AOS-W 6.2.1.9

Release Notes

AOS-W 6.2.1.9 is a software patch release that introduces new features and fixes to the issues identified in the previous releases. For details on the features described in the following sections, see the *AOS-W 6.2 User Guide*, *AOS-W 6.2 CLI Reference Guide*, and *AOS-W 6.2 MIB Reference Guide*.

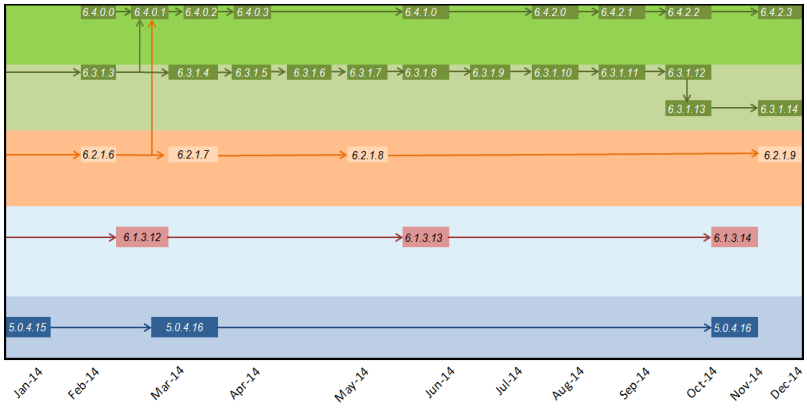
Chapter Overview

- Features in AOS-W 6.2.1.x Releases on page 14 provides a description of features and enhancements added in AOS-W 6.2.1.x
- Resolved Issues on page 24 provides a description of issues resolved in AOS-W 6.2.1.x.
- Known Issues on page 70 provides a description and workaround for the issues identified in AOS-W 6.2.1.x.
- Upgrade Procedures on page 86 describes the procedures for upgrading a switch to AOS-W 6.2.1.x.

Release Mapping

The following illustration shows the patch and maintenance releases that are included in their entirety in AOS-W 6.2.1.9.

Figure 1 *AOS-W Releases and Code Stream Integration*



Supported Browsers

The following browsers are officially supported to use with AOS-W 6.2.1.9 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 higher on Mac OS

Contacting Support

Table 1: *Contact Information*

Contact Center Online	
• Main Site	http://www.alcatel-lucent.com/enterprise
• Support Site	https://service.esd.alcatel-lucent.com
• Email	esd.support@alcatel-lucent.com
Service & Support Contact Center Telephone	
• North America	1-800-995-2696
• Latin America	1-877-919-9526
• EMEA	+800 00200100 (Toll Free) or 1650385-2193
• Asia Pacific	+65 6240 8484
• Worldwide	1-818-878-4507

This chapter describes features introduced in AOS-W 6.2.1.x. For more information about features introduced in AOS-W 6.2.0.x, refer to the *AOS-W 6.2.x User Guide.*

Features Introduced in AOS-W 6.2.1.9

This section lists the new features introduced in AOS-W 6.2.1.9.

Username Length Restriction

The maximum length of the switch management (SSH) username and password is restricted to 64 and 32 characters respectively.

Security Bulletin

As part of CVE-2014-3566 security vulnerabilities and exposures, SSLv3 transport layer security is disabled in AOS-W starting from version 6.2.1.9.

Client web browsers exclusively using SSLv3 will fail to access the Captive Portal or the switch WebUI. You must use TLSv1.0 transport layer security.

To address this vulnerability, the following changes are introduced under the **web-server ssl-protocol** command.

Parameter	Description	Range	Default
`ssl-protocol TLS v1.0`	Specifies the Transport Layer Security (TLS) protocol version used for securing communication with the web server.	—	tlsv1

Features Introduced in AOS-W 6.2.1.8

This section lists the new features introduced in AOS-W 6.2.1.8.

MIB and Trap Enhancements

The **wlsxAccessPointIsUP** and **wlsxAccessPointIsDown** traps are deprecated and replaced by **wlsxNAccessPointIsUp** and **wlsxNAccessPointIsDown** traps for AP up and down events respectively. For more information on these traps, download the **aruba-mibs_6.2.1.8_43656.tar** from the support site and view the **aruba-trap.my** file.

Features Introduced in AOS-W 6.2.1.7

There are no new features added in AOS-W 6.2.1.7.

Features Introduced in AOS-W 6.2.1.6

Change in User Idle Timeout Behavior

Starting from AOS-W 6.2, the split-tunnel and bridge users are timed out based on the aaa user idle-timeout value and not based on the value set in the L2 ageout. This change causes Captive portal with split-tunnel users to fall to pre-cp role for a short idle time. To avoid the occurrence of this issue, you can set the value of the **aaa user idletimeout** parameter in each captive portal profile.

Features Introduced in AOS-W 6.2.1.5

There are no new features added in AOS-W 6.2.1.5.

Features Introduced in AOS-W 6.2.1.4

There are no new features added in AOS-W 6.2.1.4.

Features Introduced in AOS-W 6.2.1.3

Default Value Changes

The **CSD Override** (Cyclic Shift Diversity) parameter is now set to be disabled by default in the **HT Radio** profile. The default behavior has changed because some clients incorrectly reported a low signal strength.

The change in default settings will not impact the upgrade if you have already disabled the **CSD Override** parameter.

The following example describes how to enable and disable the **CSD Override** parameter:

```
(host) (config) #rf ht-radio-profile default-a
(host) (High-throughput radio profile "default-a") csd-override
(host) (High-throughput radio profile "default-a") no csd-override
(host) (High-throughput radio profile "default-a") #end
(host) #show rf ht-radio-profile default-a
High-throughput radio profile "default-a" (Predefined (editable))
-----------------------------------------------------------------
Parameter                 Value
---------                 -----
40 MHz intolerance        Disabled
Honor 40 MHz intolerance  Enabled
CSD override              Disabled
```

Features Introduced in AOS-W 6.2.1.2

There are no new features added in AOS-W 6.2.1.2.

Features Introduced in AOS-W 6.2.1.1

There are no new features added in AOS-W 6.2.1.1

Features Introduced in AOS-W 6.2.1.0

Support for New Modem Types

AOS-W 6.2.1.0 introduces support for the Novatel Ovation MC551 4G LTE USB Modem and the Pantech UML290 4G USB modem.

Enhanced MultiMode Modem Provisioning

AOS-W 6.2.1.0 introduces a new method of provisioning a multimode USB modem (such as a Verizon UML290) for a remote AP. These changes simplify modem provisioning for both 3G and 4G networks.

The previous modem configuration procedure required that you define a driver for a 3G modem in the **USB modem** field in the AP provisioning profile, or define a driver for a 4G modem in the **4G USB type** field. Starting with AOS-W 6.2.1.0, you can configure drivers for both a 3G or a 4G modem using the **USB field**, and the 4**G USB Type** field is deprecated.

In the WebUI

The AP provisioning profile in AOS-W 6.2.1.0 includes a new **Cellular Network Preference** setting that allows you to select how the modem should operate. This setting includes parameters described in Table 2.

Table 2: *Cellular Network Preference Parameters*

Parameter	Description
auto (default)	In this mode, modem firmware will control the cellular network service selection; so the cellular network service failover and fallback is not interrupted by the remote AP (RAP).
3g_only	Locks the modem to operate only in 3G
4g_only	Locks the modem to operate only in 4G
advanced	The remote AP (RAP) controls the cellular network service selection based on an Received Signal Strength Indication (RSSI) threshold-based approach. • Initially the modem is set to the default **auto** mode. This allows the modem firmware to select the available network. • The RAP determines the RSSI value for the available network type (for example 4G), checks whether the RSSI is within required range, and if so, connects to that network. • If the RSSI for the modem's selected network is not within the required range, the RAP will then check the RSSI limit of an alternate network (for example, 3G), and reconnect to that alternate network. • The RAP will repeat the above steps each time it tries to connect using a 4G multimode modem in this mode.

In the CLI

```
(host) (config) #provision-ap
(Host) (AP provisioning) #cellular_nw_preference ?
3g-only                 Set the modem to operate only in 3G
4g-only                 Set the modem to operate only in 4G
advanced                Use advanced algorithm to select the available network
auto                    Let modem to select the network preference (default)
```

The following regulatory updates were introduced in AOS-W 6.2.1.x releases.

Periodic regulatory changes may require modifications to the list of channels supported by AP. For a complete list of channels supported by AP using a specific country domain, access the switch command-line interface and issue the command **show ap allowed-channels country-code <country-code> ap-type <ap-model>**.

Regulatory Updates in AOS-W 6.2.1.9

The following table describes regulatory enhancements introduced in AOS-W 6.2.1.9:

NOTE

Contact your local Alcatel-Lucent sales representative on device availability and support for the countries listed in the following table.

Table 3: *Regulatory Domain Updates*

Regulatory Domain	Update
Chile	Added support for OAW-225 access points.
Mexico, Macau, and Saudi Arabia	Added support for OAW-RAP108 and OAW-RAP109 remote access points.

Regulatory Updates in AOS-W 6.2.1.8

The following table describes regulatory enhancements introduced in AOS-W 6.2.1.8:

NOTE

Contact your local Alcatel-Lucent sales representative on device availability and support for the countries listed in the following table.

Table 4: *Regulatory Domain Updates*

Regulatory Domain	Update
India and Indonesia	Added support for OAW-AP114 and OAW-AP115 access points.
Colombia, Dominican Republic, Puerto Rico, Montenegro, Albania, and Bosnia, and Herzegovina	Added support for OAW-RAP155 remote access points.
Mexico	Added support for OAW-224 and OAW-225 access points.
Algeria	Added support for OAW-AP104 access points.

Regulatory Updates in AOS-W 6.2.1.7

The following table describes regulatory enhancements introduced in AOS-W 6.2.1.7:

NOTE

Contact your local Alcatel-Lucent sales representative on device availability and support for the countries listed in the following table.

Table 5: *Regulatory Domain Updates*

Regulatory Domain	Update
Costa Rica	Added support for OAW-AP92, OAW-AP93, OAW-AP134, and OAW-AP135 access points.
Senegal	Added support for OAW-AP134 and OAW-AP135 access points.

Regulatory Updates in AOS-W 6.2.1.6

The following table describes regulatory enhancements introduced in AOS-W 6.2.1.6:

Contact your local Alcatel-Lucent sales representative on device availability and support for the countries listed in the following table.

Table 6: *Regulatory Domain Updates*

Regulatory Domain	Update
Algeria	Added support for OAW-AP175P, OAW-AP175AC, and OAW-AP175DC access points.
Argentina	Added support for OAW-AP93, OAW-AP92, OAW-RAP108, and OAW-RAP109 access points.
Thailand	Added support for the OAW-RAP109 access point.
Israel	Added support for the OAW-RAP3WN, OAW-RAP3WNP, OAW-RAP108, OAW-RAP109, OAW-224, OAW-225, OAW-AP114, and OAW-AP115 access points.
Uruguay	Added support for OAW-AP93, OAW-AP92, and OAW-AP104 access points.
Vietnam	Added support for OAW-AP93 and OAW-AP92 access points.
Costa Rica	Added support for OAW-AP134 and OAW-AP135 access points.

Regulatory Updates in AOS-W 6.2.1.5

There are no regulatory updates introduced in AOS-W 6.2.1.5.

Regulatory Updates in AOS-W 6.2.1.4

The following table describes regulatory enhancements introduced in AOS-W 6.2.1.4:

Contact your local Alcatel-Lucent sales representative on device availability and support for the countries listed in the following table.

Table 7: *Regulatory Domain Updates*

Regulatory Domain	Update
Columbia, Dominican Republic, India, Macau, Pakistan, Puerto Rico, Qatar, Saudi Arabia, South Korea, and UAE	Added support for OAW-RAP108 and OAW-RAP109 access points.
Brazil	Added support for the OAW-RAP2WG access point.

Regulatory Updates in AOS-W 6.2.1.3

The following table describes regulatory enhancements introduced in AOS-W 6.2.1.3.

Contact your local Alcatel-Lucent sales representative on device availability and support for the countries listed in the following table.

