensive web site with migration tools listed below.

https://support.arubanetworks.com/MIGRATIONTOOL/tabid/85/Default.aspx

The tools include:

- Migration Design Guide

  https://support.arubanetworks.com/UPGRADEGUIDE/tabid/88/Default.aspx)
- Video

  https://support.arubanetworks.com/UPGRADETUTORIAL/tabid/87/Default.aspx
- Online Migration Tool

  https://support.arubanetworks.com/25to3xTool/tabid/84/Default.aspx

Upgrading from RN-3.x.x to 5.0

If you are upgrading from a releaser older than RN-3.1.4, you must upgrade to the most recent RN build that is available on the support site. Once your RN release is current, you can upgrade to ArubaOS 5.0.

Once you have completed the upgrade to the latest version of RN-3.x.x, then follow the steps in "Upgrading from 3.3.x to 5.0" on page 22 to complete your last "upgrade hop".

Caveat

Should you need to downgrade from ArubaOS 5.0., you can only downgrade to version RN-3.1.4.

Upgrading in a Multi-Controller Network

In a multi-controller network (a network with two or more Aruba controllers), special care must be taken to upgrade all controllers based on the controller type (master or local). Be sure to back up all controllers being upgraded, as described in "Backing up Critical Data" on page 17.

NOTE

For proper operation, all controllers in the network must be upgraded with the same version of ArubaOS software. For redundant (VRRP) environments, the controllers should be the same model.

To upgrade an existing multi-controller system to ArubaOS 5.0:

1. Load the software image onto all controllers (including redundant master controllers).
2. If all the controllers cannot be upgraded with the same software image and reloaded simultaneously, use the following guidelines:
   a. Remove the link between the master and local mobility controllers.
   b. Upgrade the software image, then reload the master and local controllers one by one.
   c. Verify that the master and all local controllers are upgraded properly.
   d. Connect the link between the master and local controllers.

Pre-shared Key for Inter-Controller Communication

A pre-shared key (PSK) is used to create IPSec tunnels between a master and backup master controllers and between master and local controllers. These inter-controller IPSec tunnels carry management traffic such as mobility, configuration, and master-local information.

NOTE

An inter-controller IPSec tunnel can be used to route data between networks attached to the controllers. To route traffic, configure a static route on each controller specifying the destination network and the name of the IPSec tunnel.

There is a default PSK to allow inter-controller communications, however, for security you need to configure a a unique PSK for each controller pair. You can use either the WebUI or CLI to configure a 6-64 character PSK on master and local controllers.

CAUTION

Do not use the default global PSK on a master or standalone controller. If you have a multi-controller network then configure the local controllers to match the new IPSec PSK key on the master controller. Leaving the PSK set to the default value exposes the IPSec channel to serious risk, therefore you should always configure a unique PSK for each controller pair.

Downgrading after an Upgrade

If necessary, you can return to your previous version of ArubaOS.

WARNING

If you upgraded from 3.3.x to 5.0, the upgrade script encrypts the internal database. Any new entries that were created in ArubaOS 5.0.1 will be lost after downgrade (this warning does not apply to upgrades from 3.4.x to 5.0),

Before you reboot the controller with the pre-upgrade software version, you must perform the following steps:

1. Verify that Disable Control Plane Security (CPSec) is disabled.

2. Set the controller to boot with the previously-saved pre-upgrade configuration file.
3. Set the controller to boot from the system partition that contains the pre-upgrade image file.

When you specify a boot partition (or copy an image file to a system partition), the software checks to ensure that the image is compatible with the configuration file that will be used on the next controller reload. An error message displays if a system boot parameters are set for incompatible image and configuration files.

After downgrading the software on the controller:

- Restore your configuration from your pre-upgrade configuration back up stored on your flash file. Do not restore the flash file system from a ArubaOS 5.0.1 backup file.
- You do not need to re-import the WMS database or RF Plan data. However, if you have added changes to RF Plan in ArubaOS 5.0.1, the changes will not appear in RF Plan in the downgraded ArubaOS version.
- If you installed any certificates while running ArubaOS 5.0.1, you need to reinstall the certificates in the downgraded ArubaOS version.

The following sections describe how to use the WebUI or CLI to downgrade the software on the controller.

Be sure to back up your controller before reverting the OS.

When reverting the controller software, whenever possible use the previous version of software known to be used on the system. Loading a release not previously confirmed to operate in your environment could result in an improper configuration.

Downgrading on the WebUI

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, copy the file to the controller by navigating to the **Maintenance > File > Copy Files** page.
   a. For Source Selection, select FTP/TFTP server, and enter the IP address of the FTP/TFTP server and the name of the pre-upgrade configuration file.
   b. For Destination Selection, enter a filename (other than default.cfg) for Flash File System.
2. Set the controller to boot with your pre-upgrade configuration file by navigating to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the saved pre-upgrade configuration file from the Configuration File menu.
   b. Click **Apply**.
3. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Controller > Image Management** page. If there is no previous software image stored on your system partition, load it into the backup system partition (you cannot load a new image into the active system partition):
   a. Enter the FTP/TFTP server address and image file name.
   b. Select the backup system partition.
   c. Click **Upgrade**.
4. Navigate to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the system partition that contains the pre-upgrade image file as the boot partition.
   b. Click **Apply**.
5. Navigate to the **Maintenance > Controller > Reboot Controller** page. Click **Continue**. The controller reboots after the countdown period.
6. When the boot process is complete, verify that the controller is using the correct software by navigating to the **Maintenance > Controller > Image Management** page.

