AOS-W 3.3.2 Software Upgrade Guide

This document describes how to upgrade your WLAN switch to AOS-W Release 3.3.2:

NOTE: See the *AOS-W 3.3.2 Release Notes* for information about new features and fixed and known issues for this release.

CAUTION: Before upgrading to AOS-W 3.3.2, make sure the correct country code is saved in the configuration file. Refer to the instructions described in "Installing AOS-W 3.3.x" on page 23.

Migrating to 3.3.2 from 3.1.x and Earlier Releases

This section describes configuration differences between AOS-W 3.3.2 and previous releases, including 3.1.x releases.

NOTE: You must upgrade the WLAN switch image to AOS-W 2.5.4 or later *before* you upgrade the WLAN switch to AOS-W 3.3.2. Upgrading from an AOS-W release prior to 2.5.4 directly to 3.3.2 is not supported.

NOTE: In addition to the information described in this section, see "Migrating to 3.3.2 from 2.5.x" on page 5 for more 3.x configuration information.

Setup Wizard

The AOS-W 3.3.2 release introduces a browser-based Setup Wizard that steps you through the tasks of configuring the WLAN switch, installing software licenses, and configuring internal and/or external WLANs.

To access the Setup Wizard, your WLAN switch must be running AOS-W 3.3.2 in factory-default mode. If you want to use the Setup Wizard, do the following after upgrading your WLAN switch to AOS-W 3.3.2:

From the WebUI:

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

From the CLI, execute the following commands:

```
write erase
reload
```

NOTE: Do not issue the 'write erase all' command if you have previously installed a license in the WLAN 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 WLAN switch after upgrading to AOS-W 3.3.2, the previous configuration is automatically backed up. The AOS-W 3.3.2 configuration file is not compatible with previous AOS-W releases. If you need to downgrade from AOS-W 3.3.2 to an earlier release, you must set the WLAN switch to boot with the previously-saved pre-3.3.2 configuration file *before* you set the system partition that contains the pre-3.3.2 image file. An error message displays if you set system boot parameters for incompatible image and configuration files.

See "Reverting to AOS-W 2.5.4 or Later" on page 27 for instructions on downgrading from AOS-W 3.3.2.

Admin and Enable Passwords

When you upgrade a WLAN switch to AOS-W 3.3.2, the configuration is automatically converted to the 3.3.2 format, with the exception of the **admin** and **enable** passwords. To save the passwords in the proper 3.3.2 format, you must explicitly save the configuration using either the WebUI or CLI (see "Saving the Configuration" on page 26).

Captive Portal Certificate

In earlier AOS-W 3.1.x 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 WLAN switch). In AOS-W 3.3.2, all certificates are stored in the same location. When you upgrade the WLAN switch to AOS-W 3.3.2, the "default" certificate is replaced by the captive portal certificate used in the previous release.

NOTE: 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.

In AOS-W 3.3.2, 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.

NOTE: 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 as described above. Then select the certificate for captive portal.

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 3.3.2, any previously-configured bandwidth rate is applied to both upstream and downstream traffic for the user role.

Remote AP

When you upgrade an existing remote AP configuration to AOS-W 3.3.2, note the following guidelines:

- If you have an existing remote AP configuration with bridge SSIDs, create an initial role after upgrading to AOS-W 3.3.2 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 "Configuring Roles and Policies," in Volume 4 of the *AOS-W 3.3.1 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 3.3.2, 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 AOS-W 3.1.x, create two different AP groups before upgrading to AOS-W 3.3.2: 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 3.3.2. APs with a specific location code are automatically provisioned into a corresponding AP group. See "AP Names and Groups" on page 6.

  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 "Configuring Access Points," in Volume 3 of the *AOS-W 3.3.1 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 3.3.x. To ensure a successful upgrade, reduce the number of IP addresses in the L2TP pool before upgrading to AOS-W 3.3.2.

Mesh

Before upgrading a mesh network, you must disable (turn off) the virtual AP profile(s) and wired AP profile(s) associated with the mesh network.

To disable the Virtual AP and Wired AP profiles in the WebUI, deselect (uncheck) the Virtual AP enable checkbox in the Virtual AP Profile Details page and the Wired AP enable checkbox in the Wired AP Profile Details page.

