

# AOS-W 6.3.1.25

Alcatel·Lucent   
Enterprise

Release Notes

## **Copyright Information**

Alcatel-Lucent and the Alcatel-Lucent Enterprise logo are trademarks of Alcatel-Lucent. To view other trademarks used by affiliated companies of ALE Holding, visit:

[enterprise.alcatel-lucent.com/trademarks](http://enterprise.alcatel-lucent.com/trademarks)

All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. (2017)

## **Open Source Code**

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses.

---

<b>Contents</b> .....	<b>3</b>
Revision History .....	4
<b>Release Overview</b> .....	<b>5</b>
Contents Overview .....	5
Important Points to Remember .....	5
Supported Browsers .....	7
Contacting Support .....	7
<b>New Features</b> .....	<b>8</b>
<b>Regulatory Updates</b> .....	<b>9</b>
<b>Resolved Issues</b> .....	<b>10</b>
<b>Known Issues and Limitations</b> .....	<b>11</b>
<b>Upgrade Procedures</b> .....	<b>12</b>
Upgrade Caveats .....	12
Important Points to Remember and Best Practices .....	13
Memory Requirements .....	14
Backing up Critical Data .....	14
Upgrading in a Multi-Switch Network .....	15
Upgrading to 6.3.x .....	16
Installing the FIPS Version of AOS-W 6.3.1.x .....	19
Downgrading .....	20
Before You Call Technical Support .....	22
<b>Acronyms and Abbreviations</b> .....	<b>23</b>

## Revision History

The following table lists the revision history of this document.

**Table 1:** *Revision History*

Revision	Change Description
Revision 01	Initial release.
Revision 02	Added the CVE numbers of the vulnerabilities resolved in this release.

AOS-W 6.3.1.25 is a software patch release that includes new feature enhancements and fixes to the issues identified in previous AOS-W releases.



---

See the [Upgrade Procedures on page 12](#) for instructions on how to upgrade your switch to this release.

---

## Contents Overview

- [New Features on page 8](#) provides a description of features and enhancements introduced in this release of AOS-W.
- [Regulatory Updates on page 9](#) describes the regulatory updates in this release of AOS-W.
- [Resolved Issues on page 10](#) describes the issues resolved in this release of AOS-W.
- [Known Issues and Limitations on page 11](#) describes the known and outstanding issues identified in this release of AOS-W.
- [Upgrade Procedures on page 12](#) describes the procedures for upgrading a switch to this release of AOS-W.



---

For information regarding prior releases, refer to the corresponding Release Notes on <https://service.esd.alcatel-lucent.com/>.

---

## Important Points to Remember

If you modify the configuration of an Access Point (AP), those changes take effect immediately; you do not need to reboot the switch or the AP for the changes to affect the current running configuration. Certain commands, however, automatically force the AP radio to restart.

### AP Settings Triggering a Radio Restart

Changing the following settings triggers the radio to restart on the OAW-AP220 Series access points. When the radio restarts, wireless services will be briefly interrupted. Clients will automatically reconnect to the network when the radio is up and running.

**Table 2:** Profile Settings in AOS-W 6.3.x

Profile	Description
802.11a/802.11g Radio Profile	<ul style="list-style-type: none"><li>● Channel</li><li>● CSA Count</li><li>● High throughput enable (radio)</li><li>● Very high throughput enable (radio)</li><li>● TurboQAM enable</li><li>● Maximum distance (outdoor mesh setting)</li><li>● Transmit EIRP</li><li>● Advertise 802.11h Capabilities</li><li>● Beacon Period/Beacon Regulate</li><li>● Advertise 802.11d Capabilities</li></ul>
Virtual AP Profile	<ul style="list-style-type: none"><li>● Virtual AP enable</li><li>● Forward Mode</li><li>● Remote-AP operation</li></ul>
SSID Profile	<ul style="list-style-type: none"><li>● ESSID</li><li>● Encryption</li><li>● Enable Management Frame Protection</li><li>● Require Management Frame Protection</li><li>● Multiple Tx Replay Counters</li><li>● Strict Spectralink Voice Protocol (SVP)</li><li>● Wireless Multimedia (WMM) settings<ul style="list-style-type: none"><li>■ Wireless Multimedia (WMM)</li><li>■ Wireless Multimedia U-APSD (WMM-UAPSD) Powersave</li><li>■ WMM TSPEC Min Inactivity Interval</li><li>■ Override DSCP mappings for WMM clients</li><li>■ DSCP mapping for WMM voice AC</li><li>■ DSCP mapping for WMM video AC</li><li>■ DSCP mapping for WMM best-effort AC</li><li>■ DSCP mapping for WMM background AC</li></ul></li></ul>
High-throughput SSID Profile	<ul style="list-style-type: none"><li>● High throughput enable (SSID)</li><li>● 40 MHz channel usage</li><li>● Very High throughput enable (SSID)</li><li>● 80 MHz channel usage (VHT)</li></ul>
802.11r Profile	<ul style="list-style-type: none"><li>● Advertise 802.11r Capability</li><li>● 802.11r Mobility Domain ID</li><li>● 802.11r R1 Key Duration</li><li>● key-assignment (CLI only)</li></ul>
Hotspot 2.0 Profile	<ul style="list-style-type: none"><li>● Advertise Hotspot 2.0 Capability</li><li>● RADIUS Chargeable User Identity (RFC4372)</li><li>● RADIUS Location Data (RFC5580)</li></ul>