Table 8: *Regulatory Domain Updates*

Regulatory Domain	Update
Russia, Brazil, South Africa, Colombia, and Macedonia	Added support for OAW-RAP3WN and OAW-RAP3WNP access points.
Algeria, Bosnia and Herzegovina, Columbia, Dominican Republic, South Korea, Macedonia, and Puerto Rico	Added support for OAW-AP104 access points.
Republic of Trinidad and Tobago	Added support for OAW-AP135 and OAW-AP175 access points.
Algeria	Added support for OAW-AP92, OAW-AP93, and OAW-AP105 access points.
Bermuda, Bosnia and Herzegovina, Colombia, Dominican Republic, and Macedonia	Added support for the OAW-AP175DC access point.
Bolivia, Ecuador, El Salvador, Guatemala, Nicaragua, Panama, Puerto Rico, Venezuela, and Zambia	Added support for the OAW-AP105 access point.
Colombia	Added support for the OAW-AP92 access point.
Colombia, Dominican Republic, Mexico, Puerto Rico, and Singapore	Added support for the OAW-AP93 access point.

Table 8: *Regulatory Domain Updates*

Regulatory Domain	Update
Azerbaijan, Belarus, Bosnia and Herzegovina, Colombia, Croatia, Kazakhstan, Peru, and Russia	Added support for the OAW-AP135 access point.
Argentina	Added support for the OAW-RAP5WN access point.
Venezuela	Added support for OAW-AP175 and OAW-AP175AC access points.
Macau	Added support for OAW-AP134 and OAW-AP135 access points.
Macau and Ukraine	Added support for the OAW-AP175P access point.
Canada	Enabled DFS channels for OAW-AP175P, OAW-AP175AC, and OAW-AP175DC access points.
Uganda and Malaysia	Added support for the OAW-AP175AC access point.
Australia, New Zealand, Brazil, South Africa, Hong Kong, Singapore, Egypt, and Ukraine	Added support for OAW-RAP108 and OAW-RAP109 access points.

Regulatory Updates in AOS-W 6.2.1.2

The following changes impact new AP and remote AP installations running AOS-W 6.2.1.2:

Contact your local Alcatel-Lucent sales representative on device availability and support for the countries listed in the following table.

Table 9: *Regulatory Domain Updates*

Regulatory Domain	Update
Changes for OAW-RAP108/OAW-RAP109 **Access Points**	
Malaysia	AOS-W now supports this country domain.
Changes for OAW-AP124/OAW-AP125 **Access Points**	
Kazakhstan and Dominican Republic	AOS-W now supports these country domains.
Australia and New Zealand	These country domains support all channels allowed by the FCC (including indoor, outdoor and DFS channels). In previous releases, Australia and New Zealand used ETSI channels.
UAE	Removed support for channels 149-165.
Mexico	This domain requires Dynamic Frequency Selection (DFS) in all 802.11a channels. In previous releases, all 802.11a channels were open without DFS support.
Serbia	Added DFS support for channels 52-64 and 100-140. These channels were not open in previous releases.

Table 9: *Regulatory Domain Updates*

Regulatory Domain	Update
New Zealand, Puerto Rico, and Columbia	Removed support for channels 120-128, because these channels were removed from the FCC list of allowed channels.
Changes for OAW-AP134/OAW-AP135 Access Points	
Kazakhstan, Chile, Serbia, Dominican Republic and Nigeria	AOS-W now supports these country domains.
Bermuda, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Kenya, Pakistan, Mauritius, Panama, Qatar, Trinidad and Tobago, and Uruguay	Removed support for OAW-AP134 and OAW-AP135 in these country domains.
South Korea and Taiwan	Added support for DFS Channels 52-64, and 100-128. Previous releases did not include any support for these channels.
Singapore	Added support for DFS Channels 100-140. Previous releases did not include any support for these channels.
Israel	Channels 36-48 require DFS. In previous releases, these channels were open without DFS support.
Saudi Arabia	Removed support for channel 165.
Ireland and UAE	Removed support for channel 149-165.
Australia and New Zealand	These country domains support all channels allowed by the FCC (including indoor, outdoor and DFS channels).
Mexico	Requires DFS in all 802.11a channels. In previous releases, all 802.11a channels were open without DFS support.
New Zealand and Puerto Rico	Added DFS channel support for channels 52-64, 100-128. Previous releases did not include any support for these channels.
Colombia and Thailand	Removed support for channels 116-128
Russia	Removed support for channel 132.
Egypt	Removed support for channels 149-165. This country domain no longer supports 40MHz on any channel.
Ukraine	Added 40 MHz support for channels 149-161.
Peru	Removed support for channels 12-13, 52-64, 100-140, and 165 (The only supported channels for this country domain are 1-11, 36-48, and 149-161).
Venezuela	Added 40MHz support for channels 36-48, 52-64, and 149-161.
Jordan	Added 40MHz support for channels 36-48 and 149-161.

Regulatory Updates in AOS-W 6.2.1.1

There are no regulatory updates introduced in AOS-W 6.2.1.1.

Regulatory Updates in AOS-W 6.2.1.0

There are no regulatory updates introduced in AOS-W 6.2.1.0.

The following issues are resolved in AOS-W 6.2.1.x releases.

Resolved Issues in AOS-W 6.2.1.9

The following issues are resolved in AOS-W 6.2.1.9.

AP-Platform

Table 10: *AP-Platform Fixed Issues*

Bug ID	Description
101510 104520 104726 105296 105627 106396 107104 108006	**Symptom:** The status of an AP was displayed as UP on the local switch, but as DOWN on the master switch. The fix ensures that when there is no change in the value of the master switch IP, an update from the IKE module is rejected. **Scenario:** This issue was observed in OAW-S3 and OAW-4704 switches running AOS-W 6.3.1.5 in a master standby-local topology.

AP-Regulatory

Table 11: *AP-Regulatory Fixed Issues*

Bug ID	Description
98628	**Symptom:** MaxEIRP for OAW-RAP3WN/ OAW-RAP3WNP access points was inconsistent. The fix ensures that the correct regulatory and hardware limits are set and the value of MaxEIRP is greater than tx-power. **Scenario:** This issue was observed when the value of the configured tx-power was greater than the MaxEIRP. This issue was observed in OAW-4750 switches running AOS-W 6.3.1.3 in a master-local topology.

Authentication

Table 12: *Authentication Fixed Issues*

Bug ID	Description
101664	**Symptom:** When a switch was rebooted, the management user account created for cert-based WebGUI access was deleted. This issue is fixed by storing the username with quotes. **Scenario:** This issue was observed when the username was created with spaces. This issue was observed in switches running AOS-W 6.1.4.7-FIPS.

BaseOS Security

Table 13: *BaseOS Security Fixed Issues*

Bug ID	Description
102259	**Symptom:** AOS-W was vulnerable to an SSL/TLS Man-In-The-Middle (MITM) attack. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in switches running OpenSSL.
102632	**Symptom:** When a switch was upgraded from AOS-W 6.1 to AOS-W 6.3, EAP-TLS termination displayed an error. The log files listed the reason for the event as **certificate verification failed**. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed when the CA-certificate that was used for verification did not contain all the certificates required for Root CA. This issue was observed in switches running AOS-W 6.2 or later.
106066 106572	**Symptom:** The Authentication module crashed. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in OAW-4550/4650/4750 Series switches running AOS-W 6.1.3.5.

Configuration

Table 14: *Configuration Fixed Issues*

Bug ID	Description
103740	**Symptom:** When the **show dot1x supplicant-info pmkid** command was executed, the correct Pairwise Master Key Identifier (PMKID) was not displayed. Internal code changes ensure that the correct PMKID is displayed. **Scenario:** This issue occurred when the client performed a 802.1X authentication. This issue was observed in switches running AOS-W 6.4 and earlier versions.

Switch-Platform

Table 15: *Switch-Platform Fixed Issues*

Bug ID	Description
95835 98034 98202 99342	**Symptom:** A switch stopped responding and rebooted. The log files for the event listed the reason as **softwatchdog reset**. This issue is resolved by removing the race conditions in the panic dump path and reimplementing the watchdog framework. **Scenario:** This issue was seen during datapath core dump. This issue was observed on 7000 Series and OAW-4550/4650/4750 Series switches running AOS-W 6.3.1.2.

GRE

Table 16: *GRE Fixed Issues*

Bug ID	Description
100210	**Symptom:** The L2 GRE tunnel crashed frequently. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in OAW-4306 Series and OAW-4x04 Series switches where the master and local switches were connected using IPSec and the L2 GRE traffic flowed through the IPSec tunnel.

Mobility

Table 17: *Mobility Fixed Issues*

Bug ID	Description
102540	**Symptom:** The IP Mobility module crashed on the switch. This issue is resolved by making code level changes to correct the error message. **Scenario:** An incorrect error message was displayed in the IP Mobility module. This issue was observed in OAW-4604 switches running AOS-W 6.2.1.7.

QoS

Table 18: *QoS Fixed Issues*

Bug ID	Description
103363	**Symptom:** When the DSCP value on the outer GRE IP was not set, a voice quality issue was observed with Vocera badges. This issue is resolved by copying the inner DSCP value to the outer DSCP parameter, when a packet is GRE encapsulated. **Scenario:** This issue was observed only when WEP was enabled. This issue was not limited to any specific switch model.

Station Management

Table 19: *Station Management Fixed Issues*

Bug ID	Description
86620 88646	**Symptom:** The **show ap association client-mac** command displayed client MAC addresses for clients that exceeded the value set for idle timeout. This issue is resolved by implementing internal code changes. **Scenario:** This issue was not limited to any specific switch model or AOS-W release version.

Resolved Issues in AOS-W 6.2.1.8

The following issues are resolved in AOS-W 6.2.1.8.

Air Management- IDS

Table 20: *Air Management- IDS Fixed Issues*

Bug ID	Description
81740 97522	**Symptom:** Traps were sent when an SSID went up or down instead of being sent when an AP went up or down. Also, an incorrect IP address of the AP was sent. This issue is resolved by replacing the incorrect traps with the correct traps, and by verifying the IP address of the AP sent is correct. **Scenario:** This issue was not limited to a specific switch model or release version.

BaseOS Security

Table 21: *BaseOS Security Fixed Issues*

Bug ID	Description
93237	**Symptom:** An internal module (Authentication) crashed on the switch. Ignoring the usage of the equivalentToMe attribute, which was not used by the master switch resolved this issue. **Scenario:** This issue was observed when the Novell® Directory System (NDS) pushed the bulk of user data as the value for the attribute to the master switch. This issue was not limited to a specific switch model or release version.
99038	**Symptom:** An increase in the memory usage was observed in the authentication module. This issue is resolved by fixing the memory leak in the authentication module. **Scenario:** This issue was observed when client devices performed EAP-TLS with EAP-termination enabled using certificates containing the optional field **Subject Alternative Name**.

Captive Portal

Table 22: *Captive Portal Fixed Issues*

Bug ID	Description
93927	**Symptom:** On OAW-4550/4650/4750 Series switches the output of **show datapath user** displayed a user entry but the user entry was not present in the control plane. This issue was resolved by internal code changes. **Scenario:** This issue occurred when WLAN was configured in the tunnel mode and was observed in AOS-W 6.2 or later versions.
94167	**Symptom:** When client traffic was moving through an L3 GRE tunnel between a data switch and a switch, the switch did not provide the captive portal page to the client. The fix ensures that the switch provides the captive portal page to the client. **Scenario:** This issue was observed after OAW-S3 switch was upgraded to AOS-W 6.1.3.10. This issue was caused because the switch was unable to find the correct role for the client traffic and, therefore, did not provide the captive portal page.

