AOS-W 3.4

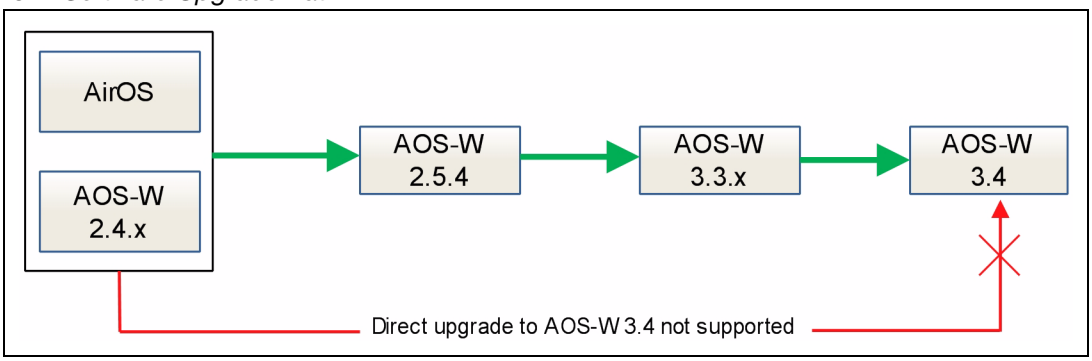
Software Upgrade Guide

This document describes how to upgrade your switch to AOS-W 3.4.

Software Upgrade Path

The following illustration describes the appropriate upgrade path to AOS-W 3.4.

Figure 1 *Software Upgrade Path*



Before You Begin

Review the following checklist and notes before you begin the upgrade process:

1. Read the *AOS-W 3.4 Release Notes* for information about new features and fixed and known issues for this release.
2. Do not upgrade to AOS-W 3.4 at this time if your network contains AP 52s. The AP 52 is not supported with the AOS-W 3.4 release.
3. Keep the migration document handy if you are upgrading from a 2.5.x release. You can download the migration guide from https://service.esd.alcatel-lucent.com.

Preparing for AOS-W 3.4 Upgrade

The following tasks are essential before you upgrade to AOS-W 3.4.


NOTE

Before upgrading your switch, review the configuration changes for AOS-W 3.3.x, as described in "Upgrading from 3.3.x and Earlier Release" on page 9 and "Upgrading from 2.5.x" on page 14. Also, review the “Known Issues and Limitations” section in the *AOS-W 3.4 Release Notes* for upgrade issues.

Obtain Licenses

Information about AOS-W 3.4 licenses and procedure to obtain them are described in detail in the “Software Licenses” chapter of *AOS-W 3.4 User Guide*. Ensure that you follow the instructions carefully to obtain and install the AOS-W 3.4 licenses in your switch.

Verify the Configured Country Code

In AOS-W 3.4, the country code is saved to the hardware and cannot be changed for certain countries. Before upgrading to AOS-W 3.4, make sure the correct country code is saved in the switch’s configuration file.

- To verify the country code using the WebUI, navigate to the **Monitoring > Switch > Switch Summary** page. The Country field displays the country code configured on the switch.
- To verify the country code using the CLI, run the following command in enable mode:

  ```
  (host) # show startup-config | include country
  ```

  - If the country code is *correct*, proceed with the upgrade. Remember that you must have AOS-W 3.3.x or later installed on the switch before you upgrade to AOS-W 3.4.
  - If the country code is *incorrect*, disable master-local switch updates by either disconnecting the local switch link or increasing the heartbeat value to a large interval (for example, issue the CLI command **cfgm set heartbeat 100000**).

To correct the country code before upgrading to AOS-W 3.4:

- Restore the switch to its factory defaults and perform a fresh manual configuration. This method is recommended for switches where there is a minimum amount of configuration required, for example, a local switch that downloads most of its configuration from a master switch.
- Send the Compact Flash backup file to Alcatel-Lucent Technical Support, along with the country to be configured. Technical Support will send back a revised file which you then restore to the switch.

The following sections describe the steps for each option.

Restore the Switch to Factory Defaults and Reconfigure

Complete the following steps to modify the country code and perform a fresh configuration on the switch. After configuring the switch, proceed to the steps in "Upgrading to AOS-W 3.4" on page 4.

Using the WebUI to Backup Current Configuration

Backup the current configuration

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.
4. Disconnect the switch from the network.

Reset the switch

1. Navigate to the **Maintenance > Switch > Clear Config** page.
2. Click **Continue**.

   This returns the switch to its factory defaults and reboots it with the default IP address 172.16.0.254.

Using the CLI to Backup Current Configuration

1. Backup the current configuration, as described in "Backing up Critical Data" on page 5.
2. Disconnect the switch from the network.
3. Reset and reboot the switch, using the following command sequence:

```
(host) # write erase
All the configuration will be deleted. Press 'y' to proceed: y
(host) # reload
Do you really want to reset the system(y/n): y
```

   This returns the switch to its factory defaults and reboots it with the default IP address 172.16.0.254.

Run the Initial Setup

During the Initial Setup, specify the country code for the country in which the switch will operate. After completing the setup, the switch reboots with the new country code. See the AOS-W 3.4 *Quick Start Guide* for information about running the Initial Setup.

Verify country code after the boot process is complete

- If the country code is incorrect, contact Alcatel-Lucent Customer Support.
- If the country code is correct, reconnect the switch to the network and reconfigure the switch.

Send the Compact Flash Backup File to Technical Support

Back up the entire Compact Flash file system to the *flashbackup.tar.gz* file. Send the file to Alcatel-Lucent Technical Support, along with the country to be set. Technical Support will send back a revised *flashbackup.tar.gz* file, which you can restore to the switch. After you restore the Compact Flash file system, proceed to the instructions in "Upgrading to AOS-W 3.4" on page 4.

Using the WebUI to Create and Restore CF Backup

To create the *flashbackup.tar.gz* file:

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.

To restore the revised *flashbackup.tar.gz* file:

1. Copy the backup file from an external server to the Compact Flash file system by navigating to the **Maintenance > File > Copy Files** page.
2. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > File > Restore Flash** page. Click **Restore**.