## Supported Browsers

The following browsers are officially supported to use with the AOS-W 6.3.1.25 Web User Interface (WebUI):

- Microsoft Internet Explorer 10.x and 11.0 on Windows 7 and Windows 8
- Mozilla Firefox 23 or higher on Windows Vista, Windows 7, and Mac OS
- Apple Safari 5.1.7 or later on Mac OS

## Contacting Support

**Table 3:** *Contact Information*

Contact Center Online	
Main Site	<a href="http://enterprise.alcatel-lucent.com">http://enterprise.alcatel-lucent.com</a>
Support Site	<a href="https://support.esd.alcatel-lucent.com">https://support.esd.alcatel-lucent.com</a>
Email	<a href="mailto:ebg_global_supportcenter@al-enterprise.com">ebg_global_supportcenter@al-enterprise.com</a>
Service & Support Contact Center Telephone	
North America	1-800-995-2696
Latin America	1-877-919-9526
EMEA	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507

There are no new features in this release of AOS-W.



The following default Downloadable Regulatory Table (DRT) version is part of AOS-W 6.3.1.25:

- DRT-1.0\_61690

For a complete list of countries certified with different AP models, refer to the DRT Release Notes at [support.esd.alcatel-lucent.com](http://support.esd.alcatel-lucent.com).



---

This software release supports the channel requirements described in *ALE Support Advisory SA-N0033*, available for download from the [support.esd.alcatel-lucent.com](http://support.esd.alcatel-lucent.com) site.

---



---

Contact your local sales representative about device availability and support for your country.

---

This release includes fixes for vulnerability documented in:

- WPA2 Key Reinstallation Vulnerabilities (CVE-2017-13077) - [CVE-2017-13077](#), [CVE-2017-13078](#), [CVE-2017-13079](#), [CVE-2017-13080](#), [CVE-2017-13081](#), [CVE-2017-13082](#), [CVE-2017-13084](#), [CVE-2017-13086](#), [CVE-2017-13087](#), and [CVE-2017-13088](#)
- ArubaOS Multiple Vulnerabilities - [CVE-2017-9000](#) and [CVE-2017-9003](#)
- Multiple Vulnerabilities in 'dnsmasq' - [CVE-2017-14491](#), [CVE-2017-14492](#), [CVE-2017-14493](#), [CVE-2017-14494](#), [CVE-2017-14495](#), and [CVE-2017-14496](#)

There are no new known and outstanding issues identified in this release of AOS-W.

This chapter details the software upgrade procedures. It is recommended that you schedule a maintenance window for upgrading your switches.



---

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

---

Topics in this chapter include:

- [Upgrade Caveats on page 12](#)
- [Important Points to Remember and Best Practices on page 13](#)
- [Memory Requirements on page 14](#)
- [Backing up Critical Data on page 14](#)
- [Upgrading in a Multi-Switch Network on page 15](#)
- [Upgrading to 6.3.x on page 16](#)
- [Installing the FIPS Version of AOS-W 6.3.1.x](#)
- [Downgrading on page 20](#)
- [Before You Call Technical Support on page 22](#)

## Upgrade Caveats

- AOS-W 6.3.1 is not recommended for customers with OAW-AP120 Series access points that routinely see over 85 clients associated to an AP. Please contact support if you have any questions.
- Beginning from AOS-W 6.3.1, the local file upgrade option in the OAW-4306 Series switch WebUI has been disabled.
- The local file upgrade option in the OAW-4x50 Series switch WebUI does not work when upgrading from AOS-W 6.2 or later. When this option is used, the switch displays the error message “Content Length exceed limit” and the upgrade fails. All other upgrade options work as expected.
- AirGroup
  - Starting from AOS-W 6.3, AirGroup is enabled by default. Upgrading the access switch from any version of AOS-W to AOS-W 6.3 converts the access switch to integrated mode switch. To continue to be in overlay mode, you must disable AirGroup on the access switch running AOS-W 6.3.
  - If you migrate from an overlay mode to an integrated mode, you must remove the already configured redirect ACLs from the user roles, and remove the L2 GRE tunnel from the access switch. It is recommended that you remove the overlay switch from the network or disable AirGroup on it.
- AOS-W 6.3 does not allow you to create redundant firewall rules in a single ACL. AOS-W considers a rule redundant if the primary keys are the same. The primary key is made up of the following variables:
  - source IP/alias
  - destination IP/alias
  - proto-port/service

If you are upgrading from AOS-W 6.1 or earlier versions and your configuration contains an ACL with redundant firewall rules, upon upgrading, only the last rule remains.