Switch-Platform

Table 23: *Switch-Platform Fixed Issues*

Bug ID	Description
91097	**Symptom:** A local switch rebooted unexpectedly. The log files for the event listed the reason for the reboot as **Mobility Processor update**. The fix ensures that the switch does not reboot unexpectedly by making code level changes to the primary and secondary nor flash boot partition. **Scenario:** This issue was observed in switches running AOS-W 6.1.3.9.
96347 94427 97078 97287 97456 97468 97988 98425 98656 105574	**Symptom:** OAW-S3 switch rebooted unexpectedly. The log files for the event listed the reason for the reboot as **User pushed reset** error. The issue is resolved by removing the lock contention. **Scenario:** This issue was observed due to panic dump or SOS crash, which was a result of jumbo packet or packet corruption. This issue was observed in OAW-S3, 3200, OAW-4604, and OAW-4704 switches, but was not limited to any specific AOS-W release version.
96712	**Symptom:** A local switch rebooted unexpectedly during a terminal/ssh related operation. The log files for the event listed the reason for the reboot as **Kernel panic**. **Scenario:** This issue was observed in OAW-4750 switches running AOS-W 6.2.1.4.
97658 97388 98373	**Symptom:** Some access points lost connectivity when the switch to which they were connected rebooted. This issue is resolved by ensuring that the boot partition information is updated in the secondary bank of the switch. **Scenario:** This issue occurred when the switch rebooted due to a watchdog reset. This issue was not limited to any specific switch model or release version.
98873	**Symptom:** OAW-4306G switch was crashing during reboot. The log files for the event listed the reason as an **address error on CPU4**. **Scenario:** This issue was observed on the OAW-4306G switches running on AOS-W 6.2.1.7.
99106	**Symptom:** A large number of **Only Bottom slots can arbitrate** debug messages were generated and as a result the switch console was flooded with these redundant messages. The issue is fixed by disabling these redundant messages in the arbitration algorithm. **Scenario:** This issue was observed in OAW-S3 switches and is not limited to any AOS-W version.

LDAP

Table 24: *LDAP Fixed Issues*

Bug ID	Description
90859	**Symptom**: A switch intermittently disconnected from the LDAP server because the LDAP server reset its TCP connection. Establishing a TCP connection for each user and binding it using admin-dn and password fixed this issue. Once the user is authenticated, the connection binds the actual user. **Scenario**: This issue was triggered by null binds created when the switch established TCP/SSK connections in advance, so that they can be used whenever a user joined the network. This issue occurred in OAW-4x04 Series switch running AOS-W 6.1.3.10.

VLAN

Table 25: *VLAN Fixed Issues*

Bug ID	Description
97117	**Symptom:** When the RADIUS server returned multiple Vendor Specific Attributes (VSAs), AOS-W did not check these attributes or set user roles. This issue is fixed by verifying the list of attributes before matching them with the rules. **Scenario:** This issue was observed when a user tried to set a role using the VSA attributes that were returned from the RADIUS server. This issue was observed in OAW-4604 Series switches running AOS-W 6.2.1.4.

Voice

Table 26: *Voice Fixed Issues*

Bug ID	Description
91910 94031 100262	**Symptom:** The output of the **show voice call-cdrs** command displayed multiple CDR with **INITIATED** state for calls between ASCOM® phones. The fix ensures correct handling of the state transitions for New Office Environment (NOE) application layer gateway. **Scenario:** This issue occurred during a consulted call scenario. This issue is observed in an NOE deployed voice environment with switches running AOS-W 6.1 or later.
94038 94600	**Symptom:** The **show voice call-cdrs** and **show voice client-status** commands displayed incorrect state transitions for consulted, transfer, and speaker announced call scenarios. The fix ensures the correct state transitions for New Office Environment (NOE) application layer gateway. **Scenario:** This issue was observed in an NOE deployed voice environment with switches running AOS-W 6.1 or later versions.
94342	**Symptom:** The Station Management (STM) process crashed in a New Office Environment (NOE) deployment. This issue is resolved by making code level changes to avoid a STM crash. **Scenario:** This issue was observed when an NOE user tried to call an extension, but disconnected the call before it was complete, as a result the CDR changed to **CONNECTING** state. This issue was observed in switches running AOS-W 6.1.3.10.
95566	**Symptom:** When two parties made a VoIP call using Microsoft® Lync 2013, media classification running on the switch prioritized the media session with wrong DSCP values. The fix ensures that the wmm value is read from the Tunnel Entry rather than the Bridge Entry, so that the value is correct. **Scenario:** The DSCP values configured under the ssid-profile did not take effect. This issue occurred when the initial VLAN and the assigned VLAN were different. This issue was observed on OAW-S3 switches running AOS-W 6.1.3.10.
97823	**Symptom:** SVP, Lync, or FaceTime calls prioritized using VoIP ALGs, continued to have call detail records in the connected state although the calls were disconnected. This caused a memory leak in the Station Management process. This issue is resolved by fixing the memory leak in the station management module. **Scenario:** This issue was observed in deployments that used SVP phones, Lync, or FaceTime with media classification enabled. This issue was observed on switches running AOS-W 6.2.1.5 or later.

WebUI

Table 27: *WebUI Fixed Issues*

Bug ID	Description
96284 100319	**Symptom**: When you click on the **Plan** tab of the switch's WebUI using Microsoft® Internet Explorer 11, the **Plan** page fails to load. This issue is resolved by making changes to the internal code such that the **Plan** page loads successfully. Also, removed the scope for function declaration and object creation. **Scenario:** This issue was observed on switches running AOS-W 6.2.1.x and AOS-W 6.1.3.x.
101734	**Symptom**: When the **traceroute** test was executed from the WebUI, the result did not appear in the **Diagnostic** window, instead the test went into a loop and displayed the asterix (*) symbol. To resolve this issue the WebUI **traceroute** code is updated to use the **busyroute** command. **Scenario:** This issue was observed when the **traceroute** command is executed using the WebUI. This issue was observed in OAW-4704 switches running AOS-W 6.2.1.8.

Resolved Issues in AOS-W 6.2.1.7

The following issues are resolved in AOS-W 6.2.1.7.

AP-Platform

Table 28: *AP-Platform Fixed Issues*

Bug ID	Description
96913	**Symptom:** When a switch was upgraded from AOS-W 5.x or AOS-W 6.0.x to AOS-W 6.3.1.3, APs failed to upgrade to AOS-W 6.3.1.3. A defensive check is made in the affected API so that PAPI messages which are smaller than the PAPI header size are handled properly in 6.0.x compared to 5.x. **Scenario:** This issue was observed in APs running AOS-W 5.x or AOS-W 6.0.x. APs running AOS-W 6.1 and later versions were not impacted.
97237	**Symptom:** A switch rebooted because of a memory leak in the module that handles address, route, and interface related configurations and notifications on the system. This issue is resolved by fixing the memory leak in the flow. **Scenario:** The memory leak occurred when an interface or STP states changed frequently with a PAPI error. This issue was observed on OAW-4306G switches running AOS-W 6.2.1.6 or later.

BaseOS Security

Table 29: *BaseOS Security Fixed Issues*

Bug ID	Description
96458	**Symptom:** A switch rebooted with the reboot cause **Nanny rebooted machine - low on free memory**. This issue is resolved by freeing the memory that was leaking in the authentication module. **Scenario:** This issue was observed for VPN users when the **cert-cn-lookup** parameter was disabled under **aaa authentication vpn** profile. This issue was not limited to a specific switch model or release version.

Mobility

Table 30: *Mobility Fixed Issues*

Bug ID	Description
96569	**Symptom:** The client did not receive an IP address through DHCP, and could not pass traffic when L3 mobility was enabled on the switch. This issue is resolved by clearing the state machine of the affected client. **Scenario:** This issue was observed when the client roamed from a Virtual AP (VAP) in which the **mobile-ip** parameter was enabled to a VAP in which the **mobile-ip** parameter was disabled. This issue was observed in AOS-W 6.2 and later versions, but was not limited to a specific switch model.

WebUI

Table 31: *WebUI Fixed Issues*

Bug ID	Description
68464	**Symptom:** The user was forced out of a WebUI session with the **Session is invalid** message. This issue is resolved by fixing the timing issue for the exact session ID from cookies in the https request. **Scenario:** This issue was observed when a web page of the parent domain name was accessed previously from the same browser. This issue was not limited to a specific switch model or release version.

Resolved Issues in AOS-W 6.2.1.6

The following issues were resolved in AOS-W 6.2.1.6:

AP-Platform

Table 32: *AP-Platform Fixed Issues*

Bug ID	Description
87857	**Symptom**: Fragmented configuration packets sent from the switch to the AP can cause the AP to come up with the “D:” (dirty) flag. Improvements to how AOS-W handles out-of-order packets resolve this issue. **Scenario**: This issue is triggered by network congestion or breaks in the connection between the switch and AP.

AP-Wireless

Table 33: *AP Wireless Fixed Issues*

Bug ID	Description
67847 69062 69346 71530 74352 74687 74792 75212 75792 75944 76142 76217 76715 77273 77275 78118 80735 82147 83242 83243 83244 83624 83833 84170 84339 84511 85015 85054 85086 85367 85959 88515 89136 89253 89256 89816 90603 91084 92871 92877 92878 92879 93923	**Symptom:** APs unexpectedly rebooted. The log files listed the reason for the reboot as **Data BUS error**. A change in the exception handling module has fixed this issue. **Scenario:** This issue was observed in OAW-AP120 Series and OAW-AP68P devices connected to switches running AOS-W 6.3.1.2.

BaseOS Security

Table 34: *BaseOS Security Fixed Issues*

Bug ID	Description
76239	**Symptom**: VPN user entries did not properly age out of the user table. These user entries became stale and prevented new users with the same IP address from associating to the network. This issue occurred when one Inner-IP address was assigned to two different L2TP outer-IP addresses. AOS-W 6.2.1.6 resolves this issue by introducing a fix that prevents a previously assigned IP address from returning to the free IP address pool during Next-pin mode using SecureID authentication. **Scenario**: The issue was identified in OAW-4324 switches running AOS-W 5.0.4.5 during Next-pin mode using SecureID as authentication.
77227	**Symptom**: An internal process that handles user authentication unexpectedly crashed in the switch due to incorrect memory allocation. The issue was fixed by making changes to the IP address pool. **Scenario**: When remote VPN users were deleted from the system, unexpected sequence of events pointed at stale memory entries. This resulted in an internal process failure. This issue is not limited to a specific switch model or release version.
93130	**Symptom:** A switch reboots unexpectedly. The log files for the event listed the reason for the reboot as **datapath exception**. This issue is resolved by adding SSL implementation to validate a packet before processing it. **Scenario**: This issue was observed when VIA was used to establish a tunnel with the switch, using SSL fallback. This issue was not limited to any specific switch model or release version.

Captive Portal

Table 35: *Captive Portal Fixed Issues*

Bug ID	Description
93674	**Symptom**: Clients are unable to access an external captive portal page after the switch resets. Changes in how AOS-W manages captive portal authentication profiles resolved this issue. **Scenario**: This issue occurred in AOS-W 6.1.3.x when the switch failed to use the correct ACL entry for a pre-authentication captive portal role.
92927	**Symptom:** When iOS 7 clients tried to connect through the Captive Portal profile, the users were not redirected to the next page even after a successful authentication. A change in the redirect URL has fixed this issue. **Scenario:** This issue was observed only in clients using Apple iOS 7 devices.

Configuration

Table 36: *Configuration Fixed Issues*

Bug ID	Description
88120	**Symptom**: The **Configuration** > **Wireless** > **AP Installation** > **AP provisioning** > **Status** tab of the switch WebUI and the output of the commands **show ap database long status up start 0 sort-by status sort-direction ascending** and **show ap database long status up start 0 sort-by status sort-direction descending** do not correctly sort the AP entries in ascending or descending order by up time. Improvements to how the switch sorts APs by status and up time resolve this issue. **Scenario**: This issue was identified in switches running AOS-W 6.2.1.2
94559	**Symptom**: An ACL configured by the user could not be edited or deleted. This issue is resolved by ensuring that the non-editable flag is reset if ACLs are reused after the whitelist is removed.. **Scenario**: This issue was observed in AOS-W 6.2.x or later, when a user configuration had a white-list defined in a Captive Portal profile, and was triggered because the ACLs that enable white-listing for destinations in a captive-portal profile were reused for user-configured ACLs.