Using the CLI to Create and Restore CF Backup

To create the *flashbackup.tar.gz* file:

1. Enter **enable** mode in the CLI on the switch. 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.
Please copy it out of the switch and delete it when done.
```

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

```
(host) # copy flash: flashbackup.tar.gz tftp: <TFTP server IP address> <filename>
```

To restore the revised *flashbackup.tar.gz* file:

1. 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: <TFTP server IP address> <filename> flash: flashbackup.tar.gz
```

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

```
restore flash
```

Upgrading to AOS-W 3.4

If you are currently running AirOS or AOS-W 2.4.x on your switch, you must upgrade the switch image to AOS-W 2.5.4 or later *before* you upgrade the switch to AOS-W 3.4.

Upgrade from 2.4.x directly to 3.3.x is not supported.

Before upgrading to AOS-W 3.4 make sure the correct country code is saved in the configuration file. Refer to the instructions described in "Verify the Configured Country Code" on page 2.

After the upgraded switch boots up with AOS-W 3.4, save the configuration to save the **admin** and **enable** passwords in the proper format

Managing Flash Memory

All Alcatel-Lucent switches store critical configuration data on an onboard compact flash memory module. To maintain the reliability of your WLAN network, Alcatel-Lucent recommends the following general best practices with respect to the use of your Alcatel-Lucent switch and its compact flash memory:

- Be careful not to 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:

- Using the internal database. DHCP lease and renew information is also stored in flash. If the file system is full, DHCP addresses will not be distributed or renewed.
- If a switch encounters a problem and 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

In certain situations, during a reboot or a shutdown you could lose the information stored in your compact flash card. To avoid such issues, it is recommended that you issue the **halt** command before rebooting or powering off your switch.

Prerequisites

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

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

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

All the above files reside on the compact flash file system on the Alcatel-Lucent switch.

Using the WebUI to Backup and Restore CF File System

If supported on your current AOS-W image, 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 switch:

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**.

Using the CLI to Backup and Restore CF File System

The following steps describe how to back up and restore the entire Compact Flash file system using the CLI on the switch:

1. Enter **enable** mode in the CLI on the switch. 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.
   Please copy it out of the switch and delete it when done.
   ```

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

   ```
   (host) # copy flash: flashbackup.tar.gz tftp: <TFTP server IP address> <filename>
   ```

   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: <TFTP server IP address> <filename> flash: flashbackup.tar.gz
   ```

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

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

Installing AOS-W 3.4

Obtain the latest, valid switch software image from the Alcatel-Lucent Customer Support website. Back up your current switch configuration and data files, as described in "Backing up Critical Data" on page 5.

Recommendations

- Alcatel-Lucent recommends scheduling network downtime when upgrading your switches to AOS-W 3.3.x
- The most current switch software image may be newer than that available at the time these installation instructions were written. Alcatel-Lucent recommends that you always download the latest software image from Alcatel-Lucent Customer Support before proceeding with these installation instructions.

When upgrading the software in a multi-switch network (one that uses two or more Alcatel-Lucent switches), special care must be taken to upgrade all the switches in the network and to upgrade them in the proper sequence. (See "Upgrading to AOS-W 3.4 in a Multi-Switch Network" on page 8.)

Using the WebUI to Install AOS-W 3.4

The following steps describe how to install the AOS-W software image from a PC or workstation using the Web User Interface (WebUI) on the switch. 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 > Switch > 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. It is recommended to load the new image into the backup partition. (To see the current boot partition, navigate to the **Maintenance > Switch > Boot Parameters** page.
5. Select **Yes** for Reboot Switch After Upgrade.
6. Click **Upgrade**.
7. When the software image is uploaded to the switch, 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 > Switch > Switch Summary** page to verify the upgrade, including country code. The Country field displays the country code configured on the switch.

Using the CLI to Install AOS-W 3.4

The following steps describe how to install the AOS-W software image using the CLI on the switch. You need to have a TFTP server on your network from which the image will be downloaded to the switch.

1. Upload the new software image to a TFTP server on your network.
2. From the CLI on the switch, verify the network connection from the target switch to the TFTP server:

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

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

3. Determine which memory partition will be used to hold the new software image. Use the following command to check the memory partitions:

   ```
   #show image version
   ----------------------------------
   Partition               : 0:0 (/dev/hda1) **Default boot**
   Software Version        : AOS-W 3.3.1.0 (Digitally Signed - Production Build)
   Build number            : 19148
   Label                   : 19148
   Built on                : 2008-08-10 04:26:35 PDT
   ----------------------------------
   Partition               : 0:1 (/dev/hda2)
   /dev/hda2: Image not present
   ```

   It is recommended to 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.
4. Use the **copy** command to load the new image into the switch:

   ```
   (host) # copy tftp: <server address> <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 switch is rebooted. There is no need to manually select the partition.

5. Verify that the new image is loaded:

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

   Information about the newly loaded software image should be displayed for the appropriate partition.
6. Reboot the switch:

```
(host) # reload
```

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

```
(host) #show version
Alcatel-Lucent Operating System-Wireless.
AOS-W (MODEL: OAW-4302), Version 3.4.0.0
Website: http://www.alcatel.com/enterprise
All Rights Reserved (c) 2005-2009, Alcatel-Lucent.
Compiled on 2009-05-31 at 22:32:40 PDT (build 21443) by p4build

ROM: System Bootstrap, Version CPBoot 1.2.11 (Sep 13 2005 - 17:39:11)