For example, in the following ACL, both ACE entries could not be configured in AOS-W 6.3. When a second ACE entry is done, it overwrites the first.

```
(host) (config) #ip access-list session allowall-laptop
(host) (config-sess-allowall-laptop)# any any any permit time-range test_range
(host) (config-sess-allowall-laptop)# any any any deny
(host) (config-sess-allowall-laptop)#end
(host) #show ip access-list allowall-laptop

ip access-list session allowall-laptop
allowall-laptop
-----
Priority  Source  Destination  Service  Action  TimeRange
-----  -
1         any     any          any      deny
```

- When upgrading the software in a multi switch network (one that uses two or more switches), special care must be taken to upgrade all the switches in the network and to upgrade them in the proper sequence. (See [Upgrading in a Multi-Switch Network on page 15.](#))
- RFPlan and RFLocate are deprecated on the switch. Use VisualRF Plan or VisualRF in OV3600 as replacements for RFPlan and RFLocate. VisualRF adds significant features including 802.11ac support, simplified work flows, and improved accuracy. If you are currently running RFPlan or RFLocate, contact your system engineer before upgrading. The upgrade removes these features from the switch.

## Important Points to Remember and Best Practices

Ensure a successful upgrade and optimize your upgrade procedure by taking the recommended actions provided in the following list. You should save this list for future use.

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any other changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network, during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of your network by answering the following questions:
  - How many APs are assigned to each switch? Verify this information by navigating to the **Monitoring > Network > All Access Points** section of the WebUI, or by executing the **show ap active** and **show ap database** CLI commands.
  - How are those APs discovering the switch (DNS, DHCP Option, Broadcast)?
  - What version of AOS-W is currently on the switch?
  - Are all switches in a master-local cluster running the same version of software?
  - Which services are used on the switches (employee wireless, guest access, remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load software images to the switch. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send 30 MB of data or more.
- In the Common Criteria evaluated configuration, software loading through SCP (secure copy) is the only supported option. Loading software through TFTP, FTP, or the WebUI 'Local File' option is not valid.
- Always upgrade the nonboot partition first. If problems occur during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the nonboot partition gives you a smoother downgrade path should it be required.
- Before you upgrade to the current AOS-W release, assess your software license requirements and load any new or expanded licenses you may require. For a detailed description of these new license modules, refer to the "Software Licenses" chapter in the *AOS-W 6.3.x User Guide*.

- The command **ip radius nas-ip** takes precedence over the command **per-server nas-ip**.

## Memory Requirements

All switches store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the switch. Loading multiple large files such as JPEG images for RF Plan can consume flash space quickly. To maintain the reliability of your WLAN network, it is recommended that the following compact memory best practices are followed:

- Execute the **show memory** command to confirm that there is at least 40 MB of free memory available for an upgrade using the CLI, or at least 60 MB of free memory available for an upgrade using the WebUI. Do not proceed unless this much free memory is available. To recover memory, reboot the switch. After the switch comes up, upgrade immediately.
- Execute the **show storage** command to confirm that there is at least 60 MB of flash space available for an upgrade using the CLI, or at least 75 MB of flash space available for an upgrade using the WebUI.



---

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

---

If the output of the **show storage** command indicates that there is insufficient flash memory space, you must free used memory. Any switch logs, crash data, or flash backups should be copied to a location off the switch, then deleted from the switch to free up flash space. You can delete the following files from the switch to free up memory before upgrading:

- **Crash Data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in [Backing up Critical Data on page 14](#) to copy the **crash.tar** file to an external server, and then execute the **tar clean crash** command to delete the file from the switch.
- **Flash Backups:** Use the procedures described in [Backing up Critical Data on page 14](#) to back up the flash directory to a file named **flash.tar.gz**, and then issue the **tar clean flash** command to delete the file from the switch.
- **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in [Backing up Critical Data on page 14](#) to copy the **logs.tar** file to an external server, and then execute the **tar clean logs** command to delete the file from the switch.

## 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 device. 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
- Custom captive portal pages
- x.509 certificates
- Switch Logs

## Back Up and Restore Compact Flash in the WebUI

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

1. Click the **Configuration** tab.
2. Click the **Save Configuration** button at the top of the page.
3. Navigate to the **Maintenance > File > Backup Flash** page.
4. Click **Create Backup** to back up the contents of the compact flash file system to the flashbackup.tar.gz file.
5. 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 using the file utility in the **Maintenance > File > Copy Files** page.
6. To restore the backup file to the compact flash file system, navigate to the **Maintenance > File > Restore Flash** page. Click **Restore**.

## Back Up and Restore Compact Flash in the CLI

The following steps describe the backup and restore procedure for the entire compact flash file system using the switch's command line:

1. Ensure you are in **enable** mode in the switch CLI, and execute the following command:  

```
(host) # write memory
```
2. Execute the **backup** command to back up the contents of the compact flash file system to the **flashbackup.tar.gz** file.

```
(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.
```

3. Use the **copy** command to transfer the backup flash file to an external server or storage device:

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

You can later transfer the backup flash file from the external server or storage device to the compact flash file system with the **copy** command:

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

4. Use the **restore** command to untar and extract the **flashbackup.tar.gz** file to the compact flash file system:  

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

## Upgrading in a Multi-Switch Network

In a multi-switch network (a network with two or more switches), special care must be taken to upgrade all switches based on the switch type (master or local). Be sure to back up all switches being upgraded, as described in [Backing up Critical Data on page 14](#).



---

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

---

To upgrade an existing multi-switch system to the current AOS-W release:

1. Load the software image onto all switches (including redundant master switches). The Master Switch should be rebooted and allowed ample time to boot up first. The Master Standby Switch should be rebooted next followed by the Local Switches.
2. In a Master - Local deployment, all switches need to be running the same AOS-W version. Switches in a Master - Local deployment do not support different AOS-W.
3. Verify that the Master, Master - Standby, and all Local switches are upgraded properly.