Switch-Datapath

Table 37: *Switch-Datapath Fixed Issues*

Bug ID	Description
93423	**Symptom:** A switch unexpectedly rebooted, and the log file listed the reason for the reboot as **Datapath timeout**. This issue is fixed by increasing the stack memory size in the data plane. **Scenario:** This issue was observed when clients using SSL VPN connected to RAP and the switch tried to decompress these packets. This issue is not limited to any specific switch model or AOS-W release version.
87417 87846 90469 90896 89641 88039 94157 89433 90746 94636 88445 95332 90024 91853 92827 92828 92829 92830 92832 87949 92464 92466 95655 88226 90458 92294 93555 95333 93825 94007 95703 92988 89539 94476	**Symptom**: A master switch reboots unexpectedly. The log files for the event listed the reason for the reboot as **datapath exception**. **Scenario**: This issue is observed in OAW-4750 switch running AOS-W 6.3.1.1 in a master-local topology.
82770	**Symptom:** Using Alcatel-Lucent Discovery Protocol (ADP), access points did not discover the master switch after enabling Broadcast/Multicast (BC/MC) rate optimization. With this fix, enabling BC/MC rate optimization does not block ADP packets. **Scenario:** When BC/MC rate optimization was enabled on the VLAN, the switch dropped ADP packets from access points. This issue was not limited to a specific switch model or release version.
95756	**Symptom**: The firewall stall-detection feature was not enabled by default in AOS-W 6.2.1.x. This issue is resolved, and firewall stall-detection is now enabled by default. The output of the show firewall CLI command now shows stall detection is enabled. **Scenario**: This issue occurred in AOS-W 6.2.1.x, and is not limited to a specific switch model.

Switch-Platform

Table 38: *Switch Platform Fixed Issues*

Bug ID	Description
90619 91950 92250 92273	**Symptom:** The switch WebUI stopped responding indefinitely. The fix ensures that the OV3600 query fails if there is no firewall visibility. **Scenario:** This issue occurred when OV3600 queried for firewall visibility details from a switch on which the firewall visibility feature was disabled. This issue was observed in switches running AOS-W 6.2 or later.
91541 94045 95079	**Symptom:** A switch rebooted due to low memory. Changes to how the switch uses buffers during the image copy process fixes this issue. **Scenario:** This issue occurred when there was continuous high traffic terminating on the control plane. This resulted in an internal component of the AOS-W software to take up high memory. This issue was observed in OAW-4306 Series, OAW-4x04 Series, and OAW-S3 switches running AOS-W 6.1 and later versions.
95044	**Symptom:** Some access points went down when the switch to which they are connected rebooted. This issue is resolved by ensuring that the boot partition information is updated in the secondary bank of the switch. **Scenario:** This issue occurred when the switch rebooted due to a watchdog reset. This issue was not limited to any specific switch model or release version.

Switch-Software

Table 39: *Switch Software Fixed Issues*

Bug ID	Description
89460	**Symptom**: When an AP used adjacent DFS channels, that AP incorrectly detected RADAR and exhausted all DFS channels. If no non-DFS channels were enabled, the AP stopped responding to clients. Improvements that prevent incorrect RADAR detection resolve this issue. **Scenario**: This issue occurred on OAW-AP135 access points using adjacent DFS channels, and was triggered when the AP misidentified a small data packet as a FCC type-5 RADAR packet, causing false RADAR detection.

IPv6

Table 40: *IPv6 Fixed Issues*

Bug ID	Description
74367	**Symptom**: Clients using temporary IPv6 addresses are not be able to communicate as traffic is getting dropped. The issue is been fixed by rotating the ipv6 addresses allocated to the client, and replacing the old IP address by new IP addresses **Scenario**: A client can support up to four IPv6 addresses. The usage of temporary IPv6 addresses on the clients replaced old IPv6 addresses allocated in user-table and sent traffic using these addresses. The issue occurred on the switches that support IPv6 clients

RADIUS

Table 41: *RADIUS Fixed Issues*

Bug ID	Description
93689	**Symptom**: When Windows phone clients run a script for 802.1X authentication, the switch sends a EAP Failure message. This issue is resolved by removing the EAP-Failure messages when the client times out during 802.1X authentication. **Scenario**: This issue was identified in AOS-W 6.1.3.8, and was not limited to any specific switch mode.

SNMP

Table 42: *SNMP Fixed Issues*

Bug ID	Description
94205	**Symptom**: The MIB **sysExtFanStatus** cannot be queried. This issue is resolved by changes that ensure that the internal **fanCount** value is initialized for OAW-4550/4650/4750 Series switches. **Scenario**: This issue occurs on OAW-4550/4650/4750 Series switches running AOS-W 6.2.x and 6.3.x. 6.3.1.1. This issue was triggered because the internal hardware monitoring process did not return the proper values for **fanStatus** SNMP queries.

WebUI

Table 43: *WebUI Fixed Issues*

Bug ID	Description
76439	**Symptom**: The Spectrum Analysis section of the AOS-W WebUI fails to respond when a connected spectrum monitor is in a DOWN state. Changes to how the WebUI displays popup messages resolve this issue. **Scenario**: This issue occurred in AOS-W 6.2.0.0, when an OAW-AP105 access point in hybrid AP mode failed to appear as a connected spectrum monitor in the switch WebUI.
92340 92649	**Symptom:** The WebUI of a switch failed to load in Internet Explorer 11 with the error message **can't create XMLHttpRequest object: Object doesn't support property or method 'creatXMLHttpRequest**. The AOS-W WebUI is updated to be compatible with the new standards in Internet Explorer 11. **Scenario:** This issue was caused by differences between Internet Explorer 11 and Internet Explorer 10. This issue was observed in Internet Explorer 11 and not limited to any specific switch model or release version.
93606	**Symptom:** Clients were not displayed in the **Monitoring** > **Switch** > **Clients** page of the WebUI when filtered with AP Name. This issue is fixed by changing the **show user-table location <ap-name>** command to **show user-table ap-name <ap-name>**. **Scenario:** This issue was triggered by changes to CLI commands. This issue was observed in switches running AOS-W 6.2 and 6.3.

Resolved Issues in AOS-W 6.2.1.5

The following issues were resolved in AOS-W 6.2.1.5:

802.1X

Table 44: *802.1X Fixed Issues*

Bug ID	Description
89106	**Symptom**: The **class** attribute was missing from RADIUS accounting messages sent to clients when previously idle clients reconnected to the network. **Scenario**: This issue occurred in a deployment using RADIUS accounting, where the RADIUS server sends **class** attributes in the access-accept messages for to 802.1X authentication. In previous releases, when an idle user timed out from the network, AOS-W deleted the **class** attribute for the user along with rest of the user data. This issue is resolved with the introduction of the **delete-keycache** parameter in the 802.1X authentication profile, which, when enabled, deletes the user keycache when the client's user entries get deleted. This forces the client to complete a full 802.1X authentication process when the client reconnects after an idle timeout, so the CLASS attributes will again be sent by the RADIUS servers.

Air Management - IDS

Table 45: *Air Management IDS Fixed Issues*

Bug ID	Description
90330	**Symptom:** An adhoc AP marked to be manually contained would not be contained unless the **protect from adhoc** feature was enabled. This issue is resolved by allowing traditional adhoc containment whenever enhanced adhoc protection is enabled, even if the **protect from adhoc** feature is not enabled. **Scenario:** This issue was observed on switches running AOS-W 6.2.x.

AP-Datapath

Table 46: *AP-Datapath Fixed Issues*

Bug ID	Description
90645	**Symptom:** When the **show datapath session ap-name** was executed, the **ap-name** option was not implemented. **Scenario:** This issue was observed in AOS-W 6.2.1.3 and is not specific to any switch model.

AP-Platform

Table 47: *AP-Platform Fixed Issues*

Bug ID	Description
88389 89882 90175 90332	**Symptom:** 802.11n-cagpable access points unexpectedly rebooted. The log files for the event listed the reason for the reboot as **kernel page fault**. Improvements in the wireless driver of the AP resolved this issue. **Scenario:** This issue was observed when a 802.11n-capable campus AP was in bridge forwarding mode and there was a connectivity issue between the AP and the switch. This issue was observed in 802.11n-capable access points running AOS-W.
89016	**Symptom**: The SNMP OID **wlanStaAccessPointESSID** had no value when a client roamed from a down AP to an active AP. Improvements to internal processes that manage Layer-2 roaming resolve this issue. **Scenario**: This issue was observed when clients roamed between APs running AOS-W 6.2.x

AP-Regulatory

Table 48: *AP-Regulatory Fixed Issues*

Bug ID	Description
86764	**Symptom:** The output of the **show ap allowed channels** command incorrectly indicated that OAW-AP68 and OAW-AP68P access points supported 5 GHZ channels. This issue is resolved by changes that modify how AOS-W displays the allowed channel list for OAW-AP68 and OAW-AP68P APs. **Scenario:** This issue was observed on OAW-AP68 and OAW-AP68P access points running AOS-W 6.1.x and 6.2.x.

AP-Wireless

Table 49: *AP-Wireless Fixed Issues*

Bug ID	Description
89046 89053 89058 84081 88044 88569 88631 88843 89044 89325 89326 89811 89901 92336 93335	**Symptom:** An access point continuously stopped responding and rebooted. This issue was resolved by improvements to the wireless drivers in AOS-W 6.1.3.11. **Scenario:** This issue was observed in OAW-AP125 and OAW-220 Series access points running AOS-W 6.1.3.x when the clients disconnected from the network.
88328 89623	**Symptom:** Wireless clients experienced packet loss when connected to remote APs in bridge mode. This issue is fixed by changes that ensure some buffer is reserved for transmitting unicast traffic. **Scenario:** This issue was observed in OAW-AP105 APs running AOS-W 6.1.3.8 with high levels of multicast or broadcast traffic in the network. This issue was not limited to a specific switch model.
90960	**Symptom**: Microsoft® Surface Pro and Surface RT clients were unable to acquire an IP address or correctly populate the ARP table with a MAC address when connecting to an AP using 20 MHz channels on 2.4 GHz or 5 GHz radios. This issue is resolved by channel scanning improvements to APs in 20 MHz mode. **Scenario**: This issue was triggered when Microsoft Surface clients running Windows 8 or Windows 8.1 connected to 20 MHz APs running AOS-W 6.1.3.8.
91856	**Symptom:** Certain 802.11b clients did not communicate with Alcatel-Lucent 802.11n-capable access points. Improvements in the wireless driver of 802.11n-capable access points resolve this issue. **Scenario:** This issue was observed when Denso® 802.11b handy terminals communicated with Alcatel-Lucent 802.11n-capable access points on channel 7. This issue was not limited to any specific switch model or release version.

BaseOS Security

Table 50: *BaseOS Security Fixed Issues*

Bug ID	Description
84164 92279	**Symptom**: Issuing the command **clear aaa device-id-cache mac <mac>**, where <mac> was the MAC address of a wireless user that did not have an entry in the station table, caused the switch to stop responding. Improvements to the internal switch module that manages user authentication resolves this issue. **Scenario**: This issue occurred in OAW-4x04 Series switches running AOS-W 6.2.1.x.
89453	**Symptom:** The **show rights** command did not display all the user roles configured in the switch. This issue is resolved by a change that ensures that the output of this command displays all the user roles configured in the switch. **Scenario:** This issue was observed when more than 50 user roles were configured in a switch running AOS-W 6.2.1.3.
90233	**Symptom:** Clients with a **logon** user role did not age out from the user-table after the **logon-lifetime** AAA timer expired. This issue is resolved by a change that ages out users with the **logon** user role if User Derivation Rule (UDR) is configured in the AAA profile. **Scenario:** This issue was observed when UDR was configured in the AAA profile with **logon** defined as the default user role. This issue was observed on switches running AOS-W 6.2.1.x.
80396	**Symptom**: An internal (profmgr) process crashed on a switch and users were not able to change, add, or delete the corrupted configuration. This issue is fixed adding additional checks that ensure internal data is copied to a valid location with correct references. **Scenario**: This issue occurred when a configuration profile referring to an external RADIUS server, for example, the aaa-server-group profile, was changed and pointed to another server. This caused the data structure and refcounts to the new RADIUS server to become invalid. This issue was not specific to any profile or the RADIUS server associated with a switch. This issue was observed on switches running AOS-W 6.1.3.x and 6.2.x.
92674 93609	**Symptom:** Class attribute was missing in Accounting STOP packet. This issue is resolved by not resetting the counters when an IPv6 user entry is deleted. **Scenario:** This issue occurred when the counters were reset during an IPv6 user entry aged out. This issue was not limited to any specific switch or AOS-W version.