Switch uptime is 2 minutes 28 seconds
Reboot Cause: User reboot.
Supervisor Card
Processor  16.20 (pvr 8081 1014) with 256M bytes of memory.
32K bytes of non-volatile configuration memory.
256M bytes of Supervisor Card System flash (model=CF 256MB).
```

In this example, version AOS-W 3.4 is loaded and running, indicating that the upgrade is complete.

Saving the Configuration

After the switch has reloaded with AOS-W 3.4, save the current system configuration. This saves the **admin** and **enable** passwords in the proper format.

Using the WebUI

1. Navigate to the **Configuration** page.
2. Click the **Save Configuration** button at the top of the screen.

Using the CLI

Enter the following command in enable or config mode:

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

Upgrading to AOS-W 3.4 in a Multi-Switch Network

In a multi-switch network (a network with two or more Alcatel-Lucent switches), special care must be taken to upgrade all switches in the proper sequence, based on the switch type (master or local). Be sure to back up all switches being upgraded, as described in "Reverting to AOS-W 3.3.x or Later" on page 23.

For proper operation, all switches in the network must be upgraded to use the same version of AOS-W software. For redundant (VRRP) environments, the switches should be the same model.

To upgrade an existing multi-switch system to AOS-W 3.4:

1. Load the software image onto all switches (including redundant master switches).
2. If all the switches cannot be loaded with the same software image and reloaded simultaneously, use the following guidelines:
   a. Remove the link between the master & local mobility switches.
   b. Load the software image and reload the master & local mobility switches separately at a time of your preference.
   c. Make sure that the master & all local mobility switches are upgraded properly.

d. Connect the link between the master & local mobility switches.

Preshared Key for Inter-Switch Communication

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

An inter-switch IPSec tunnel can be used to route data between networks attached to the switches if you have installed VPN licenses in the switches. To route traffic, configure a static route on each switch specifying the destination network and the name of the IPSec tunnel.

There is a default PSK to allow inter-switch communications, however, for security you need to configure a a unique PSK for each switch pair. See the “Best Security Practices for the Preshared Key” section on page 366 of the *AOS-W 3.4 User Guide*. You can use either the WebUI or CLI to configure a 6-64 character PSK on master and local switches

Do not use the default global PSK on a master or stand-alone switch. If you have a multi-switch network then configure the local switches to match the new IPSec PSK key on the master switch. 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 switch pair.

Upgrading from 3.3.x and Earlier Release

This section describes important upgrade information that are useful if you are upgrading from AOS-W 3.3.x and earlier release to AOS-W 3.4.

Important information regarding configuration differences between AOS-W 3.4 and previous releases, including 3.3.x releases are also described in this section. In addition to the information described in this section, see "Upgrading from 2.5.x" on page 14 for more 3.3.x configuration information.

Upgrading from 2.4.x directly to AOS-W 3.4 is not supported.

- **Upgrade to AOS-W 2.5.4**—If you are currently running AirOS or AOS-W 2.4.x on your switch, you must first upgrade the switch image to AOS-W 2.5.4 or later *before* you upgrade the switch to AOS-W 3.3.x.
- **Use FTP to copy image**—If you are upgrading from a version prior to AOS-W 3.4, you must use FTP instead of TFTP to copy the image to your switch.
- **Reset switch to factory-default mode**—Reset your switch to factory default mode to use the new switch setup wizard. The switch setup wizard steps you through the tasks of configuring the switch and installing software licenses.You can use WebUI or CLI to reset your switch to factory-default mode.

  Using the WebUI

  1. Navigate to the **Maintenance > Switch > Clear Config** page.
  2. Click **Continue** to return the switch to its factory-default state.
  3. At the pop-up window, click **Yes** to reboot the switch.

Using CLI

```
(host) #write erase
(host) #reload
```

Do not issue the '`write erase all`' command if you have previously installed a license in the switch, as this command will effectively remove licenses as well as existing configurations. The Setup Wizard will display any installed licenses.

Configuration File

When you first boot up the switch after upgrading to AOS-W 3.4, the previous configuration is automatically backed up. The AOS-W 3.4 configuration file is not compatible with previous releases of AOS-W. To downgrade from AOS-W 3.4 to an earlier release, follow the steps below:

1. Set the switch to boot with the previously-saved pre-3.3.x configuration file
2. *S*et the system partition that contains the pre-3.3.x image file.

An error message displays if you set system boot parameters for incompatible image and configuration files.

See "Reverting to AOS-W 3.3.x or Later" on page 23 for instructions on downgrading from AOS-W 3.4.

Admin and Enable Passwords

When you upgrade a switch to AOS-W AOS-W 3.4, the configuration is automatically converted to the AOS-W 3.4 format, with the exception of the **admin** and **enable** passwords. To save the passwords in the proper AOS-W 3.4 format, you must explicitly save the configuration using either the WebUI or CLI (see "Saving the Configuration" on page 8.)

Captive Portal Certificate

In AOS-W 3.1.x or earlier releases, the certificate used with captive portal is stored separately from other certificates, including the certificate called "default" (this is the server certificate that is factory-installed in the switch). In AOS-W 3.4, all certificates are stored in the same location. When you upgrade the switch to AOS-W 3.4, the "default" certificate is replaced by the captive portal certificate used in the previous release.

In AOS-W 3.3.x, you can install a server certificate for captive portal from the certificate upload page in the WebUI (navigate to the **Configuration** > **Management** > **Certificates** > **Upload** page). You then select the certificate for use with captive portal by navigating to the **Configuration** > **Management** > **General** page.

If you had installed a server certificate for captive portal in a previous AOS-W release, you need to reimport the certificate using the certificate upload page. Then select the certificate for captive portal.

The factory-installed "default" server certificate is intended for demonstration purposes only and should not be used for authentication in a production environment. Alcatel-Lucent strongly recommends that you obtain and use custom certificates issued for your site or domain by a trusted Certificate Authority.

Bandwidth Contracts

In previous releases, you could configure a bandwidth contract for a user role, however, the same bandwidth rate is applied to both upstream and downstream traffic. This release allows you to apply different bandwidth contracts to upstream or downstream traffic for the same user role or for each user in a specified user role. When you upgrade to AOS-W 3.4, any previously-configured bandwidth rate is applied to both upstream and downstream traffic for the user role.

Remote AP

When you upgrade from AOS-W 3.1.x with an existing remote AP configuration to AOS-W 3.4, note the following guidelines:

- If you have an existing remote AP configuration with bridge SSIDs, create an initial role after upgrading to AOS-W 3.4 that allows those users unrestricted network access. To do this, select the predefined "*allowall*" firewall policy for the initial role. After gaining network access with the initial role, clients can then be placed into other user roles as they pass authentication.

  For more information about user roles, see Chapter 10, "Configuring Roles and Policies", of the *AOS-W 3.4 User Guide*.
- In previous releases, remote APs did not support LMS. If an LMS IP address was configured in the AP system profile, remote APs would ignore this configuration. In AOS-W 3.4, remote APs support LMS. If your configuration has an internal LMS IP address, remote APs may attempt to switch over to the LMS IP address, which is not reachable from the Internet. If this occurs, remote APs will not come up after the upgrade.

  As a workaround if you are migrating from an earlier AOS-W release, create two different AP groups before upgrading to AOS-W 3.4: one for thin APs and one for remote APs.

  As a workaround if you are migrating from AOS-W 2.5.x, create two different location codes before upgrading: one for thin APs and one for remote APs. When you upgrade to AOS-W 3.4, APs with a specific location code are automatically provisioned into a corresponding AP group. See "AP Names and Groups" on page 15.

  For remote APs, ensure that the LMS IP address in the AP system profile for the AP group has an externally routable IP address. For more information about AP groups, see Chapter 5, "Configuring Access Points," of the *AOS-W 3.4 User Guide*.

Layer-2 Tunneling Protocol

If you have more than 641,560 IP addresses (10 Class C subnets) in a Layer-2 Tunneling Protocol (L2TP) pool, you may lose that configuration when upgrading to AOS-W 3.4. To ensure a successful upgrade, reduce the number of IP addresses in the L2TP pool before upgrading to AOS-W 3.3.x.

Mesh

The AOS-W 3.4 upgrade script converts the old mesh configuration to new configuration. The Configuration file *default.cfg* is available in the */flash/config/* folder of the switch. It contains all relevant information which the switch should load during reload. As part of 3.4 release, the radio on which the mesh is configured can be used to access virtual APs. This makes a mesh radio behave as any other radio.

Before the AOS-W 3.4 release, a mesh radio profile (MRP) configuration contained the 11a-channel, 11g-channel, beacon period, and Tx-power details. These configuration parameters are now moved to the regular radio profile and removed from the MRP configuration.

The upgrade script for mesh creates and modifies the following parameters:

- Mesh Radio Profile
- AP Group
- AP Name
- Dot11a/g Profile

Mesh radio profile

For each MRP, the upgrade script generates a dot11a/dot11g radio profile with the radios in disabled state and Tx-power set to max if its not explicitly specified in MRP. The beacon period, Tx-power, channel-a, and

channel-g values are copied to the new dot11a/g profile. The name of the new radio profile is the MRP name suffixed with **-MeSh** string.

See the following example:

```
ap mesh-radio-profile "default"
   children 23
   11g-portal-channel   1
   11a-portal-channel   44
   Beacon-period      80
!
rf dot11a-radio-profile "default_MeSh"
   no radio-enable
   channel 44
   Beacon-period      80
   Tx-power       127
!
rf dot11g-radio-profile "default_MeSh"
   no radio-enable
   channel 1
   Beacon-period      80
   Tx-power       127
!
```

AP Group

For each group that has a mesh cluster profile, the upgrade script will create new group suffixed with **_MeSh** string. Except for the dol11a/g profiles, the new AP group will contain values similar to the previous group, and will modify dot11a/g profiles based on mesh cluster profile. If mesh cluster profile references *a*, then dot11a profile will be modified to form the new profiles with the MRP name.

Table 1 *Example of Old and New Mesh Group*

Old Group	New Group
ap-group "mesh grp2" dot11a-radio-profile "default" dot11g-radio-profile "default" mesh-radio-profile "mr prof1" mesh-cluster-profile "mesh-2" priority 1	ap-group "mesh grp2-MeSh" dot11a-radio-profile "mr prof1_MeSh" dot11g-radio-profile "default" mesh-radio-profile "mr prof1" mesh-cluster-profile "mesh-2" priority 1

In the above example mesh cluster profile points to ‘a’ radio.

AP Name

If a mesh cluster profile or mesh radio profile is defined to override the group definitions for a specific AP, then the upgrade script will create or modify a dot11a/g profile similar to the rules as shown in the following example and create or modify the existing dot11 profiles.

Table 2 *Example of Old and New Mesh AP Name*

Old Name	New Name
ap-name "MP65-8" virtual-ap "MP65-8" dot11a-radio-profile "default" dot11g-radio-profile "default" mesh-radio-profile "mr prof1" !	ap-name "MP65-8" virtual-ap "MP65-8" dot11a-radio-profile "mr prof1_MeSh" dot11g-radio-profile "default" mesh-radio-profile "mr prof1"

If AP group of *MP65-8* mesh cluster profile points to 'a' radio, then the dot11a profile will be modified. After successfully upgrading the mesh network, enable the associated profiles.

NOTE

Assuming that the AP name MP65-8 points to mesh-cluster profile which has the 'a' band.

WebUI Changes for MRP and MCP

When you upgrade to AOS-W 3.4 from a 3.3.x release, you will notice change in the WebUI configuration screens for mesh radio profile (MRP). The following screenshots illustrates the differences in AOS-W 3.4 and an AOS-W 3.3.x release.

Figure 2 *Mesh Radio Profile Screen in AOS-W 3.3.x*

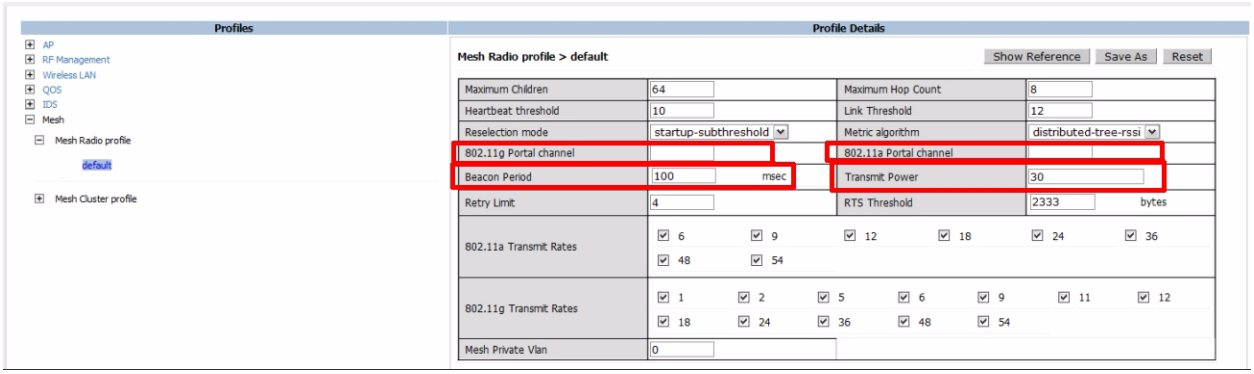


Figure 3 *Mesh Radio Profile Screen in AOS-W 3.4*

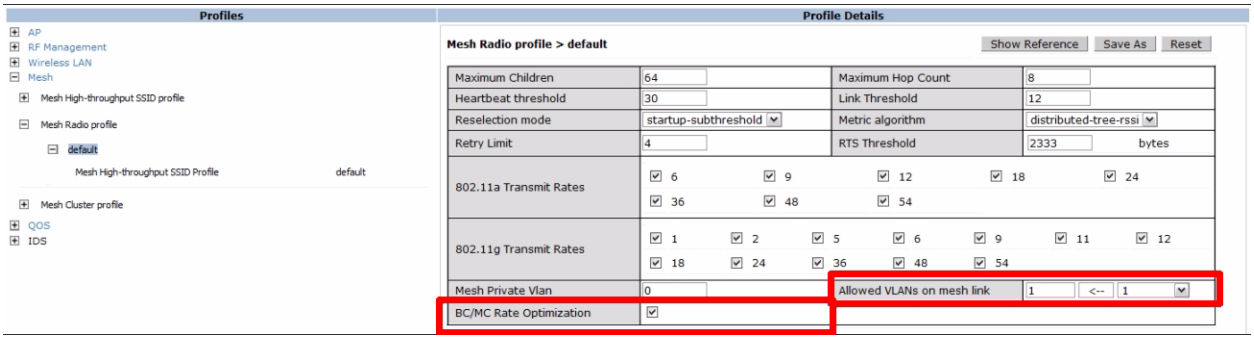


Table 3 *MRP Configuration Screen Changes*

Fields Deleted	Fields Added
• Fields Removed • 802.11g port channel • 802.11a port channel • Beacon Period • Transmit Power	• Allowed VLANs on mesh link • BC/MC Rate Optimizations

Auto provisioning

After the upgrade, every mesh AP from the GAP database is auto provisioned to new group.

Downgrade

If you downgrade from AOS-W 3.4 to AOS-W 3.3.x and retain the AOS-W 3.4 mesh configurations the mesh AP's will remain in the same groups.

Things to remember:

- Alcatel-Lucent recommends that the 3.3.x configuration be restored and mesh APs reprovisioned to the original AP groups.
- If the AOS-W 3.4 configuration is retained then the changed MRP parameters (dot11a/g portal channel, beacon-period and Tx power) should be reset appropriately.

The default transmit EIRP value on a mesh-radio in AOS-W 3.4 is 127, which is the maximum permitted value as per regulations.

Firewall

The `voip-proxy-arp` parameter in the firewall command is deprecated in AOS-W 3.3.2. This parameter is available as part of the `wlan virtual-ap <profile>` command. All previous usage of voip-proxy-arp parameter in the firewall command will be disabled after you upgrade to AOS-W 3.3.2.

Upgrading from 2.5.x

If you are upgrading from AOS-W 2.5.x or earlier release, you must first upgrade to Alcatel-Lucent 3.3.x version. You cannot directly upgrade to AOS-W 3.4 from 2.5.x or earlier release. See "Software Upgrade Path" on page 1 for more details.

Upgrading to 3.3.x

AOS-W 3.3.x releases provide a new framework for configuring Alcatel-Lucent access points (APs) that is different from AOS-W 2.5.x releases. This section describes configuration differences between AOS-W 2.5.x and 3.3.x releases:

In addition to the information described in this section, see "Upgrading from 3.3.x and Earlier Release" on page 9 for more 3.x configuration information.

AP Names and Groups

In AOS-W 2.5.x releases, APs were configured with location codes in the form *building.floor.location*. In AOS-W 3.3.x, each AP is given an AP name and an AP group:

- For APs that were provisioned in a previous AOS-W release, the AP name defaults to *building.floor.location*.
- For APs that were not previously configured, the AP name defaults to the Ethernet MAC address of the AP in the format *xx:xx:xx:xx:xx:xx*.

You can change the name of an AP. See “Configuring Access Points” in Volume 3 of the AOS-W *3.3.1 User Guide*.

- Unprovisioned APs and APs with 0.0.0 location IDs initially belong to the “default” AP group. You can create additional groups as necessary, however keep in mind that an AP can belong to only one AP group at a time. See “Configuring Access Points” in Volume 3 of the AOS-W *3.3.1 User Guide* for more information.

APs in RF Plan

In RF Plan or RF Live, the AP name can be part of a fully-qualified location name (FQLN) in the format *APname.floor.building.campus* (the *APname* portion of the FQLN must be unique).

Note the following about APs that were provisioned with location IDs when you upgrade from AOS-W 2.5.x to 3.3.x:

- If the AP location ID includes *building*, the FQLN for the AP is automatically set after the upgrade and the AP should appear on an existing campus or building plan.
- If the AP location ID does not include *building*, there is no FQLN set for the AP after the upgrade. You have to manually set the FQLN for the AP by clicking the AP FQLN Mapper button in RF Plan. After you set the FQLN, the AP should appear on an existing campus or building plan.

Configuration File Migration

When you boot the switch with AOS-W 3.3.x, the configuration file created in AOS-W 2.5.4 (or later) software is saved and automatically migrated to a new configuration file. During the migration, the following occurs:

- The "default" profiles are populated by global configuration parameters (for example, authentication) and AP configuration parameters for location 0.0.0.