Downgrading on the CLI

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the controller:

   ```
   (host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
   ```

   or

   ```
   (host) # copy tftp: <tftphost> <image filename> system: partition 1
   ```

2. Set the controller to boot with your pre-upgrade configuration file.

   ```
   # boot config-file <backup configuration filename>
   ```

3. Execute the **show image version** command to view the partition on which your previous software image is stored.

   In the following example, partition 0, the backup system partition, contains the backup release 3.4.1.23. Partition 1, the default boot partition, contains the ArubaOS 5.0.1 image:

   ```
   #show image version
   ---------------------------------
   Partition               : 0:0 (/dev/hda1)
   Software Version        : ArubaOS 3.4.1.23 (Digitally Signed - Production Build)
   Build number            : 20219
   Label                   : 20219
   Built on                : 2009-12-11 20:51:46 PST
   ---------------------------------
   Partition               : 0:1 (/dev/hda2) **Default boot**
   Software Version        : ArubaOS 5.0.0.0 (Digitally Signed - Production Build)
   Build number            : 23711
   Label                   : 23711
   Built on                : 2010-03-25 01:59:13 PDT
   ```

You cannot load a new image into the active system partition (the default boot).

4. Set the backup system partition as the new boot partition:

   ```
   # boot system partition 0
   ```

5. Reboot the controller:

   ```
   # reload
   ```

6. When the boot process is complete, verify that the controller is using the correct software:

   ```
   # show image version
   ```

Controller Migration

This section outlines the steps involved in migrating from an Aruba PPC controller environment to MIPS controller environment. These steps takes into consideration the common Aruba WLAN controller environment. You must have an operational PPC controller in the environment when migrating to a new controller. The controllers are classified as:

- MIPS Controllers—M3, Aruba 3000 Series, 600 Series
- PPC Controllers—Aruba 200, Aruba 800, Aruba 2400, 5000 and SC1/SC2

Use this procedure to upgrade from one Aruba controller model to another. Take care to ensure that the new controller has equal or greater capacity than the controller you are replacing.

Migration instructions include:

- "Single Controller Environment" on page 27
- "Multiple Master Controller Environment" on page 27
- "Master/Local Controller Environment" on page 27

Single Controller Environment

A single controller environment is one active controller, or one master controller that may have standby master controller that backs up the master controller.

- Replacing the standby controller—Does not require downtime
- Replacing the master controller—Requires downtime

Multiple Master Controller Environment

An all master environment is considered an extension of the single master controller. You can back up the master controllers with a standby controller. In an all master controller deployment, each master controller is migrated as if it were in a standalone single controller environment.

For every master-standby controller pair

- Replacing the standby controller—Does not require downtime
- Replacing the master controller—Requires downtime

Master/Local Controller Environment

In a master/local environment, replace the master controller first and then replace the local controllers.

- Replacing the local standbys (when present)
- Replacing local controllers—one controller at a time

Before You Start

You must have:

- Administrative access to the controller via the network
- Administrative access to the controller via the controller's serial port
- Pre-configured FTP/TFTP server that can be reached from the controller
- Aruba serial cable
- The ArubaOS version (same as the rest of the network)

Basic Migration Steps

1. Upgrade your network to the newer image to ensure that the image on the newer controllers match the image on the rest of the controllers in your network.
2. Backup the controller data from the PPC controller.
3. Physically swap the hardware (for example, mounting, cabling, power).
4. Initialize the new controller.
5. Install the backed up data onto the new controller.
6. Test the new setup.

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 controller with IP addresses and Interface numbers if possible).
2. Provide the controller logs and output of the **show tech-support** command via the WebUI Maintenance tab or via the CLI (**tar logs tech-support**).
3. Provide the syslog file of the controller at the time of the problem.

   Aruba strongly recommends that you consider adding a syslog server if you do not already have one to capture from the controller.
4. Let the support person know if this is a new or existing installation. This helps the support team to determine the troubleshooting approach, depending on whether you have:
   - an outage in a network that worked in the past.
   - a network configuration that has never worked.
   - a brand new installation.
5. Let the support person know if there are any recent changes in your network (external to the Aruba controller) or any recent changes to your controller and/or AP configuration.
6. If there was a configuration change, list the exact configuration steps and commands used.
7. Provide the date and time (if possible) when the problem first occurred.
8. If the problem is reproducible, list the exact steps taken to recreate the problem.
9. Provide any wired or wireless sniffer traces taken during the time of the problem.
10. Provide the wireless device's make and model number, OS version (including any service packs or patches), wireless NIC make and model number, wireless NIC's driver date and version, and the wireless NIC's configuration.
11. Provide the controller site access information, if possible.

Contacting Support

Table 1 *Web Sites and Emails*

Web Site	
• Main Site	http://www.arubanetworks.com
• Support Site	https://support.arubanetworks.com
• Software Licensing Site	https://licensing.arubanetworks.com/login.php
• Wireless Security Incident Response Team (WSIRT)	http://www.arubanetworks.com/support/wsirt.php
Support Emails	
Americas and APAC	support@arubanetworks.com
EMEA	emea_support@arubanetworks.com
WSIRT Email Please email details of any security problem found in an Aruba product.	wsirt@arubanetworks.com

Table 2 *Contact Phone Numbers*

Telephone Numbers	
• Aruba Corporate	+1 (408) 227-4500
• FAX	+1 (408) 227-4550
Support	
United States	800-WI-FI-LAN (800-943-4526)
Universal Free Phone Service Number (UIFN): Australia, Canada, China, France, Germany, Hong Kong, Ireland, Israel, Japan, Korea, Singapore, South Africa, Taiwan, and the UK	+800-4WIFI-LAN (+800-49434-526)
All other countries	+1 (408) 754-1200