Captive Portal

Table 51: *Captive Portal Fixed Issues*

Bug ID	Description
91442	**Symptom**: When configuring the captive portal login page using the master switch's command line interface, the question mark symbol was not getting added to the configuration or pushed to the local switch. This issue is resolved by making sure that the master switch's command line interface accepts the question mark symbol as part of the login page configuration. **Scenario:** This issue was observed when synchronizing the captive portal configuration from the master switch to the local switch.

Switch-Datapath

Table 52: *Switch-Datapath Fixed Issues*

Bug ID	Description
88469	**Symptom:** A switch denied any FTP download which used Extended Passive mode over IPv4. This issue is resolved by modifying the FTP ALG to handle the Extended Passive mode correctly. **Scenario:** This issue was observed when an IPv4 FTP client used the Extended Passive mode. In such a case, the FTP ALG on the switch detected it as a Bounce Attack and denied the session. This issue was not limited to a specific switch model or release version.
90454	**Symptom**: A remote AP unexpectedly rebooted because it failed to receive heartbeat responses from the switch. Changes to the order in which new IPSec SAs are added and older IPSec SAs are removed resolve this issue. **Scenario**: This issue occurred after a random IPSec rekey, and was triggered when the outbound IPSec SA was deleted before the inbound IPSec SA was added. This removed the route cache for the inner IP, causing the session entry to incorrectly point to the default gateway, and preventing heartbeat responses from reaching the AP.

Switch-Platform

Table 53: *Switch-Platform Fixed Issues*

Bug ID	Description
82736 82875 84022 85628 86005 86572 86589 87410 87505 87587 88332 88351 88434 88921 89818 90909 91269 91308 91370 91517 93294	**Symptom:** A switch rebooted unexpectedly. Changes in the watchdog implementation on the switch resolve the issue. **Scenario:** Log files for the event indicated the reason for the reboot as **soft watchdog reset**. This issue was not limited to any specific switch model or release version.
86216 85566 87090 87635 88321 88387 88699 89436 89727 89839 89911 90162 90338 90481 91193 91387 91941 92139 92187 92516 92808 93630 93693 93931 94308	**Symptom**: During a kernel panic or crash, the panic dump generated by the switch was empty. New infrastructure has been added to improve the collection of crash dumps. **Scenario**: This issue impacts OAW-4x04 Series, OAW-4306 Series, and OAW-S3 switches and was observed in AOS-W 6.1.3.7.
83502 83762 85355 85370 86029 86031 88005 89636 92823	**Symptom:** A switch rebooted unexpectedly. Changes in the watchdog implementation on the switch resolved the issue. **Scenario:** Log files for the event indicated the reason for the reboot as **user pushed reset** This issue was identified in AOS-W 6.1.3.x, and is not limited to any specific switch model.

Table 53: *Switch-Platform Fixed Issues*

Bug ID	Description
89155	**Symptom**: OAW-4306 Series switches experienced high levels of CPU usage during bootup, triggering the warning messages **Resource 'Controlpath CPU' has exceeded 30% threshold**. This issue is resolved by changes to internal CPU thresholds that better reflect expected CPU usage levels. **Scenario**: This issue was observed in switches running AOS-W 6.1.2.3.
90751 90633 90863 91154 91138 91474 91656	**Symptom**: Switches continuously stopped responding and rebooted. Enhancements to memory allocation resolved this issue. **Scenario**: The issue occurred when an internal module (FPCLI) stopped responding due to memory corruption. This issue was observed in OAW-S3 switches and is not limited to a specific version of AOS-W.
91383	**Symptom**: Issuing a **show** command causes the switch command-line interface to display the error **Module Configuration Manager is busy. Please try later**. Improvements to how the switch manages HTTP session keys resolve this issue. **Scenario**: This issue occurred when issuing show commands from the command-line interface of OAW-4x04 Series standby switch, and is triggered when the database synchronization process attempts to simultaneously replace and add an HTTP session key in the user database.

DHCP

Table 54: *DHCP Fixed Issues*

Bug ID	Description
90611 91512	**Symptom:** The Dynamic Host Configuration Protocol (DHCP) module crashed on a switch and users were not able to perform a new DHCP configuration. Improvements to internal DHCP processes fix this issue in AOS-W 6.2.1.5. **Scenario:** This issue was triggered by a race condition that caused the DHCP wrapper process to continually crash and restart. This issue was not specific to any switch model or release version.

Hardware Management

Table 55: *Hardware Management Fixed Issues*

Bug ID	Description
87481	**Symptom:** The OAW-4550/4650/4750 Series switches returned an invalid value when an SNMP query was performed on the internal temperature details (OID .1.3.6.1.4.1.14823.2.2.1.2.1.10). The fix ensures that the SNMP attribute is set correctly for the temperature details. **Scenario:** This issue was limited to OAW-4550/4650/4750 Series switches running AOS-W 6.3 or later versions.

IPv6

Table 56: *IPv6 Fixed Issues*

Bug ID	Description
88814	**Symptom:** Users connected to the switch with derived VLANs received IPv6 router advertisements from VLANs other than those to which the clients were associated. This issue is resolved by updating the switch datapath with a router advertisement conversion flag so the datapath converts multicast router advertisements to unicast. **Scenario**: This issue was observed in IPv6 networks with derived VLANs and was not limited to a specific switch model or release version.

Master-Redundancy

Table 57: *Master-Redundancy Fixed Issues*

Bug ID	Description
80041	**Symptom**: The database that synchronizes settings between a master and a backup switch failed to synchronize. Log files for the event listed the reason for the error as **Last failure cause: Standby switch did not respond to the start request or is not ready**. This issue is resolved by changes that allow AOS-W to ignore any aborted database synchronization sequence number on the master switch. This allows subsequent database synchronization attempts to proceed without waiting for the standby switch to respond to the previously aborted synchronization attempt. **Scenario**: This issue was triggered when the standby switch database was out-of-sync with the master switch. Any switchover during this out-of-sync state caused the switch to be in an inconsistent state. This issue was observed on switches in a master-standby configuration and was not specific to a release version.

Mesh

Table 58: *Mesh Issues*

Bug ID	Description
92614	**Symptom**: A Mesh Point rebooted frequently as it could not connect to a Mesh Portal. **Scenario**: This issue occurred when the transmission power on the Mesh Point was very low compared to the configured power. This issue was observed in OAW-AP105 and OAW-AP175 access points with switches running AOS-W 6.1.x and later versions.

Mobility

Table 59: *Mobility Fixed Issues*

Bug ID	Description
88281	**Symptom:** IP mobility entries were not cleared even when the client leaves the switch and user entries aged out. Additionally, the command **clear ip mobile host <mac-address>** did not clear the stale entry. **Scenario:** This issue was caused by a message loss between the switch's Mobile IP and Authentication internal processes. This message loss caused the affected clients to become stuck. All switch models running AOS-W 6.3.x, 6.2.x, and 6.1.x were impacted by this issue.

Remote AP

Table 60: *Remote AP Fixed Issues*

Bug ID	Description
85473	**Symptom**: OAW-RAP3WN AP using a USB modem was unable to come up as an active AP until it rebooted. Changes to how the switch determines modem product IDs resolves this issue. As a result of this issue, the default dial string for a TATA photon plus Huawei E156 USB modem is changed from **AATTDDTT##777777** to **AATTDDTT**9999##**. **Scenario**: This issue occurred on a OAW-RAP3WN AOS-W AP running 6.2.1.2 when it was connected to a Huawei E156 modem.
86096	**Scenario:** DHCP clients connected to an AP received only the first entry of the DNS server list, even though the switch was configured with multiple DNS server IP addresses. With the new fix, DHCP clients get the complete list of DNS server IP addresses. **Scenario:** This issue was observed on switches running AOS-W 6.2.x when a user configured multiple DNS servers in local Remote AP (RAP) DHCP pool. This issue was observed when a user configured multiple DNS server in local Remote AP (RAP) DHCP pool, DHCP clients received only the first entry of the DNS server list. This issue was observed in switches running AOS-W 6.2 and later versions.
86650	**Symptom:** A switch sent continuous RADIUS requests for the clients connected behind the wired port of a remote AP (RAP). This issue is resolved by AOS-W enhancements that prevent memory corruption. **Scenario:** This issue was observed when a RAP used a PPPoE uplink and operated as a wired AP in split-tunnel or bridge mode. This issue occurred on AOS-W running 6.1.3.6, and was not limited to any specific switch model.
90355	**Symptom**: OAW-AP70 and OAW-RAP108 access points connecting to the network using a cellular uplink were not able to achieve a 3G connection. This issue is resolved by improvements to the AP boot process, and changes that allow cellular modems to support multiple ports on the AP. **Scenario**: This issue was observed in 6.3.x. and 6.2.x when OAW-AP70 and OAW-RAP108 access points connected to a Huawei® E220 Modem.

Voice

Table 61: *Voice Fixed Issues*

Bug ID	Description
74401 88173 88174	**Symptom:** Avaya® IP desk phones did not register in the switch and the **show voice call-cdrs** and **show voice-client status** commands displayed incorrect call status for these phones. Changes to the H.323 parser in the switch fixed the issue. **Scenario:** This issue was observed when an Avaya IP desk phone was connected to the wired port of an access point. This issue was observed on switches running AOS-W 6.2.x.
77716 88996 90000	**Symptom**: Incompatibility issues observed between OAW-4704 switches and a Cisco CUCM using SCCP version 20. Users were able to make and receive calls using a Cisco phone but there was no audio. This issue is resolved by changes to that allow the switch to handle Open Receive Channel Acknowledge (ORCA) messages for SCCP Version 20. **Scenario**: The Cisco CUCM was compatible with the Skinny Client Control Protocol (SCCP) version 20, while the OAW-4704 switch supported only up to version 17 of the SCCP. This incompatibility issue resulted in media traffic not passing through the OAW-4704 switch as it was not able to parse the SCCP signaling packets. This issue was observed in OAW-4704 switch running AOS-W 6.0 or later.
86683	**Symptom:** The **show voice call-cdrs** and **show voice client-status** command outputs did not display the call details for Lync wired clients with media classification configured on session ACL. This issue is resolved by ensuring to handle the message appropriately for wired clients. **Scenario:** This issue was observed when Lync clients were identified as voice clients via media classification. This issue occurred on AOS-W running 6.2.x and not limited to any specific switch version.
93517	**Symptom:** Access points rebooted unexpectedly resulting in wireless clients to lose network connectivity. Releasing CDR events for AP statistics and AP event in the CDR buffer resolved the issue. **Scenario:** This issue was observed in a VoIP deployment when the Station Management (STM) process that handles AP management and user association crashed on the switch. This issue was observed in switches running AOS-W 6.1 and later versions.

WebUI

Table 62: *WebUI Fixed Issues*

Bug ID	Description
88398	**Symptom:** The **Dashboard** > **Security** page of a switch did not allow network administrators to manually contain or reclassify a group of detected rogue APs. This issue is fixed by adding support to select multiple rogue APs. **Scenario:** This issue occurred when multiple rogue APs were selected in the **Dashboard** > **Security** page. This issue was observed in switches running AOS-W 6.2.1.3.
90110	**Symptom:** The AOS-W Campus WLAN Wizard was not accessible. **Scenario:** The Campus WLAN wizard was not accessible due to the presence of an ampersand (&) in the LDAP server filter. LDAP server filters can now include an ampersand. This issue was observed in OAW-4306G switch running AOS-W 6.2.1.3 but could impact any switch model.