- Wildcard configurations are used to create AP groups and profiles that are assigned to them. Location *building*.*floor*.0 configuration entries are used to create groups named "*building*.*floor*.0" with location *building*.0.0 configurations inherited appropriately. Location *building*.0.0 configuration entries are used to create groups named "*building*.0.0". Appropriate group settings are automatically programmed onto the corresponding APs.
- AP-specific configuration entries are used to create AP name-based configurations using the name "*building*.*floor*.*location*". If an SNMP hostname is specified in the AP configuration, that name is used instead and is automatically provisioned on the AP.

Example:

The following section is an example of a 2.5.x configuration and how the configuration will appear after the automatic migration:

Table 4 *Configuration before and after upgrading to 3.3.x*

Pre 3.3.x Configuration	After Automatic Upgrade

ap location 1.0.0
  ageout 700
  phy-type a
  channel 64
  !
!
 	
ap location 1.2.0
  lms-ip 10.3.4.5
!
 	
ap location 1.2.3
  rf-band a
!
	wlan ssid-profile 1.0.0
	  ageout 700
	!
	
	wlan virtual-ap 1.0.0
	  ssid-profile 1.0.0
	!
	
	rf radio-profile 1.0.0
	  a-channel 64
	!
	
	ap system-profile 1.2.0
	  lms-ip 10.3.4.5
	!
	
	ap system-profile 1.2.3
	  lms-ip 10.3.4.5
	  rf-band a
	!
	
	ap-group 1.0.0
	  virtual-ap 1.0.0
	  dot11a-radio-profile 1.0.0
	  dot11g-radio-profile 1.0.0
	!
	
	ap-group 1.2.0
	  virtual-ap 1.0.0
	  dot11a-radio-profile 1.0.0
	  dot11g-radio-profile 1.0.0
	  ap-system-profile 1.2.0
	!
	
	ap-name 1.2.3
	  ap-system-profile 1.2.3
	!

The automatic upgrade also causes all APs with location 1.2.x to be provisioned into group 1.2.0. All other APs with location 1.x.x are provisioned into group 1.0.0.

Mapping of Show Commands

The CLI command **show command-mapping** maps AOS-W 3.3.x to AOS-W 2.5.x commands, as shown in "Command Mapping" on page 18 (use the **reverse** option to display 2.5.x to 3.x command mapping):

Table 5 *Command Mapping*

New Command	Old Command
show ap active show ap arm neighbors show ap arm rf-summary show ap arm scan-times show ap arm state show ap association show ap blacklist-clients show ap bss-table show ap client status	show wlan ap show ap arm-neighbors show am rf-summary show am scan-times show wlan arm show stm association show wlan client show wlan remote-client show stm dos-sta show stm connectivity show stm state
show ap coverage-holes show ap database show ap debug association-failure show ap debug bss-config show ap debug bss-stats show ap debug client-mgmt-counters show ap debug client-stats show ap debug client-table	show rfsm coverage-holes show ap global-list show sapm ap search show ap registered show wlan association-failure show stm ap-config show ap detailed-stats show stm counters show ap detailed-stats show ap status
show ap debug counters show ap debug datapath show ap debug driver-log show ap debug log show ap debug mgmt-frames show ap debug radio-stats show ap debug received-config show ap debug system-status show ap debug trace-addr show ap essid	show sapm counters show stm hidden-essid show ap status show ap debug-log show stm packets show ap detailed-stats show ap received-config show ap status show stm trace-addr show wlan essid
show ap license-usage show ap load-balancing show ap monitor active-laser-beams show ap monitor ap-list show ap monitor arp-cache show ap monitor association show ap monitor channel show ap monitor client-list show ap monitor debug counters show ap monitor debug status	show wlan license-usage show rfsm load-balance show am active-laser-beams show am ap-search show am arp-cache show am association show am channel show am sta-search show am counters show am status

Table 5 *Command Mapping*

New Command	Old Command
show ap monitor ids-state show ap monitor pot-ap-list show ap monitor pot-client-list show ap monitor stats show ap monitor stats advanced show ap monitor wired-mac show ap pcap status show ap provisioning show ap remote association show ap remote bridge-table show ap remote counters show ap remote debug mgmt-frames show ap tech-support show ap vlan-usage provision-ap show provisioning-params	show am ids-state show am pot-ap-list show am pot-sta-list show am stats show am state show am wired-mac show pcap status NEW show stm ap association show ap bridge-table show stm ap counters show stm ap packets show ap-tech-support show wlan vlan-usage program-ap show ap-params

Command Changes

Removed Commands

The following AOS-W 2.5.x AP commands do not exist in 3.3.x:

Table 6 *Commands Removed in AOS-W 3.x*

Commands removed in 3.1	Use the following commands instead:
ap location	ap-group ap-name
show ap config location	show ap config ap-group show ap config ap-name show ap config bssid
show ap locations	show ap-group show ap-name
show ap node-config location	N/A
show enet1-config location	show ap enet-link-profile
show enet1-effective-config location	N/A
show ap snmp location	show ap snmp-profile show ap snmp-user-profile
show ap keys location	N/A
show firewall voip-proxy-arp	N/A

Replaced Commands

The following AOS-W 2.5.x commands are replaced with the new **show ap database** command:

- show ap global-list
- show ap registered
- show sapm ap search

Modified Commands

The **show log** command includes the following new options:

- ap-debug
- bssid-debug
- errorlog
- essid-debug
- network
- security
- system
- user
- user-debug
- wireless

The **show virtual-ap profile** includes the following new option:

- voip-proxy-arp

New Parameters for apboot Command

When issuing the **apboot** command, you can now specify the following additional parameters:

- **all** to reboot all APs connected to this switch. You can optionally specify **global** to reboot APs on all switches, or **local** to reboot APs registered on the switch on which you entered the **apboot** command.
- **ap-name** *name* to reboot the specified AP.

If you are rebooting an AP after changing its name, use the "old" name for the AP with the **apboot** command.

- **ap-group** *name* to reboot APs in the specified group. You can optionally specify **global** to reboot APs on all switches, or **local** to reboot APs registered on the switch on which you entered the **apboot** command.

If you are rebooting APs after assigning them to a new group, use the "old" AP group name.

Switch Country-Specific Code

In AOS-W 3.3.x, the country code is saved to the hardware and, for certain countries, cannot be changed. If you upgrade to this release in the United States or Israel, the switch is restricted to operate only in these countries.