## Upgrading to 6.3.x

### Upgrading the OAW-4306 Series Switches to AOS-W 6.3.x

Customers upgrading the OAW-4306 Series switches must note the following:

- Ensure that memory and flash space requirements are met before starting the upgrade process. See [Memory Requirements on page 14](#) for details.
- User scalability on both the OAW-4306 switch and the OAW-4306G switch has been revised to 128 and 150 users, respectively.
- The following AOS-W 6.3.x features are not supported on the OAW-4306 Series switches.
  - AppRF
  - AirGroup
  - ClearPass Profiling with IF-MAP
  - IAP-VPN

### Install Using the WebUI



CAUTION

---

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash space available for an upgrade using the WebUI. For details, see [Memory Requirements on page 14](#).

---



NOTE

---

When you navigate to the **Configuration** tab of the switch's WebUI, the switch may display an error message **Error getting information: command is not supported on this platform**. This error occurs when you upgrade the switch from the WebUI and navigate to the **Configuration** tab as soon as the switch completes rebooting. This error is expected and disappears after clearing the Web browser cache.

---

### Upgrading From an Older AOS-W Version

Before you begin, verify the version of AOS-W currently running on your switch. If you are running one of the following versions of AOS-W, you must download and upgrade to an interim version of AOS-W before upgrading to the current AOS-W release.

- For switches running AOS-W 5.0.x versions earlier than AOS-W 5.0.3.1, download the latest version of AOS-W 5.0.4.x.
- For switches running AOS-W versions 6.0.0.0 or 6.0.0.1, download the latest version of AOS-W 6.0.1.x.

Follow step 2 to step 11 of the procedure described in [Upgrading From a Recent AOS-W Version](#) to install the interim version of AOS-W, and then repeat step 1 to step 11 of the procedure to download and install AOS-W 6.3.

### Upgrading From a Recent AOS-W Version

The following steps describe the procedure to upgrade from one of the following recent AOS-W versions:

- 6.0.1.0 or later



- 5.0.3.1 or later (If you are running AOS-W 5.0.3.1 or the latest 5.0.x.x, review [Upgrading With OAW-RAP5 and OAW-RAP5WN APs on page 17](#) before proceeding further.)
- 3.4.4.1 or later

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. Download the current AOS-W release from the customer support site.
2. Upload the new software image(s) to a PC or workstation on your network.
3. Validate the SHA hash for a software image:
  - a. Download the file **Alcatel.sha256** from the download directory.
  - b. To verify the image, load the image onto a Linux system and execute the **sha256sum <filename>** command or use a suitable tool for your operating system that can generate a **SHA256** hash of a file.
  - c. Verify if the output produced by this command matches the hash value found on the support site.



The AOS-W image file is digitally signed, and is verified using RSA2048 certificates preloaded onto the switch at the factory. Therefore, even if you do not manually verify the SHA hash of a software image, the switch does not load a corrupted image.

4. Log in to the AOS-W WebUI from the PC or workstation.
5. Navigate to the **Maintenance > Switch > Image Management** page. Select the **Upload Local File** option, then click **Browse** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. In the **partition to upgrade** field, select the non-boot partition.
8. In the **Reboot Switch After Upgrade** option field, the best practice is to select **Yes** to automatically reboot after upgrading. If you do not want the switch to reboot immediately, select **No**. Note however, that the upgrade does not take effect until you reboot the switch.
9. In **Save Current Configuration Before Reboot** field, select **Yes**.
10. Click **Upgrade**.
11. When the software image is uploaded to the switch, a popup window displays the message **Changes were written to flash successfully**. Click **OK**. If you chose to automatically reboot the switch in step 7, the reboot process starts automatically within a few seconds (unless you cancel it).
12. When the reboot process is complete, log in to the WebUI and navigate to the **Monitoring > Switch > Switch Summary** page to verify the upgrade.

When your upgrade is complete, perform the following steps to verify that the switch is functioning as expected.

1. Log in to the WebUI to verify all your switches are up after the reboot.
2. Navigate to **Monitoring > Network > Network Summary** to determine if your APs are up and ready to accept clients.
3. Verify that the number of access points and clients are what you expected.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See [Backing up Critical Data on page 14](#) for information on creating a backup.

### Upgrading With OAW-RAP5 and OAW-RAP5WN APs

If you have completed the first upgrade, hop to the latest version of AOS-W and your WLAN includes OAW-RAP5/OAW-RAP5WN APs. Do not proceed until you complete the following process. Once complete, proceed

to [step 5 on page 17](#). Note that this procedure can only be completed using the switch's command line interface.

1. Check the provisioning image version on your OAW-RAP5/OAW-RAP5WN APs by executing the **show ap image version** command.
2. If the flash (Provisioning/Backup) image version string shows the letters *m*, for example, 3.3.2.11-rn-3.0, note those AP names and IP addresses.
3. For each of the OAW-RAP5/OAW-RAP5WN APs noted in the step 2, upgrade the provisioning image on the backup flash partition by executing the following command:

```
apflash ap-name <Name_of_RAP> backup-partition
```

The OAW-RAP5/OAW-RAP5WN reboots to complete the provisioning image upgrade.