To disable the virtual AP and Wired AP profiles using the CLI:

```
wlan virtual-ap <profile> no vap-enable
ap wired-ap-profile <profile> no wired-ap-enable
```

After successfully upgrading the mesh network, re-enable (turn on) the associated profiles.

To enable the Virtual AP and Wired AP profiles in the WebUI, select (check) the Virtual AP enable checkbox in the Virtual AP Profile Details page and the Wired AP enable checkbox in the Wired AP Profile Details page.

To enable the virtual AP and Wired AP profiles using the CLI:

```
wlan virtual-ap <profile> vap-enable
ap wired-ap-profile <profile> wired-ap-enable
```

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.

Migrating to 3.3.2 from 2.5.x

AOS-W 3.x releases provide a new framework for configuring OmniAccess 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.x releases:

- "AP Names and Groups" on page 6
- "Voice Services Module License" on page 14
- "Configuration File Migration" on page 6
- "Mapping of Show Commands" on page 9
- "Command Changes" on page 10
- "Feature-Specific Differences" on page 13

NOTE: In addition to the information described in this section, see "Migrating to 3.3.2 from 3.1.x and Earlier Releases" on page 2 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 of *building.floor.location*. In AOS-W 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*.

  NOTE: 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.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 need 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 WLAN switch with AOS-W 3.x, the configuration file created in AOS-W 2.5.4 (or later) software is saved, then 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:

Pre 3.x Configuration

```
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
!
```

After Automatic Migration

```
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 migration 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.x to AOS-W 2.5.x commands, as shown (use the **reverse** option to display 2.5.x to 3.x command mapping):

```
Command Map
-----------
New Command                         Old Command
-----------                         -----------
show ap active                      show wlan ap
show ap arm neighbors               show ap arm-neighbors
show ap arm rf-summary              show am rf-summary
show ap arm scan-times              show am scan-times
show ap arm state                   show wlan arm
show ap association                 show stm association
                                    show wlan client
                                    show wlan remote-client
show ap blacklist-clients           show stm dos-sta
show ap bss-table                   show stm connectivity
show ap client status               show stm state

show ap coverage-holes              show rfsm coverage-holes
show ap database                    show ap global-list
                                    show sapm ap search
                                    show ap registered
show ap debug association-failure   show wlan association-failure
show ap debug bss-config            show stm ap-config
show ap debug bss-stats             show ap detailed-stats
show ap debug client-mgmt-counters  show stm counters
show ap debug client-stats          show ap detailed-stats
show ap debug client-table          show ap status