The country code determines the 802.11 wireless transmission spectrum in which the switch operates. Most countries impose penalties and sanctions for operators of wireless networks with devices set to improper transmission spectrums.

Before upgrading to 3.3.x, make sure the correct country code is saved in the configuration file. Refer to the instructions described in “Installing AOS-W 3.4” on page 6.

Feature-Specific Differences

The AP-52 is not supported with the AOS-W 3.3.x release. Do not upgrade to AOS-W 3.3.x at this time if your network contains AP-52s.

Captive Portal

In AOS-W 2.5.2 and later 2.5.x releases, captive portal users in the base operating system are placed into the predefined *cpbase* initial user role before authentication. The *cpbase* role is not supported in AOS-W 3.3.x. You need to create captive portal authentication profiles in the base operating system, as described in “Configuring Captive Portal” in Volume 4 of the AOS-W *3.3.1 User Guide*. Creating a captive portal authentication profile automatically generates the required policies and role.

In 3.3.x, the captive portal authentication profile instance is configured for a user role. The user role can be the logon user role, a role that is configured for that SSID, or a role that is derived from user or server derivation rules. You must manually apply the captive portal authentication profile to a user role.

IP Mobility

There is no migration of AOS-W 2.5.x mobility features to mobility domain configuration; all previously-configured layer-3 mobility configuration will be lost.

Mobility is disabled by default on switches in 3.3.x. You must explicitly enable and configure mobility domains as described in “Configuring IP Mobility” in Volume 5 of the AOS-W *3.3.1 User Guide*.

Server Derivation Rules

In 3.3.x, you can configure server rules for a server group and not for individual servers. If you configured server rules for specific servers in 2.5.x releases, the server rules are automatically applied to all servers in the server group in 3.x.

User Roles and Policies

User role policies that reference specific location codes (*building.floor.location*) in 2.5.x releases must be manually re-configured for an AP group, since there is no automatic mapping of location IDs to an AP group.

MMS Configuration Management

AOS-W 3.3.x provides support in the switch for configuration management by the OmniVista Mobility Manager System (MMS) 2.0. Your switch must be running 3.1 or later, and your MMS server or MM-100 appliance must be running release 2.0 or later. MMS configuration management is not supported in pre-3.1 releases.

In AOS-W 3.x, you configure the IP address of the MMS server and an SNMP username and password for the MMS server to use to communicate with the master switch. The MMS configuration commands for 3.x are different from those in 2.5.x, however if you are upgrading an AOS-W 2.5.x switch to AOS-W 3.3.x, the MMS server configuration commands are automatically converted to the equivalent 3.3.x commands.

To support configuration by the MMS server, you must enable the master switch to receive, apply, and communicate the status of configuration changes with the MMS server (this is disabled by default).

For more information about configuring a master switch for MMS, see “OmniVista Mobility Manager” in “Configuring Management Access” in Volume 7 of the AOS-W *3.3.1 User Guide*.

Voice Services Module License

AOS-W 3.x supports the Voice Services Module license for many voice-related features. This license must be installed in the switch and is available for each Alcatel-Lucent switch model or supervisor card.

The following features available in 2.5.x now require the Voice Services Module license:

- Call admission control for SIP, SCCP, Vocera, SVP, and NOE
- Active VoIP load balancing and disconnect of excess calls options in the CAC profile
- Voice-aware ARM scanning
- Automatic assignment of voice traffic to high-priority queues without a PEF license.

When the PEF license is installed in the switch, you can permit/deny or assign queues for voice traffic in a session ACL even if the Voice Services Module license is not present.

See the *AOS-W 3.4 User Guide* for information about new features available with the Voice Services Module license.

Client Blacklisting

AOS-W 3.3.x allows you to enable automatic client blacklisting specifically for spoofed deauthentication, as seen with “man-in-the-middle” attacks; you enable this blacklisting in the IDS DoS profile. Automatic client blacklisting due to other reasons is enabled by default in the virtual AP profile. The virtual AP profile also allows you to configure both the amount of time that a client is blacklisted due to authentication failure and the amount of time that a client is blacklisted due to other reasons.

Adaptive Radio Management (ARM) and Calibration

Previous AOS-W releases support two methods for calibrating and managing radio settings for the wireless network: through Adaptive Radio Management (ARM) or through site survey calibration run on a per-building, per-ratio type basis. With the 3.x release, only ARM is supported.

For new installations, the Adaptive Radio Management (ARM) feature for single-band radio assignment is enabled by default. If you were running an earlier version of AOS-W with ARM disabled, ARM remains disabled when you upgrade to this release. If you were running radio calibration in a previous release, you now need to use ARM.

Predefined Management User Roles

With AOS-W 3.x, there are predefined roles that can be assigned to management users:

- root: superuser role
- guest-provisioning: allows for guest provisioning only
- read-only: allows execution of read-only commands
- location-api-mgmt: allows access to location API information only
- network operations: permits access to Monitoring, Reports, and Events pages in the WebUI

If you previously configured a management user with a user role that is not one of the above predefined roles, you need to reconfigure the management user to use one of the predefined roles. Use either the **Configuration > Management > Administration** page in the WebUI or the **mgmt-user** CLI command.

You can only define 10 management user roles in AOS-W 3.3.x.

Syslog Processor

With AOS-W 3.x, the ESI feature is expanded to support a more flexible message parser. If you previously used ESI to process messages from a Fortinet antivirus firewall device, you need to reconfigure the ESI rules for the expanded syslog processor capabilities:

1. Define the syslog processor domain. For example, in the following command, <ipaddr> is the IP address of the Fortinet syslog source:

```
esi parser domain fortinet
   server <ipaddr>
```

2. Define the syslog processor rule. For example:

```
esi parser rule forti_rule
    condition "log_id=[0-9]{10}[ ]"
   match ipaddr "src=(.*)[ ]"
   set blacklist
   domain fortinet
   enable
```

See the "External Services Interface" chapter in the AOS-W *3.3 .1User Guide* for more information.

Per-SSID RADIUS Server Selection

With 2.x releases, you can specify the "match ESSID" option when configuring RADIUS servers. This allows authentication server selection on a per-SSID basis. With AOS-W 3.x, you configure this function with profiles: configure the authentication server group, select the authentication server group in the AAA profile, then map the AAA profile to a virtual AP profile.

Reverting to AOS-W 3.3.x or Later

If necessary, you can to return to AOS-W 3.3.x or later software after upgrading to AOS-W 3.4.

When you upgrade to AOS-W 3.4, the upgrade script encrypts the internal DB. If you decide to downgrade, you must restore the saved copy of 3.3.x internal DB. Also, any new entries that were created in AOS-W 3.4 will be lost after downgrade.

Before you reboot the switch with pre-3.3.x software, you must perform the following steps:

1. Set the switch to boot with the previously-saved pre-3.3.x configuration file.
2. Set the switch to boot from the system partition that contains the pre-3.3.x 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 switch bootup. An error message displays if system boot parameters are set for incompatible image and configuration files.

After downgrading the software on the switch:

- Do not restore the flash file system from a AOS-W 3.4 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 AOS-W 3.4, the changes will not appear in RF Plan in the downgraded AOS-W version.
- If you installed any certificates while running AOS-W 3.4, you need to reinstall the certificates in the downgraded AOS-W version.

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

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

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

Using the WebUI

1. If the saved pre-3.3.x configuration file is on an external TFTP server, copy the file to the switch by navigating to the **Maintenance > File > Copy Files** page.
   a. For Source Selection, select TFTP server, and enter the IP address of the TFTP server and the name of the pre-3.3.x configuration file.
   b. For Destination Selection, enter a filename (other than default.cfg) for Flash File System.
2. Set the switch to boot with your pre-3.3.x configuration file by navigating to the **Maintenance > Switchs > Boot Parameters** page.
   a. Select the saved pre-3.3.x 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 > Switch > Image Management** page. If there is no previous software image stored on a system partition, load it into the backup system partition (you cannot load a new image into the active system partition):
   a. Enter the TFTP server address and image file name.
   b. Select the backup system partition.
   c. Click **Upgrade**.
4. Navigate to the **Maintenance > Switch > Boot Parameters** page.
   a. Select the system partition that contains the pre-3.3.x image file as the boot partition.
   b. Click **Apply**.
5. Navigate to the **Maintenance > Switch > Reboot Switch** page. Click **Continue**. The switch reboots after the countdown period.
6. When the boot process is complete, verify that the switch is using the correct software by navigating to the **Maintenance > Switch > Image Management** page.

Using the CLI

1. If the saved pre-3.3.x configuration file is on an external TFTP server, use the following command to copy it to the switch:

   ```
   copy tftp: <TFTP server IP address> <backup filename> flash: <backup configuration filename>
   ```

2. Set the switch to boot with your pre-3.3.x configuration file.

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

3. Determine the partition on which your previous software image is stored.

   Use the following command to check the memory partitions:

   ```
   #show image version
   ---------------------------------
   Partition               : 0:0 (/dev/hda1)
   Software Version        : AOS-W 3.3.1.0 (Digitally Signed - Production Build)
   Build number            : 19148
   Label                   : 19148
   Built on                : 2008-08-10 04:26:35 PDT
   ```