4. When all the OAW-RAP5/OAW-RAP5WN APs with a 3.3.2.x-based RN provisioning image have successfully upgraded, verify the provisioning image by executing the following command:

```
show ap image version
```

The flash (Provisioning/Backup) image version string should now show a version that does not contain the letters "rn", for example, 5.0.4.8.

If you skip the above process or fail to complete the flash (Provisioning/Backup) image upgrade to 5.0.4.x and the OAW-RAP5/OAW-RAP5WN was reset to factory defaults, the RAP cannot connect to a switch running AOS-W 6.3.1 and upgrade its production software image.

## Install Using the CLI



---

Confirm that there is at least 40 MB of free memory and at least 60 MB of flash space available for an upgrade using the CLI. For details, see [Memory Requirements on page 14](#).

---

### Upgrading From an Older AOS-W Version

Before you begin, verify the version of AOS-W currently running on your switch. If you are running one of the following versions of AOS-W, you must download and upgrade to an interim version of AOS-W before upgrading to the current AOS-W release.

- For AOS-W 3.x versions earlier than AOS-W 3.4.4.1, download the latest version of AOS-W 3.4.5.x.
- For AOS-W 3.x or AOS-W 5.0.x versions earlier than AOS-W 5.0.3.1, download the latest version of AOS-W 5.0.4.x.
- For AOS-W versions 6.0.0.0 or 6.0.0.1, download the latest version of AOS-W 6.0.1.x.

Follow step 2 - step 7 of the procedure described in [Upgrading from a Recent AOS-W Version](#) to install the interim version of AOS-W, and then repeat step 1 to step 7 of the procedure to download and install AOS-W 6.3.

### Upgrading from a Recent AOS-W Version

The following steps describe the procedure to upgrade from one of the following recent AOS-W versions:

- 6.0.1.0 or later
- 5.0.3.1 or later. (If you are running AOS-W 5.0.3.1 or the latest 5.0.x.x, review [Upgrading With OAW-RAP5 and OAW-RAP5WN APs on page 17](#) before proceeding further.)
- 3.4.4.1 or later

To install the AOS-W software image from a PC or workstation using the Command-Line Interface (CLI) on the switch:

1. Download the latest version of AOS-W from the customer support site.
2. Open a Secure Shell session (SSH) on your master (and local) switch(es).

- Execute the **ping** command to verify the network connection from the target switch to the SCP/FTP/TFTP server.

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

or

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

or

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

- Use the **show image version** command to check if the AOS-W images loaded on the switch's flash partitions. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.

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

- Use the **copy** command to load the new image onto the nonboot partition:

```
(host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition <0|1>
```

or

```
(host) # copy tftp: <tftphost> <image filename> system: partition <0|1>
```

or

```
(host) # copy scp: <scphost> <scpusername> <image filename> system: partition <0|1>
```

or

```
(host) # copy usb: partition <partition-number> <image filename> system: partition <0|1>
```



---

The USB option is only available on the OAW-4x50 Series switches.

---

- Execute the **show image version** command to verify that the new image is loaded.

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

- Reboot the switch.

```
(host) # reload
```

- Execute the **show version** command to verify that the upgrade is complete.

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

When your upgrade is complete, perform the following steps to verify that the switch is functioning as expected.

- Log in to the CLI to verify that all your switches are up after the reboot.
- Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
- Execute the **show ap database** command to verify that the number of access points and clients are what you would expect.
- Test a different type of client for each access method that you use, and in different locations when possible.
- Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See [Backing up Critical Data on page 14](#) for information on creating a backup.

## Installing the FIPS Version of AOS-W 6.3.1.x

Download the FIPS version of the software from <https://service.esd.alcatel-lucent.com>.

## Instructions on Installing FIPS Software

---



Before you install a FIPS version of the software on a switch that is currently running a non-FIPS version of the software, follow the procedure below. If you are currently running a FIPS version of the software on the switch, you do not have to perform a **write erase** to reset the configuration as mentioned in step 2.

---

Follow the steps below to install the FIPS software on a switch that is currently running a non-FIPS version of the software:

1. Install the FIPS version of the software on the switch.
2. Execute the **write erase** command to reset the configuration to the factory default; otherwise, you cannot log in to the switch using the CLI or WebUI.
3. Reboot the switch by executing the **reload** command.

This is the only supported method of moving from non-FIPS software to FIPS software.

## Downgrading

If necessary, you can return to your previous version of AOS-W.



If you upgraded from 3.3.x to 5.0, the upgrade script encrypts the internal database. New entries created in the current release are lost after the downgrade (this warning does not apply to upgrades from 3.4.x to 6.1).

---



If you do not downgrade to a previously-saved pre-6.1 configuration, some parts of your deployment may not work as they previously did. For example, when downgrading from AOS-W 6.3.1.0 to 5.0.3.2, changes made to WIPS in AOS-W 6.x prevents the new predefined IDS profile assigned to an AP group from being recognized by the older version of AOS-W. This unrecognized profile can prevent associated APs from coming up, and can trigger a profile error.

These new IDS profiles begin with *ids-transitional*, while older IDS profiles do not include *transitional*. If you think you have encountered this issue, use the **show profile-errors** and **show ap-group** commands to view the IDS profile associated with the AP Group.