Resolved Issues in AOS-W 6.2.1.4

The following issues were resolved in AOS-W 6.2.1.4:

802.1X

Table 63: *802.1X Fixed Issues*

Bug ID	Description
71930	**Symptom:** Client 802.1X authentication failed after the switch uploaded a new security certificate. This issue was the result of a rare condition where values in a RSA private key were less than 128 bytes in length, and is resolved by changes to the process by which the switch manages RSA keys. **Scenario:** This issue occurred on switches running AOS-W 6.1.3.2 in a master-local topology when the switches were updated with new certificates.
85896	**Symptom**: A switch rebooted after an internal switch module stopped responding. Internal memory improvements resolve this issue. **Scenario**: This issue was caused by memory corruption while the switch processed 802.1X packets in an error flow. It was observed in switches running AOS-W 6.1 or later, and is not specific to any switch model.
86162	**Symptom**: Clients using WPA2-PEAP authentication failed due to an EAP-failure error after the switch switched to a new 2k server certificate. This issue is fixed by changing the method in which RSA constants are handled. **Scenario**: This issue was triggered by some 2k server certificates. This issue was observed in OAW-4x04 Series and OAW-4306 Series switches running AOS-W 6.2.x.

AP-Datapath

Table 64: *AP-Datapath Fixed Issues*

Bug ID	Description
86469 89714	**Symptom:** An AP unexpectedly rebooted due to errors triggered by internal timers. Changes that prevent address bit flipping resolve this issue. **Scenario**: This issue was observed in OAW-AP120 Series access points associated to a switch that upgraded from AOS-W 6.1.3.7 to AOS-W 6.1.3.x.

AP-Regulatory

Table 65: *AP-Regulatory Fixed Issues*

Bug ID	Description
83338	**Symptom:**OAW-AP93 access points configured to use the regulatory maximum transmission power displayed mismatching EIRP and the maximum EIRP values in the output of the **show ap active** and **show ap radio-summary** commands. An improvement to the algorithm used to determine the regulatory limit resolves this issue. **Scenario:** This was observed on OAW-AP93 access points, and was not limited to any specific release of AOS-W.

AP-Wireless

Table 66: *AP-Wireless Fixed Issues*

Bug ID	Description
81508	**Symptom:** Clients associated to OAW-AP93 access points configured as remote APs aged out and were deauthorized. This issue is resolved by additional checks in station ageout behavior that ensure clients are not aged out unnecessarily. **Scenario:** This was observed on OAW-AP93 access points running AOS-W 6.2.0.0.

ARM

Table 67: *ARM Fixed Issues*

Bug ID	Description
87026 86951	**Symptom:** The mode-aware Adaptive Radio Management (ARM) feature changed an unexpectedly high number of APs using the 5 GHz band into Air Monitors (AMs). This issue is resolved by improvements to interference idx calculations. **Scenario:** This issue occurred in a high density deployment when an AP radio was associated to multiple Virtual APs. It was triggered when the Signal-to-Noise Ratio (SNR) of the radio was counted many times when the neighbor's view of the coverage index was calculated. This issue was observed in AOS-W 6.2.1.2 and was not specific to any AP or switch model.

BaseOS Security

Table 68: *BaseOS Security Fixed Issues*

Bug ID	Description
81390	**Symptom**: When clients connected using EAP-TLS authentication, the following error message appeared in the switch error log files: **<ERRS> |authmgr| user.c, derive_role2:5759: {04:f7:e4:26:c3:fb-??} Missing server in attribute list, auth=802.1x, utype=L2**. Improvements in the process that manages server names resolves this issue. **Scenario**: This issue was observed when Common Name (CN) lookup was disabled in the client certificate. The issue was not specific to any AOS-W version or switch model.
92817	**Symptom**: Wireless clients were blacklisted even when the rate of the IP Session did not exceed the threshold value set. This issue is resolved by increasing the storage of the threshold to 16 bits. **Scenario**: This issue was observed if the threshold of the IP Session rate was set to a value greater than 255. This issue was observed in switches running AOS-W 6.x.

Captive Portal

Table 69: *Captive Portal Fixed Issues*

Bug ID	Description
87294	**Symptom**: When user role was assigned by a captive portal profile, the ACL configuration synchronized from a master switch to a standby switch did not include the captive portal whitelist. This issue is resolved by the addition of internal checks that verify that a configured whitelist is correctly attached to the user role. **Scenario**: This issue was identified in a network topology with a master switch, standby switch and four local switches running AOS-W 6.2.1.2.

Switch-Datapath

Table 70: *Switch-Datapath Fixed Issues*

Bug ID	Description
84071	**Symptom**: A switch stopped responding and unexpectedly rebooted. The log files for the event listed the reason for the reboot as **Datapath exception**. Improvements to how frame headers are managed resolve this issue. **Scenario**: This issue occurred when an SSL-encapsulated invalid ESP frame was received and processed by the switch. It occurred on OAW-4x04 Series and OAW-4550/4650/4750 Series switches running AOS-W 6.2.1.0.
83029	**Symptom**: OAW-4550/4650/4750 Series or OAW-4x04 Series switch with the firewall-visibility feature enabled failed to respond when the switch had a high number of IPv6 sessions. This issue is resolved by improvements to IPv6 session management. **Scenario**: This issue occurred on a switch running AOS-W 6.2.1.0. The datapath CPUs utilization reaches 100% and fails to return to nominal levels.

Switch-Platform

Table 71: *Switch-Platform Fixed Issues*

Bug ID	Description
85398	**Symptom:** A switch configured as a DNS server responded to DNS queries, even if the IP domain lookup and captive portal redirect features were disabled. This issue is resolved by a change that prevents the switch from providing DNS services when DNS hostname translation is disabled using the **no ip domain lookup** command. **Scenario:** This issue occurred on OAW-4604 switch configured to operate as a DNS server while running AOS-W 6.1.3.6.
85685	**Symptom:** OAW-S3 switch module running AOS-W 6.1.3.8 stopped responding and rebooted. The log files for the event listed the reason for the crash as **fpapps: Segmentation fault**. The internal fpapps process handles the VLAN interfaces on the switch. Changes to the internal fpapps process fix the issue. **Scenario**: This issue was observed when the VLAN interface on the switch constantly changed between an UP and DOWN state, resulting in a VRRP status change. This issue is not limited to any specific switch model or software version.
86266	**Symptom**: In rare cases, issuing commands through a telnet shell caused an internal switch process to stop responding, triggering an unexpected switch reboot. This issue is resolved by changes that prevent AOS-W from referencing null pointers within the software. **Scenario**: This issue was triggered by varying sequences of commands issued via the telnet shell, and is not specific to any switch model or software version.

Table 71: *Switch-Platform Fixed Issues*

Bug ID	Description
87721 88368 89434 89441 89742 89924 90029 90059 90492 90634 91777 92675 94053	**Symptom**: When the switch performs an SNMP walk on a voice client, an internal switch process that manages client stations stopped responding. Changes to how SNMP entries are deleted resolve this issue. **Scenario**: This issue occurred on a switch running AOS-W 6.3.x and AOS-W 6.2.x, with voice clients connected to the switch using a wired connection.
87794 88311 88360 88683 88740 88505 88833	**Symptom**: OAW-4550/4650/4750 Series switch unexpectedly rebooted. Switch log files listed the reason for the event as a **datapath timeout**. Improvements to how tunnels are created in the internal switch datapath resolve this issue. **Scenario**: This issue occurred in OAW-4550/4650/4750 Series switches running AOS-W 6.2.1.x.

Intrusion Detection System

Table 72: *Intrusion Detection System Fixed Issues*

Bug ID	Description
86681	**Symptom:** The IDS (Intrusion Detection System) feature frequently triggered false alarms. AOS-W resolves this issue by changing the default setting for the IDS Large Duration Attack Detection feature from **enabled** to **disabled**. **Scenario:** This issue occurred because legitimate frames sent with a large duration were also treated as an IDS Large Duration attack, triggering false alarms.

Mobility

Table 73: *Mobility Fixed Issues*

Bug ID	Description
88063	**Symptom**: If a switch uses the IP mobility feature and RADIUS server vendor specific attributes (VSAs) to derive a user role for RADIUS-authenticated clients, the user role assigned to the client at its home agent (HA) can incorrectly change to the default AAA profile role after that client roams to a foreign agent (FA). This issue is resolved by improvements to mobile IP role management. **Scenario**: This issue occurs when a client with a VSA-derived user role roams between switches in an IP mobility domain. It is triggered when a user gets a dynamically assigned role from a foreign agent, and that role is not present on the client's home agent. As a result, the client gets assigned the default AAA profile role when it roams back to its home agent.

WebUI

Table 74: *WebUI Fixed Issues*

Bug ID	Description
73459	**Symptom:** The output of the **show acl hits** CLI command and the **firewall hits** information that appears on the **UI Monitoring** page of the switch WebUI displayed conflicting information. **Scenario:** This issue was triggered by formatting errors in the XML response from the switch to the WebUI that appeared when the output was larger than a specified limit. This issue was not limited to any specific switch model or software version.
80233 82724 83235 83949 84159 85375 85445 85686 85805 86423 86424 86632 86839 86933 87335 87933 88826 89523 91212	**Symptom**: The **Monitoring** > **Access Points** and **Monitoring** > **Network** > **All Access Points** pages of the switch WebUI showed APs as DOWN, even when the status of the AP is UP in the command-line interface. This issue is resolved by improving internal processes that handles AP IP addresses. **Scenario**: This issue occurred on a master/local topology with one OAW-6000 master switch and two local switches running AOS-W 6.2.1.0.

Resolved Issues in AOS-W 6.2.1.3

The following issues are resolved in AOS-W 6.2.1.3:

Air Management - IDS

Table 75: *Air Management - IDS Fixed Issues*

Bug ID	Description
84889	**Symptom:** False alarms for AP spoof detection were observed in AOS-W 6.2.1.2. This issue is resolved by removing the **Detect AP Spoofing** check that looks for frames sent to the AP on the wrong channel. **Scenario:** This issue occurred when the **Detect AP Spoof** option was enabled in the **Configuration** > **Wizards** > **Configure WIP** page of the WebUI. This issue was not specific to any software version.

AP-Platform

Table 76: *AP-Platform Fixed Issues*

Bug ID	Description
64778 63852 84004	**Symptom:** Users were unable to make calls to IP phones. This issue is fixed by increasing the maximum acceptable frame size to 1518 bytes in OAW-RAP3WN AP's Ethernet driver. **Scenario:** This issue occurred when the IP phone was connected to the Ethernet interface of OAW-RAP3WN AP, and was observed in AOS-W 6.2.1.1.
85397 78289	**Symptom:** An internal switch module stopped responding when a client disconnected. This issue is resolved by changes to references to objects in memory after the switch frees and allocates memory to another object. **Scenario:** This issue was triggered by aggressive client station roaming and power save settings, and was not specific to any software version.

AP-Datapath

Table 77: *AP-Datapath Fixed Issues*

Bug ID	Description
85279	**Symptom:** In a master-local topology, all users connected to an AP in bridge or split-tunnel forwarding mode experienced low throughput even though bandwidth contracts were not configured. This issue is resolved by correcting the role-to-bandwidth-contract mapping table. **Scenario:** This issue occurred on switches running AOS-W 6.2 or later, due to incorrect mapping of a user role to the bandwidth contract when the ACL IDs in the master and local switches were different for the same role. It was also observed during an authentication process restart.

AP-Regulatory

Table 78: *AP-Regulatory Fixed Issues*

Bug ID	Description
76222	**Symptom:** The country code for Algeria was not supported on OAW-AP105, OAW-AP92, and OAW-AP93 access points. The country code for Algeria is added in the country list for these APs to fix this issue. **Scenario:** This issue was observed in AOS-W 6.2.1.0 and was not limited to a switch model.

AP-Wireless

Table 79: *AP-Wireless Fixed Issues*

Bug ID	Description
85806	**Symptom:** Excessive jitter was observed in Blackberry devices making voice calls when the switch enabled the Wireless Multimedia UAPSD (Unscheduled Automatic Power Save Delivery) option from the **Configuration** > **Wireless** > **AP Configuration** > **Select AP** > **SSID** profile > **Advanced** tab in the WebUI. This issue is fixed in AOS-W 6.2.1.3 by enhancing the packet queuing mechanism for UAPSD hardware transmit queues, reducing packet loss. **Scenario:** This issue was triggered by high packet loss in a UAPSD-enabled configuration. This issue was observed in OAW-AP124, OAW-AP125, and OAW-AP105 access points running AOS-W 6.1.3.6.