```
--------------------------------
Partition               : 0:1 (/dev/hda2) **Default boot**
Software Version        : AOS-W 3.4.0.0 (Digitally Signed - Production Build)
Build number            : 21234
Label                   : 21234
Built on                : 2009-05-03 01:53:04 PDT
```

In this example, partition 0, the backup system partition, contains the release 3.3.1.0 backup. Partition 1, the active system partition, contains the AOS-W 3.4 image.

If a previous software image is not stored, load it into the backup system partition.


NOTE

You cannot load a new image into the active system partition

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

4. Set the backup system partition as the new boot partition:
   ```
   # boot system partition 0
   ```
5. Reboot the switch:
   ```
   # reload
   ```
6. When the boot process is complete, verify that the switch is using the correct software:
   ```
   # show version
   ```

Troubleshooting

If you have any issues with the switch, for example, insufficient disk, 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 Alcatel-Lucent switch with IP addresses and Interface numbers if possible).

   The diagram can be a Visio, PowerPoint, JPEG, TIF, etc. file, or it can even be hand written and faxed to support at 1-408-227-4550.
2. Provide the switch 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 server file of the switch at the time of the problem.

   Alcatel-Lucent strongly recommends that you consider adding a syslog server if you do not already have one to capture logs of the switch.
4. Let the support person taking your call 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 anything has recently changed in your network (external to the Alcatel-Lucent system) or if anything has recently been changed in the switch 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 switch site access information, if possible.

    Alcatel-Lucent recommends that access to your site should only be enabled when a problem occurs (or if Alcatel-Lucent 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 switch, or you limit access methods to analog dialup to the switch or SSH access to a device that the support person can then telnet to the switch.

Upgrade and Installation Checklist

The following checklist table is a quick reference to items that you must know before and during AOS-W 3.4 upgrade. You can take a printout of this table for handy purpose.

Table 7 *Upgrade and Installation Checklist*

Upgrade and Installation Checklist		
AOS-W 3.4 Release Notes	Download from Alcatel-Lucent Support web site.	
Migration Guide	Download from Alcatel-Lucent Support web site	
Quick Start Guide	Download from Alcatel-Lucent Support web site	
Direct upload to AOS-W 3.4 not supported. Upgrade to AOS-W 3.3.x first.		
Back up your data	See "Backing up Critical Data" on page 5.	
Back up your configuration.	See "Saving the Configuration" on page 8.	
Restore switch to factory defaults.	See "Restore the Switch to Factory Defaults and Reconfigure" on page 2.	
Keep the correct country code handy.		
Set up a system on your network to temporarily store the AOS-W 3.4 image.		
Alcatel-Lucent Support web site	https://service.esd.alcatel-lucent.com	
Alcatel-Lucent Support Phone Numbers		
North America	1-800-995-2696	
Latin America	1-877-919-9526	
Europe	+33 (0) 38 855 6929	
Asia Pacific	+65 6240 8484	
Worldwide	1-818-878-4507	

Contacting Alcatel-Lucent

Table 8 *Alcatel-Lucent Contacts*

Contact Center Online	
• Main Site	http://www.alcatel-lucent.com/enterprise
• Support Site	https://service.esd.alcatel-lucent.com
• Email	support@ind.alcatel.com
Service & Support Contact Center Telephone	
• North America	1-800-995-2696
• Latin America	1-877-919-9526
• Europe	+33 (0) 38 855 6929
• Asia Pacific	+65 6240 8484
• Worldwide	1-818-878-4507