---



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

---

## Before you Begin

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

1. Back up your switch. For details, see [Backing up Critical Data on page 14](#).
2. Verify that control plane security is disabled.
3. Set the switch to boot with the previously-saved pre-6.3 configuration file.
4. Set the switch to boot from the system partition that contains the previously running AOS-W image.  
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 used on the next switch reload. An error message displays if system boot parameters are set for incompatible image and configuration files.
5. After downgrading the software on the switch, perform the following steps:
  - Restore pre-6.3 flash backup from the file stored on the switch. Do not restore the AOS-W 6.3.1.0 flash backup file.

- If you installed any certificates while running AOS-W 6.3.1.0, you need to reinstall the certificates in the downgraded AOS-W version.

## Downgrading Using the WebUI

The following section describes how to use the WebUI to downgrade the software on the switch.

1. If the saved preupgrade configuration file is on an external FTP/TFTP server, copy the file to the switch by navigating to the **Maintenance > File > Copy Files** page.
  - a. For **Source Selection**, select FTP/TFTP server, and enter the IP address of the FTP/TFTP server and the name of the preupgrade 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 preupgrade configuration file by navigating to the **Maintenance > Switch > Boot Parameters** page.
  - a. Select the saved preupgrade 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 your system partition, load it into the backup system partition (you cannot load a new image into the active system partition).
  - a. Enter the FTP/TFTP server address and image file name.
  - b. Select the backup system partition.
  - c. Click **Upgrade**.
4. Navigate to the **Maintenance > Switch > Boot Parameters** page.
  - a. Select the system partition that contains the preupgrade 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.

## Downgrading Using the CLI

The following section describes how to use the CLI to downgrade the software on the switch.

1. If the saved preupgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the switch:

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

2. Set the switch to boot with your preupgrade configuration file.

```
(host)# boot config-file <backup configuration filename>
```

3. Execute the **show image version** command to view the partition on which your previous software image is stored. You cannot load a new image into the active system partition (the default boot).

In the following example, partition 0, the backup system partition, contains the backup release AOS-W 6.1.3.5. Partition 1, the default boot partition, contains the AOS-W 6.3.1.6 image.

```
(host)#show image version
-----
Partition           : 0:0 (/dev/hda2)
Software Version    : AOS-W 6.3.1.6(Digitally Signed - Production Build)
Build number        : 43088
Label               : 43088
```

```
Built on           : Mon Apr 07 16:46:24 2014
-----
Partition         : 0:1 (/dev/hda2)**Default boot**
Software Version  : AOS-W 6.1.3.6(Digitally Signed - Production Build)
Build number      : 43301
Label            : 43301
Built on         : Friday Apr 18 20:41:12 2014
```

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

```
(host)# boot system partition 0
```

5. Reboot the switch.

```
(host)# reload
```

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

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

## Before You Call Technical Support

Before you place a call to Technical Support, 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).
2. 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.
3. 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**).
4. Provide the syslog file of the switch at the time of the problem. It is strongly recommended that you consider adding a syslog server if you do not already have one to capture logs from the switch.
5. Let the support person know if this is a new or existing installation. This helps the support team to determine the troubleshooting approach, depending on whether you have an outage in a network that worked in the past, a network configuration that has never worked, or a brand new installation.
6. Let the support person know if there are any recent changes in your network (external to the Alcatel-Lucent switch) or any recent changes to your switch and/or AP configuration. 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. If the problem is reproducible, list the exact steps taken to re-create the problem.
8. Provide any wired or wireless sniffer traces taken during the time of the problem.
9. Provide the switch site access information, if possible.

The following table lists the acronyms and abbreviations used in Aruba documents.

**Table 4:** *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
3G	Third Generation of Wireless Mobile Telecommunications Technology
4G	Fourth Generation of Wireless Mobile Telecommunications Technology
AAA	Authentication, Authorization, and Accounting
ABR	Area Border Router
AC	Access Category
ACC	Advanced Cellular Coexistence
ACE	Access Control Entry
ACI	Adjacent Channel interference
ACL	Access Control List
AD	Active Directory
ADO	Active X Data Objects
ADP	Aruba Discovery Protocol
AES	Advanced Encryption Standard
AIFSN	Arbitrary Inter-frame Space Number
ALE	Analytics and Location Engine
ALG	Application Layer Gateway
AM	Air Monitor
AMON	Advanced Monitoring
AMP	AirWave Management Platform
A-MPDU	Aggregate MAC Protocol Data Unit
A-MSDU	Aggregate MAC Service Data Unit
ANQP	Access Network Query Protocol
ANSI	American National Standards Institute

**Table 4:** *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
AP	Access Point
API	Application Programming Interface
ARM	Adaptive Radio Management
ARP	Address Resolution Protocol
AVF	AntiVirus Firewall
BCMC	Broadcast-Multicast
BGP	Border Gateway protocol
BLE	Bluetooth Low Energy
BMC	Beacon Management Console
BPDU	Bridge Protocol Data Unit
BRAS	Broadband Remote Access Server
BRE	Basic Regular Expression
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CA	Certification Authority
CAC	Call Admission Control
CALEA	Communications Assistance for Law Enforcement Act
CAP	Campus AP
CCA	Clear Channel Assessment
CDP	Cisco Discovery Protocol
CDR	Call Detail Records
CEF	Common Event Format
CGI	Common Gateway Interface
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CLI	Command-Line Interface