show ap debug counters              show sapm counters
show ap debug datapath              show stm hidden-essid
show ap debug driver-log            show ap status
show ap debug log                   show ap debug-log
show ap debug mgmt-frames           show stm packets
show ap debug radio-stats           show ap detailed-stats
show ap debug received-config       show ap received-config
show ap debug system-status         show ap status
show ap debug trace-addr            show stm trace-addr
show ap essid                       show wlan essid
```

`show ap license-usage`	`show wlan license-usage`
`show ap load-balancing`	`show rfsm load-balance`
`show ap monitor active-laser-beams`	`show am active-laser-beams`
`show ap monitor ap-list`	`show am ap-search`
`show ap monitor arp-cache`	`show am arp-cache`
`show ap monitor association`	`show am association`
`show ap monitor channel`	`show am channel`
`show ap monitor client-list`	`show am sta-search`
`show ap monitor debug counters`	`show am counters`
`show ap monitor debug status`	`show am status`
`show ap monitor ids-state`	`show am ids-state`
`show ap monitor pot-ap-list`	`show am pot-ap-list`
`show ap monitor pot-client-list`	`show am pot-sta-list`
`show ap monitor stats`	`show am stats`
`show ap monitor stats advanced`	`show am state`
`show ap monitor wired-mac`	`show am wired-mac`
`show ap pcap status`	`show pcap status`
`show ap provisioning`	`NEW`
`show ap remote association`	`show stm ap association`
`show ap remote bridge-table`	`show ap bridge-table`
`show ap remote counters`	`show stm ap counters`
`show ap remote debug mgmt-frames`	`show stm ap packets`
`show ap tech-support`	`show ap-tech-support`
`show ap vlan-usage`	`show wlan vlan-usage`
`provision-ap`	`program-ap`
`show provisioning-params`	`show ap-params`

Command Changes

Removed Commands

The following AOS-W 2.5.x AP commands do not exist in 3.x:

TABLE II-1 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`

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

  NOTE: 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 WLAN switches, or **local** to reboot APs registered on the WLAN switch on which you entered the **apboot** command.

  NOTE: If you are rebooting APs after assigning them to a new group, use the “old” AP group name.

WLAN Switch Country-Specific Code

In AOS-W 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 WLAN switch is restricted to operating only in these countries.

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

NOTE: 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 3.3.x” on page 23.

Feature-Specific Differences

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.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.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 WLAN switches in 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.x, you 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 reconfigured for an AP group, since there is no automatic mapping of location IDs to an AP group.

OV-MM Configuration Management

AOS-W 3.x provides support in the WLAN switch for configuration management by the OmniVista Mobility Manager (OV-MM) 2.0. Your WLAN switch must be running 3.1 or later, and your OV-MM server or OV-MM appliance must be running release 2.0 or later. OV-MM configuration management is not supported in pre-3.1 releases.

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

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

For more information about configuring a master WLAN switch for OV-MM, 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 WLAN switch and is available for each OmniAccess WLAN 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

  NOTE: When the PEF license is installed in the WLAN 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 3.3.1 User Guide* for information about new features available with the Voice Services Module license.

Client Blacklisting

AOS-W 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.

NOTE: You can only define 10 management user roles in ArubaOS 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.

Before Upgrading

NOTE: Before upgrading your WLAN switch, review the configuration changes for AOS-W 3.3.x, as described in "Migrating to 3.3.2 from 3.1.x and Earlier Releases" on page 2 and "Migrating to 3.3.2 from 2.5.x" on page 5. Also, review the "Known Issues and Limitations" section in the *AOS-W 3.3.1 Release Notes* for upgrade issues.

Verify the Configured Country Code

With AOS-W 3.x, the country code is saved to the hardware and cannot be changed for certain countries. Before upgrading to 3.3.x, make sure the correct country code is saved in the WLAN 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 WLAN 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 2.5.4 or later installed on the WLAN switch before you upgrade to AOS-W 3.3.x.

If the country code is *incorrect*, disable master-local WLAN switch updates by either disconnecting the local WLAN switch link or increasing the heartbeat value to a large interval (for example, issue the CLI command **cfgm set heartbeat 100000**).

You have the following options to correct the country code before upgrading to AOS-W 3.3.x:

- Restore the WLAN switch to its factory defaults and perform a fresh manual configuration. This method is recommended for WLAN switches where there is a minimum amount of configuration required, for example, a local WLAN switch that downloads most of its configuration from a master WLAN 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 WLAN switch.

The following sections describe the steps for each option.

Restore the WLAN Switch to Factory Defaults and Reconfigure