BaseOS Security

Table 80: *BaseOS Security Fixed Issues*

Bug ID	Description
72093	**Symptom:** A switch did not display a portion of the output of the **show run result** command when it is sent using SSH/telnet connections to a teraterm client. An increase in the socket buffer size resolves this issue. **Scenario:** This issue was not limited to a specific switch model or software version.
80006 85167	**Symptom:** The internal switch module that manages authentication stopped responding. Enhancements to the internal code that provide valid values to the authentication process fixes this issue in AOS-W 6.2.1.3. **Scenario:** This issue occurred when XML API was used to add or modify a user with a session timeout configured on for that user. The issue was not specific to a switch model or a software version.
80805 81775 85642	**Symptom:** Some wireless users were displayed as wired users with an incorrect tunnel ID in the user table. Disabling the **wired-ap** parameter in the **ap-group** profile fixes this issue in AOS-W 6.2.1.3. **Scenario:** This issue occurred when some APs rebootstrapped and the **wired-ap** parameter was enabled in the **ap-group** profile. This issue was not specific to any switch model or a software version.
81458	**Symptom:** Wired user-entries were displayed in the user-table even though wired users were not connected to any of the APs. This issue is resolved by clearing the entries for the table which tracks the ap-wired ports in the authentication module when an internal module (STM) was restarted. **Scenario:** This issue occurred when the user entries for ap-wired ports were not cleared in the table if the internal switch module that handles client stations restarted. The issue was not specific to a switch model or a software version.
83776	**Symptom:** Atheros clients did not support multiple relay counters using WPA-TKIP encryption and were unable to connect to the network after upgrading to AOS-W 6.1.3.8. This issue is fixed by disabling the use of a multiple Traffic Identifier (TID) for WPA-TKIP. **Scenario:** This issue was observed when Wireless Multimedia Extensions (WMM) was enabled and the atheros clients did not support multiple relay switches.
84628 86814	**Symptom:** OAW-6000 switch unexpectedly rebooted. Log files for the event listed the reason for the reboot as **Datapath timeout**. This issue is resolved by validating the bridge entries for VoIP clients. **Scenario:** This issue occurred when an invalid bridge value was computed and stored in an internal switch module. This issue is occurred in Alcatel-Lucent OAW-6000 switches running AOS-W 6.2.0.0.
85519	**Symptom:** One or more SSH (Secure Shell) sessions to a switch failed when multiple simultaneous SSH sessions occurred. This issue is resolved by updates that ensure every SSH Daemon process corresponding to a SSH login session uses a different IPC (Inter-Process Communication) port number. **Scenario:** This issue was triggered by sshd processes using the same IPC port number, causing collisions when multiple SSH sessions tried to authenticate. This issue was observed in AOS-W 6.1.x and 6.2.x.

Switch-Datapath

Table 81: *Switch-Datapath Fixed Issues*

Bug ID	Description
81214 82914 85597 87043 87338	**Symptom:** High central processing unit (CPU) utilization on a network processors resulted in loss of IP connectivity for some users. The issue is resolved by fixing the automatic update of the clients route cache entries. **Scenario:** This issue was caused by a loop while routing L2 Virtual Local Area Network (VLAN) traffic. It was observed on switches running AOS-W 6.2 and routing L2 VLAN traffic.

Switch-Platform

Table 82: *Switch-Platform Fixed Issues*

Bug ID	Description
80956 81014 81555 83239	**Symptom:** A switch crashed and rebooted after upgrading from AOS-W 6.1.3.6 to 6.1.3.7. The log files for the event listed the reason for the crash as **watchdog timeout**. The interrupt handler for packet parsing is modified to ensure that CPU is not overwhelmed with traffic packets. **Scenario:** A race condition triggered the switch crash in a high-traffic deployment. This issue was not specific to any switch models.
83738	**Symptom:** A crash was observed in all APs associated to the local switch, followed by Access Control Lists (ACLs) configuration loss. Updates to the banner delimiter fixes this issue. **Scenario:** This issue was caused by banner message-of-the-day (motd) with an exclamation point (!) as a delimiter, because the same character **!** is used to exit from a sub-mode command. The issue was not limited to a specific versions of AOS-W.
84825	**Symptom:** OAW-4306G switch crashed or failed to respond. This issue is resolved by adding checks to deny access to invalid DRAM channels for the OAW-4306G switch. **Scenario:** This issue was observed on a OAW-4306G switch running AOS-W 6.1.3.7.

DHCP

Table 83: *DHCP Fixed Issues*

Bug ID	Description
77280	**Symptom:** When the **show running-config** command was executed, the **Module DHCP Daemon is busy. Please try later.** error was observed. This issue is resolved by modifying the DHCP pool user options. **Scenario:** This issue was observed when switches configured with DHCP pools, used non-alphanumeric characters in the pool name. As a result, an error in the syntax was observed when the DHCP user options were generated in the configuration file.

Local Database

Table 84: *Local Database Fixed Issues*

Bug ID	Description
84494	**Symptom:** A switch unexpectedly rebooted. The log files for the event listed the reason for the reboot as **Nanny rebooted machine - udbserver process died**. This issue is resolved by improvements to how MYSQL database failures are handled, in that AOS-W better validates returned values and checks for missing values in certain failure scenarios. **Scenario:** This issue occurred on a standalone master OAW-4550 switch with one associated OAW-AP135 access point.

OSPF

Table 85: *OSPF Fixed Issues*

Bug ID	Description
82730	**Symptom**: A switch failed to add the default route when a neighboring router advertised the default route. This issue is resolved by ensuring that the default route is not missed while adding the route information. **Scenario**: This issue was not limited to a specific switch model and was observed in AOS-W 6.2.1.0.

Remote AP

Table 86: *Remote AP Fixed Issues*

Bug ID	Description
74024	**Symptom:** When a client sent DHCP packets with 802.1X packets, an IP address was returned even if 802.1X was not authenticated. As a result, the slot port information displayed in the user table was incorrect for wired users connected to a remote AP. This issue is resolved by updating the slot/port with the correct information. **Scenario:** This issue was observed in AOS-W switches, and OAW-RAP3WN, and OAW-RAP5 access points.
78914	**Symptom:** Stale user entries are present in the switch when a user moves from one AP coverage to another, if the new AP has a different VLAN configuration for the same Extended Service Set Identification (ESSID). This issue is resolved by removing the split-tunnel mobility that triggered the error. **Scenario:** This issue occurs if the first AP deletes the user entry without notifying the switch when the user moves from one AP to another. This issue was observed in APs running AOS-W versions prior to 6.2.1.3.
81245	**Symptom**: The user table contained stale entries for users that aged out or disassociated from the network. Internal improvements to the user table resolve this issue. **Scenario**: This issue occurred when users associated to a AP in split-tunnel forwarding mode and used captive portal authentication roam to multiple APs exhibiting the same ESSID.
84752 84391 84893 85160 85629 86217 86339 86372 86375 86738 86742 89701	**Symptom:** Campus APs (CAPs) and Remote (RAPs) rebooted after upgrading the software to AOS-W 6.2.1.3. Memory improvements resolve this issue. **Scenario:** This issue was triggered by to insufficient memory and was not specific to any switch or AP model.
85499	**Symptom**: In some instances, calls from IP phones connected to OAW-RAP3WN AP failed because the AP dropped packets. VLAN tagging improvements resolve this issue. **Scenario**: This issue occurred on IP phones connected to an AP in tunnel forwarding mode, and was first identified in AOS-W 6.2.0.2.
85053	**Symptom**: A switch frequently stopped responding and rebooted in a topology with split-tunnel wired users in a configuration with the RADIUS accounting enabled. This issue occurred in Alcatel-Lucent OAW-6000 switches running AOS-W 6.2.1.1. **Scenario**: This issue was identified in AOS-W 6.2.1.1, when a RADIUS server was configured on the switch.

RADIUS

Table 87: *RADIUS Fixed Issues*

Bug ID	Description
84060 85623	**Symptom:** The source interface for a RADIUS server configured at a global level was not available after the switch rebooted. Changes that prevent source interface values from being lost after a reboot resolve this issue. **Scenario:** This was an intermittent issue and was not limited to a specific switch model or software version.
85277	**Symptom:** The **AvgRspTm** field in the output of the **show aaa authentication-server radius statistics** command was incorrectly set to 0 in a software image for OAW-4550/4650/4750 Series switch. This issue is resolved by changing parts of the software which were initially specific only to the OAW-S3 switch module platform, allowing the value of the **AvgRspTm** field to correctly update, and increasing switch stability. **Scenario:** This issue was identified in an AOS-W 6.2.1.1 software image for OAW-4550/4650/4750 Series switch, when a RADIUS server was configured on the switch.

Role/VLAN Derivation

Table 88: *Role/VLAN Derivation Fixed Issues*

Bug ID	Description
77242	**Symptom:** Changes to the AOS-W External Service Interface (ESI) Syslog parsing rule were not reflected in the user table. Also, the changes to a user role was reflected only in the system table and switch datapath. This issue is fixed by updating the user table with the ESI role-change. **Scenario:** This issue was observed in switches and APs running AOS-W 6.1.3.x.

SNMP

Table 89: *SNMP Fixed Issues*

Bug ID	Description
77584 81499	**Symptom**: An SNMP get request to poll *sysExtCardStatus* for the operational status of any installed cards could return the message “No such instance currently exists at this OID” and trigger an alert. Improvements to SNMP polling allow a get request to *sysExtCardStatus* to display the cached information from the previous poll status instead of an error message. **Scenario**: This issue was identified in AOS-W 6.1.2.5, and occurred when the SNMP request was issued while the internal switch hardware monitor polled for hardware status. The SNMP request would time out, but the switch would return the error message instead of a timeout message.

Station Management

Table 90: *Station Management Fixed Issues*

Bug ID	Description
83091 83547	**Symptom:** Active APs of a local switch were not displayed on the master switch when the local switch showed the APs were active on the master switch. A change that introduces a new action to handle the race condition fixes this issue. **Scenario:** This issue was triggered by a race condition which resulted in creating session entries before IPSec tunnel and Network Address Translation (NAT) rules were created. The session removal mechanism could not remove the session entries without NAT flags. This issue was observed in switches running AOS-W 6.2.1.0.
84718 84719 84725	**Symptom:** The internal switch module that manages station authentication stopped responding and temporarily prevented clients from associating to the network. This issue is resolved by adding validations to prevent this switch module from crashing. **Scenario:** This issue was not limited to a specific switch model or release version.

Voice

Table 91: *Voice Fixed Issues*

Bug ID	Description
83517 84723	**Symptom:** The process that handles the AP management and user association crashed when voice clients were cleared. This impacted all the wireless clients and voice clients associated to the switch. Enhancements to the internal code fixed this issue in AOS-W 6.2.1.3. **Scenario:** This issue occurred when the voice clients (SIP, H323, and SCCP) that were created as servers were getting deleted twice at every client timeout. This issue was observed on switches running AOS-W 6.2.1.1.

WebUI

Table 92: *WebUI Fixed Issues*

Bug ID	Description
77933 85051 85740	**Symptom:** The firewall rule count was not displayed correctly in the **Configuration** > **Security** > **User Roles** > **Edit Role <role_name>** page of the WebUI. Modifications to the parsing and calculation logic fixed this issue and now the WebUI displays the accurate firewall rule count. **Scenario:** The incorrect rule count was triggered by an issue in the parsing logic and calculation. This issue was observed in OAW-S3 switches in a master-local topology running AOS-W 6.1.3.5 and 6.2.1.1.
84387	**Symptom:** Clicking on the **Locate** button in the **Security** page for **Valid Clients** displayed the **Internal error while executing query** error. This issue is resolved by generating the correct locate query for the filter related to the client. **Scenario:** This issue was not limited to a specific switch model or release version.
83744 85222 85646	**Symptom**: Changes to the account start and end date fields did not take effect when adding a new guest user. **Scenario**: When the administrator changed the account start and end date fields under **Guest User** page of the switch's WebUI, the changes did not take effect. This issue was not limited to a specific switch model and was observed in AOS-W 6.2.1.2 and later versions.