**Table 4:** *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
CN	Common Name
CoA	Change of Authorization
CoS	Class of Service
CPE	Customer Premises Equipment
CPsec	Control Plane Security
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSA	Channel Switch Announcement
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CSR	Certificate Signing Request
CSV	Comma Separated Values
CTS	Clear to Send
CW	Contention Window
DAS	Distributed Antenna System
dB	Decibel
dBm	Decibel Milliwatt
DCB	Data Center Bridging
DCE	Data Communication Equipment
DCF	Distributed Coordination Function
DDMO	Distributed Dynamic Multicast Optimization
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection
DFT	Discreet Fourier Transform
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DMO	Dynamic Multicast optimization

**Table 4:** *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
DN	Distinguished Name
DNS	Domain Name System
DOCSIS	Data over Cable Service Interface Specification
DoS	Denial of Service
DPD	Dead Peer Detection
DPI	Deep Packet Inspection
DR	Designated Router
DRT	Downloadable Regulatory Table
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DSSS	Direct Sequence Spread Spectrum
DST	Daylight Saving Time
DTE	Data Terminal Equipment
DTIM	Delivery Traffic Indication Message
DTLS	Datagram Transport Layer Security
DU	Data Unit
EAP	Extensible Authentication Protocol
EAP-FAST	EAP-Flexible Authentication Secure Tunnel
EAP-GTC	EAP-Generic Token Card
EAP-MD5	EAP-Method Digest 5
EAP-MSCHAP EAP-MSCHAPv2	EAP-Microsoft Challenge Handshake Authentication Protocol
EAPoL	EAP over LAN
EAPoUDP	EAP over UDP
EAP-PEAP	EAP-Protected EAP
EAP-PWD	EAP-Password
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunneled Transport Layer Security

**Table 4:** *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
ECC	Elliptical Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EIGRP	Enhanced Interior Gateway Routing Protocol
EIRP	Effective Isotropic Radiated Power
EMM	Enterprise Mobility Management
ESI	External Services Interface
ESS	Extended Service Set
ESSID	Extended Service Set Identifier
EULA	End User License Agreement
FCC	Federal Communications Commission
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
FIB	Forwarding Information Base
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
FQLN	Fully Qualified Location Name
FRER	Frame Receive Error Rate
FRR	Frame Retry Rate
FSPL	Free Space Path Loss
FTP	File Transfer Protocol
GBps	Gigabytes per second
Gbps	Gigabits per second
GHz	Gigahertz
GIS	Generic Interface Specification
GMT	Greenwich Mean Time
GPP	Guest Provisioning Page
GPS	Global Positioning System

**Table 4:** *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
GVRP	GARP or Generic VLAN Registration Protocol
H2QP	Hotspot 2.0 Query Protocol
HA	High Availability
HMD	High Mobility Device
HSPA	High-Speed Packet Access
HT	High Throughput
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAS	Internet Authentication Service
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IDS	Intrusion Detection System
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
IKE PSK	Internet Key Exchange Pre-shared Key
IoT	Internet of Things
IP	Internet Protocol
IPM	Intelligent Power Monitoring
IPS	Intrusion Prevention System
IPsec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider

**Table 4:** *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
JSON	JavaScript Object Notation
KBps	Kilobytes per second
Kbps	Kilobits per second
L2TP	Layer-2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LDPC	Low-Density Parity-Check
LEA	Law Enforcement Agency
LEAP	Lightweight Extensible Authentication Protocol
LED	Light Emitting Diode
LEEF	Log Event Extended Format
LI	Lawful Interception
LLDP	Link Layer Discovery Protocol
LLDP-MED	LLDP-Media Endpoint Discovery
LMS	Local Management Switch
LNS	L2TP Network Server
LTE	Long Term Evolution
MAB	MAC Authentication Bypass
MAC	Media Access Control
MAM	Mobile Application Management
MBps	Megabytes per second
Mbps	Megabits per second
MCS	Modulation and Coding Scheme
MD5	Message Digest 5

**Table 4:** *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
MDM	Mobile Device Management
mDNS	Multicast Domain Name System
MFA	Multi-factor Authentication
MHz	Megahertz
MIB	Management Information Base
MIMO	Multiple-Input Multiple-Output
MLD	Multicast Listener Discovery
MPDU	MAC Protocol Data Unit
MPLS	Multiprotocol Label Switching
MPPE	Microsoft Point-to-Point Encryption
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSS	Maximum Segment Size
MSSID	Mesh Service Set Identifier
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
MU-MIMO	Multi-User Multiple-Input Multiple-Output
MVRP	Multiple VLAN Registration Protocol
NAC	Network Access Control
NAD	Network Access Device
NAK	Negative Acknowledgment Code
NAP	Network Access Protection
NAS	Network Access Server Network-attached Storage
NAT	Network Address Translation
NetBIOS	Network Basic Input/Output System
NIC	Network Interface Card
Nmap	Network Mapper
NMI	Non-Maskable Interrupt