Complete the following steps to modify the country code and perform a fresh configuration on the WLAN switch. After configuring the WLAN switch, proceed to the steps in "Upgrading to AOS-W 3.3.x" on page 21.

Using the WebUI

1. Backup the current configuration on the WLAN switch:

   A. Navigate to the **Maintenance** > **File** > **Backup Flash** page.

   B. Click **Create Backup** to back up the contents of the Compact Flash file system to the file flashbackup.tar.gz.

   C. Click **Copy Backup** to copy the file to an external server.

2. Disconnect the WLAN switch from the network.

3. Reset the WLAN switch. Navigate to the **Maintenance** > **Switch** > **Clear Config** page.

4. Click **Continue**.

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

5. Run the Initial Setup.

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

6. When the boot process is complete, verify the country code.

   If the country code is incorrect, contact Alcatel-Lucent customer support.

   If the country code is correct, reconnect the WLAN switch to the network and reconfigure the WLAN switch.

Using the CLI

1. Backup the current configuration, as described in "Backing up Critical Data" on page 22.

2. Disconnect the WLAN switch from the network.

3. Reset and reboot the WLAN 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 WLAN switch to its factory defaults and reboots it with the default IP address 172.16.0.254.

4. Run the Initial Setup.

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

5. When the boot process is complete, verify the country code.

   If the country code is incorrect, contact Alcatel-Lucent Customer Support.

   If the country code is correct, reconnect the WLAN switch to the network and reconfigure the WLAN 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 then restore to the WLAN switch. After you restore the Compact Flash file system, proceed to the instructions in “Upgrading to AOS-W 3.3.x” on page 21.

Using the WebUI

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 the flashbackup.tar.gz file:

1. Enter **enable** mode in the CLI on the WLAN 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:

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

Upgrading to AOS-W 3.3.x

If you are currently running AOS-W 2.4.x on your WLAN switch, you must upgrade the WLAN switch image to AOS-W 2.5.4 or later *before* you upgrade the WLAN switch to AOS-W 3.3.x. Upgrading from 2.4.x directly to 3.3.x is not supported.

Before upgrading to AOS-W 3.3.x 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 17.

Depending on the size and complexity of your configuration, you may want to start over with a fresh configuration when upgrading to 3.3.x, rather than migrating your existing configuration. Contact Alcatel-Lucent Customer Support for assistance.

NOTE: After the upgraded WLAN switch boots up with AOS-W 3.3.x, save the configuration to save the **admin** and **enable** passwords in the proper format.

Managing Flash Memory

All OmniAccess WLAN 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 WLAN 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 WLAN 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.

CAUTION: 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 WLAN Switch.

Prerequisites

You should ensure the following before installing a new image on the WLAN 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 off the WLAN switch.

Backing up Critical Data

It is important to back up frequently 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 WLAN switch.

Using the WebUI

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 WLAN 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

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

1. Enter **enable** mode in the CLI on the WLAN 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 3.3.x

CAUTION When upgrading the software in a multi-WLAN switch network (one that uses two or more WLAN switches), special care must be taken to upgrade all the WLAN switches in the network and to upgrade them in the proper sequence. (See "Upgrading Multi-WLAN Switch Networks" on page 27.)

Obtain the latest, valid WLAN switch software image from the Alcatel-Lucent Customer Support website. Back up your current WLAN switch configuration and data files, as described in "Backing up Critical Data" on page 22.

Alcatel-Lucent recommends scheduling network downtime when upgrading your WLAN switches to AOS-W 3.3.2.

NOTE: The most current WLAN 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.

Using the WebUI

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 WLAN 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.
4. Select the Upload Local File option, then click the **Browse** button to navigate to the image file on your PC or workstation.
5. 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).
6. Select **Yes** for Reboot Switch After Upgrade.
7. Click **Upgrade**.
8. When the software image is uploaded to the WLAN switch, a popup appears. Click **OK** in the popup window. The boot process starts automatically within a few seconds (unless you cancel it).
9. 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 WLAN switch.

Using the CLI

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

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

2. From the CLI on the WLAN switch, verify the network connection from the target WLAN switch to the TFTP server:

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

NOTE A valid IP route must exist between the TFTP server and the WLAN 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:

```
(host) # show image version
----------------------------------
Partition               : 0:0 (/dev/hda1) **Default boot**
Software Version        : AOS-W 2.5.4.1
Build number            : 13515
Label                   : 13515
Built on                : 2006-10-24 13:22:04 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 WLAN switch:

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

NOTE When using the **copy** command to load a software image, the specified partition automatically becomes active the next time the WLAN 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 WLAN switch:

```
(host) # reload
```

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

```
(host) #show version
Alcatel Operating System-Wireless.
AOS-W (MODEL: OAW-4324-US), Version 3.3.2
Website: http://www.alcatel.com/enterprise
All Rights Reserved (c) 2005-2008, Alcatel.
Compiled on 2008-01-21 at 04:23:10 PST (build 17420) by p4build

ROM: System Bootstrap, Version CPBoot 1.0.8 (Oct 10 2003 - 11:59:29)

Switch uptime is 3 days 4 hours 56 minutes 33 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.
128M bytes of Supervisor Card System flash (model=128MB CHH).
(host) #
```

In this example, version 3.3.2 is loaded and running, indicating that the upgrade is complete.

Saving the Configuration

After the WLAN switch has booted up with AOS-W 3.3.x, 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:

```
write memory
```

Upgrading Multi-WLAN Switch Networks

In a multi-WLAN switch network (a network with two or more WLAN switches), special care must be taken to upgrade all WLAN switches in the proper sequence, based on the WLAN switch type (master or local). Be sure to back up all WLAN switches being upgraded, as described in "Before Upgrading" on page 17.

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

To upgrade an existing multi-WLAN switch system to AOS-W 3.3.x:

1. Load the software image onto all WLAN switches (including redundant master WLAN switches).
2. If all the WLAN Switch cannot be loaded with the same software image and reloaded simultaneously, use the following guidelines:

   A. Remove the link between the master & local WLAN Switch.

   B. Load the software image and reload the master & local WLAN Switch separately at a time of your preference.

   C. Make sure that the master & all local WLAN Switch are upgraded properly.

Reverting to AOS-W 2.5.4 or Later

If necessary, you can to return to AOS-W 2.5.4 or later software after upgrading to AOS-W 3.3.x. Before you reboot the WLAN switch with pre-3.3.x software, you must perform the following steps:

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

   NOTE: 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 WLAN switch bootup. An error message displays if system boot parameters are set for incompatible image and configuration files.

After downgrading the software on the WLAN switch:

- Do not restore the flash file system from a 3.3.x 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 3.3.x, the changes will not appear in RF Plan in the downgraded AOS-W version.
- If you installed any certificates while running 3.3.x, 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 WLAN switch.

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

CAUTION When reverting the WLAN 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 WLAN 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 WLAN switch to boot with your pre-3.3.x configuration file by navigating to the **Maintenance > Switch > 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 WLAN switch reboots after the countdown period.

6. When the boot process is complete, verify that the WLAN 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 WLAN switch:

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

2. Set the WLAN 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:

```
(host) #show image ver
----------------------------------
Partition               : 0:0 (/dev/hda1)
Software Version        : AOS-W 2.5.4.1
Build number            : 13515
Label                   : 13515
Built on                : 2006-10-24 13:22:04 PDT
----------------------------------
Partition               : 0:1 (/dev/hda2) **Default boot**
Software Version        : AOS-W 3.3.2
Build number            : 17420
Label                   : 17420
Built on                : 2008-01-21 04:23:10 PST
```

   In this example, partition 0, the backup system partition, contains the release 2.5.4.1 backup. Partition 1, the active system partition, contains the AOS-W 3.3.x image.

   If there is no previous software image stored, load it into the backup system partition (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|1}
```

5. Reboot the WLAN switch:

```
# reload
```

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

```
# show version
```

Troubleshooting

If there is trouble with the WLAN switch (for example, there is less than 10 MB of flash space), do the following:

1. Disconnect the link to the APs.
2. Remove all unnecessary files from flash, including the db_dump.sql type files.
3. Remove any crash files.
4. Import the old wms DB file and reboot.
5. Reconnect the link for the APs.

Before You Call Technical Support

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

1. Provide a detailed network topology (including all the devices in the network between the user and the WLAN 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 handwritten and faxed to support.

2. Provide the WLAN 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 WLAN 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 WLAN 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 OmniAccess system) or if anything has recently been changed in the WLAN 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 WLAN 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 WLAN switch, or you limit access methods to analog dialup to the WLAN switch or SSH access to a device that the support person can then telnet to the WLAN switch.

Contacting Alcatel-Lucent

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

Copyright

Specifications in this manual are subject to change without notice.

Originated in the USA.

Trademarks

AOS-W, Alcatel 4308, Alcatel 4324, Alcatel 6000, Alcatel 41, Alcatel 60/61/65, Alcatel 70, and Alcatel 80 are trademarks of Alcatel-Lucent in the United States and certain other countries.

Any other trademarks appearing in this manual are the property of their respective companies.

Legal Notice

The use of Alcatel-Lucent switching platforms and software, by all individuals or corporations, to terminate Cisco or Nortel VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Alcatel-Lucent from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of Cisco Systems or Nortel Networks.