**Table 4:** *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
NMS	Network Management Server
NOE	New Office Environment
NTP	Network Time Protocol
OAuth	Open Authentication
OCSP	Online Certificate Status Protocol
OFA	OpenFlow Agent
OFDM	Orthogonal Frequency Division Multiplexing
OID	Object Identifier
OKC	Opportunistic Key Caching
OS	Operating System
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
OVA	Open Virtual Appliance
OVF	Open Virtualization Format
PAC	Protected Access Credential
PAP	Password Authentication Protocol
PAPI	Proprietary Access Protocol Interface
PCI	Peripheral Component Interconnect
PDU	Power Distribution Unit
PEAP	Protected Extensible Authentication Protocol
PEAP-GTC	Protected Extensible Authentication Protocol-Generic Token Card
PEF	Policy Enforcement Firewall
PFS	Perfect Forward Secrecy
PHB	Per-hop behavior
PIM	Protocol-Independent Multicast
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard

**Table 4:** *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PMK	Pairwise Master Key
PoE	Power over Ethernet
POST	Power On Self Test
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
PPTP	PPP Tunneling Protocol
PRNG	Pseudo-Random Number Generator
PSK	Pre-Shared Key
PSU	Power Supply Unit
PVST	Per VLAN Spanning Tree
QoS	Quality of Service
RA	Router Advertisement
RADAR	Radio Detection and Ranging
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RAP	Remote AP
RAPIDS	Rogue Access Point and Intrusion Detection System
RARP	Reverse ARP
REGEX	Regular Expression
REST	Representational State Transfer
RF	Radio Frequency
RFC	Request for Comments
RFID	Radio Frequency Identification
RIP	Routing Information Protocol
RRD	Round Robin Database



**Table 4:** *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
RSA	Rivest, Shamir, Adleman
RSSI	Received Signal Strength Indicator
RSTP	Rapid Spanning Tree Protocol
RTCP	RTP Control Protocol
RTLS	Real-Time Location Systems
RTP	Real-Time Transport Protocol
RTS	Request to Send
RTSP	Real Time Streaming Protocol
RVI	Routed VLAN Interface
RW RoW	Rest of World
SA	Security Association
SAML	Security Assertion Markup Language
SAN	Subject Alternative Name
SCB	Station Control Block
SCEP	Simple Certificate Enrollment Protocol
SCP	Secure Copy Protocol
SCSI	Small Computer System Interface
SDN	Software Defined Networking
SDR	Software-Defined Radio
SDU	Service Data Unit
SD-WAN	Software-Defined Wide Area Network
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SIRT	Security Incident Response Team

**Table 4:** *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
SKU	Stock Keeping Unit
SLAAC	Stateless Address Autoconfiguration
SMB	Small and Medium Business
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transport Protocol
SNIR	Signal-to-Noise-Plus-Interference Ratio
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio
SNTP	Simple Network Time Protocol
SOAP	Simple Object Access Protocol
SoC	System on a Chip
SoH	Statement of Health
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On
STBC	Space-Time Block Coding
STM	Station Management
STP	Spanning Tree Protocol
STRAP	Secure Thin RAP
SU-MIMO	Single-User Multiple-Input Multiple-Output
SVP	SpectraLink Voice Priority
TAC	Technical Assistance Center
TACACS	Terminal Access Controller Access Control System
TCP/IP	Transmission Control Protocol/ Internet Protocol
TFTP	Trivial File Transfer Protocol

**Table 4:** *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
TIM	Traffic Indication Map
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TLV	Type-length-value
ToS	Type of Service
TPC	Transmit Power Control
TPM	Trusted Platform Module
TSF	Timing Synchronization Function
TSPEC	Traffic Specification
TTL	Time to Live
TTLS	Tunneled Transport Layer Security
TXOP	Transmission Opportunity
U-APSD	Unscheduled Automatic Power Save Delivery
UCC	Unified Communications and Collaboration
UDID	Unique Device Identifier
UDP	User Datagram Protocol
UI	User Interface
UMTS	Universal Mobile Telecommunication System
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Coordinated Universal Time
VA	Virtual Appliance
VBN	Virtual Branch Networking
VBR	Virtual Beacon Report
VHT	Very High Throughput

**Table 4:** *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
VIA	Virtual Intranet Access
VIP	Virtual IP Address
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over IP
VoWLAN	Voice over Wireless Local Area Network
VPN	Virtual Private Network
VRD	Validated Reference Design
VRF	Visual RF
VRRP	Virtual Router Redundancy Protocol
VSA	Vendor-Specific Attributes
VTP	VLAN Trunking Protocol
WAN	Wide Area Network
WebUI	Web browser User Interface
WEP	Wired Equivalent Privacy
WFA	Wi-Fi Alliance
WIDS	Wireless Intrusion Detection System
WINS	Windows Internet Naming Service
WIPS	Wireless Intrusion Prevention System
WISPr	Wireless Internet Service Provider Roaming
WLAN	Wireless Local Area Network
WME	Wireless Multimedia Extensions
WMI	Windows Management Instrumentation
WMM	Wi-Fi Multimedia
WMS	WLAN Management System
WPA	Wi-Fi Protected Access
WSDL	Web Service Description Language

**Table 4:** *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
WWW	World Wide Web
WZC	Wireless Zero Configuration
XAuth	Extended Authentication
XML	Extensible Markup Language
XML-RPC	XML Remote Procedure Call
ZTP	Zero Touch Provisioning