Table 92: *WebUI Fixed Issues*

Bug ID	Description
85229	**Symptom**: The **Security Summary** page in the WebUI timed out as the event table in the WMS database became very large. This issue is resolved by enabling periodic clean-up of the WMS event table entries. **Scenario**: This issue was observed when too many APs where terminating on a switch. This issue was not limited to any specific switch model.
85784 76383	**Symptom:** The **Dashboard** > **Security** page of the WebUI was not loaded in Microsoft IE 8 (Internet Explorer) or lower versions and displayed a JavaScript error. This issue is fixed in AOS-W 6.2.1.3 for all the browsers. **Scenario:** This issue was triggered by JSON (JavaScript Object Notation) parser in IE. This issue was observed in AOS-W 6.2.1.2 and not specific to any switch or release version.

Resolved Issues in AOS-W 6.2.1.2

The following issues were resolved in AOS-W 6.2.1.2:

802.1X

Table 93: *802.1X Fixed Issues*

Bug ID	Description
83375	**Symptom:** Client failed to connect to Lightweight Extensible Authentication Protocol (LEAP) SSID when operation mode was set to Dynamic-WEP and Use Session Key was enabled on the client. The issue occurred when some of the clients failed to negotiate a separate session key. Enhancements in the security protocols fixed this issue in AOS-W 6.2.1.2. **Scenario**: This issue was observed in switches running AOS-W 6.2.1.0 and was not specific to any switch model.

AP-Platform

Table 94: *AP-Platform Fixed Issues*

Bug ID	Description
71978 75776	**Symptom**: An AP model OAW-AP68 unexpectedly rebooted due to a memory corruption. Memory improvements fixed this issue in AOS-W 6.2.1.2. **Scenario**: This issue was observed in an OAW-AP68 running AOS-W 6.2.0.0.

AP-Wireless

Table 95: *AP-Wireless Fixed Issues*

Bug ID	Description
82493	**Symptom:** An AP crashed when a virtual AP configuration changed any downlink traffic from an AP to its associated the clients. Checks are added to the code to prevent and resolve this issue. **Scenario:** This issue is not specific to any AP model, and was identified in AOS-W 6.1.3.7.

BaseOS Security

Table 96: *BaseOS Security Fixed Issues*

Bug ID	Description
55419 65936 79704	**Symptom**: An internal AOS-W process (Certmgr) became busy when the OCSP server is unreachable. The issue is fixed by changes to the OCSP code base. **Scenario**: Users were unable to authenticate because this process was busy queuing the OCSP requests (clients using 802.1X, IKE, and management authentication can be affected). This issue was observed in AOS-W 6.2.x.
68581	**Symptom:** When a mobile client roamed from a home agent (HA) switch to a foreign agent (FA) switch, issuing the CLI command **show user-table** from the FA switch incorrectly showed the client in an authenticated/derived role, whereas the output of the **show datapath user** command correctly showed the client in its dynamic role. The output of the **show user-table** command now shows correct information. **Scenario:** This issue was triggered when a mobile client roamed to a foreign agent switch running AOS-W 6.2.x, and is not limited to any specific switch model.
83620 84429	**Symptom:** Clients using Temporal Key Integrity Protocol (TKIP) or Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) suddenly stopped receiving traffic.This issue is resolved by improvements to the process by which AOS-W manages counters when new keys are installed. **Scenario:** This issue was observed on OAW-4550/4650/4750 Series switches running AOS-W 6.2.1.1.
81426	**Symptom:** A memory leak was observed in wired clients with RADIUS accounting enabled. This issue is resolved by freeing the memory allocated for RADIUS context when a user was deleted. **Scenario:** This issue was observed when wired clients were connected to the APs with RADIUS accounting enabled on AAA profile. This issue was not specific to any switch model.
84077	**Symptom:** A switch unexpectedly rebooted. The log files for the event listed the reason for the reboot as **Crypto Post Failure**. This issue is resolved by enabling logs for the error message without automatically reloading the switch. **Scenario:** This issue is not specific to any switch model.

Command Line Interface

Table 97: *Command Line Interface Fixed Issues*

Bug ID	Description
62292	**Symptom**: The switch stopped responding and rebooted due to an internal process failure. Changes to the way the command **show hostname** handles filters fixes the issue. **Scenario**: When users executed the command **show hostname | include <filter>**, an internal process failed, causing the switch to crash. The issue was not specific to a switch model or a software version.

Control Plane Security

Table 98: *Control Plane Security Fixed Issues*

Bug ID	Description
66413 67875 68010	**Symptom**: Occasionally, the control plane security (CPsec) whitelist database entries did not synchronize between the master and local switch. AOS-W 6.2.1.2 transmits smaller sized CPsec records. resolving the issue. **Scenario**: This issue was observed when the CPsec whitelist database size was large. A lossy network between the master and local switch caused some whitelist synchronization fragments to be lost. This issue was not limited to a specific switch model or release version.

Switch-Datapath

Table 99: *Switch-Datapath Fixed Issues*

Bug ID	Description
80625	**Symptom:** A switch unexpectedly rebooted. Log files for the event listed the reason for the reboot as a Datapath timeout due to change in the tunnel MTU while processing a frame. This issue is resolved by ensuring that the same tunnel MTU is used for processing a given frame. **Scenario:** This issue was observed when tunnels were used on switches running AOS-W 6.1.3.x or later.
83216	**Symptom**: A switch generated proxy ARP responses out of the same trusted port from where it the switch learned the MAC address. Disabling the option **bcmc-optimization** in the VLAN interface resolves the issue. **Scenario**: The issue occurred when the trusted port was a port channel and the **bcmc-optimization** option was enabled on the VLAN interface. The issue was not specific to a switch model or a software version.
83409	**Symptom:** A switch rebooted due to missing heartbeats, and log files for the event listed the reason for the reboot as **watchdog timeout**. This issue is resolved by improvements to the communication infrastructure. **Scenario:** This issue was observed when a huge traffic hit the control plane causing loss of acknowledgments in the communication infrastructure. This is not specific to any switch model.

Switch-Platform

Table 100: *Switch-Platform Fixed Issues*

Bug ID	Description
79719 81014 81086 81087 81181 81207 81368 81393 81479 81669 81853 82085 82232 82645 82708 82835	**Symptom:** A switch crashed and rebooted frequently after upgrading the software from AOS-W 6.1.3.6 to AOS-W 6.1.3.7. Improvements to packet processing fix this issue in AOS-W 6.1.3.7. **Scenario:** A high amount of control traffic triggered this issue, which is not specific to any switch model.
80326 80780 81399 81462 82385 82775	**Symptom:** A switch failed to respond and rebooted without saving crash log tar files after upgrading to AOS-W 6.1.3.7. The log files for the event listed the reason for the reboot as **Control Processor Kernel Panic**. This issue is resolved by improvements to the way internal datapath information is sent to the control plane security process in the event of a datapath module failure. **Scenario:** This issue was first observed in AOS-W 6.1.3.7.

Switch-Software

Table 101: *Switch-Software Fixed Issues*

Bug ID	Description
84622	**Symptom:** Bridge Protocol Data Units (BPDUs) in tagged VLANs were not flooded by the switch when spanning tree is disabled on the switch. Improvements to how process packets with a BDPU MAC address are handled resolves this issue. **Scenario**: This issue occurred when spanning tree was disabled on the switch and spanning tree was enabled on the uplink switch on the tagged vlan.

IPv6

Table 102: *IPv6 Fixed Issues*

Bug ID	Description
76426 78962	**Symptom**: An increase in CPU utilization by the user authentication process was observed on the switch. Creating a rule in the valid user Access Control List (ACL) to deny packets from the host source IPv6 address fe80::/128 fixed this issue in AOS-W 6.2.1.2. **Scenario**: This issue was triggered when an HTC One X smartphone running Android version 4.1.1 generated a link-local IPv6 address fe80::/128, resulting in an increased CPU utilization on the switch. This issue was not limited to any specific version of AOS-W.
79452 77012	**Symptom**: IPv6 traffic from L3 mobility clients sent from a foreign agent (FA) to a home agent (HA) was double encrypted and sent through an IPSec tunnel instead of a Generic Routing Encapsulation (GRE) tunnel without encryption. AOS-W 6.2.1.2 updates the packets with tunnel flag so that data traffic doesn't get double encryption in an IPSec tunnel. **Scenario**: This issue was triggered by an internal flag that determines whether the packets parsed into the GRE tunnel should be encrypted. This issue was observed in all switch platforms running AOS-W 6.2.x.

Mobility

Table 103: *Mobility Fixed Issues*

Bug ID	Description
82673	**Symptom:** DHCP packets from the clients at foreign agent were getting redirected through IPIP tunnel due to wrong order of the ACL. This caused a delay in allocating a valid IP address to the clients. This issue is resolved by correcting the order of the ACL. **Scenario:** This issue was observed when L3 mobility was enabled on switches running AOS-W 6.1.x.

RADIUS

Table 104: *RADIUS Fixed Issues*

Bug ID	Description
76484	**Symptom:** RADIUS authentication failed in networks that had different Maximum Transmission Values (MTUs). **Scenario:** The RADIUS authentication failed when the MTU value in the network between the switch and RADIUS server was different. This issue was observed in switches running AOS-W 6.2.1.2 or earlier and was not specific to any switch model.

SNMP

Table 105: *SNMP Fixed Issues*

Bug ID	Description
77225 82330 82560 88618	**Symptom**: OAW-4x04 Series switch running AOS-W 6.2.1.0 was unable to use an SNMP MIB walk to determine values in the table wlsxSysXMemoryTable. Improvements to how file descriptors are managed resolve this issue. **Scenario**: This issue was triggered by an SNMP MIB walk on OAW-4x04 Series switch.

Voice

Table 106: *Voice Fixed Issues*

Bug ID	Description
78034	**Symptom**: A client connected to a 3G uplink port was unable to connect to the Internet when the option **firewall session-tunnel-fib** was enabled. The issue is fixed by changing a flag set in the route cache entry and adding the static ARP entry. **Scenario**: When an uplink port on the switch was connected via 3G link, a NAT client was not able to connect to the Internet. The issue was not specific to a switch model or a software version.
81487 83707 83757 84631	**Symptom:** Voice clients registered as SIP clients were overridden with the application-level gateway (ALG) value as Vocera or New Office Environment (NOE). This issue is resolved by improvements that prevent subsequent updates to the initially configured ALG value. **Scenario:** This issue was observed in OAW-4550/4650/4750 Series switches running AOS-W 6.1.3.3 or later.

WebUI

Table 107: *WebUI Fixed Issues*

Bug ID	Description
76451	**Symptom:** When guest users were imported using a .CSV file in the **Configuration** > **Security** > **Authentication** > **Internal DB** > **Guest User** page of the WebUI, the sponsor's email address was not imported. **Scenario**: The issue was observed in switches running AOS-W 6.1.3.4 and 6.2.x.
80269	**Symptom:** The Gigabit Ethernet interface 10 option was missing in the VRRP tracking Interface drop-down under **Advanced Services** > **Redundancy** > **Add virtual Router** > **Tracking Interface table** of the WebUI. AOS-W 6.2.1.2 now includes the Gigabit Ethernet interface 10 option in the VRRP tracking Interface. **Scenario:** This issue was observed in OAW-S3 switch modules running AOS-W 6.1.3.1.
82959	**Symptom:** User was not able to navigate to the fields properly using the tab key in the **Configuration** > **Security** > **Authentication** > **Internal DB** > **Guest User** page of the WebUI and use the options: **create New**, **import**, **delete**, **print**, and **cancel**. Adding code to the guest provisioning page to create an appropriate tab index for new, import, and edit windows fixed this issue in AOS-W 6.2.1.2. **Scenario:** This issue was observed in AOS-W 6.2.x and is not specific to any switch model.

Resolved Issues in AOS-W 6.2.1.1

The following issues were resolved in AOS-W 6.2.1.1:

802.1X

Table 108: *802.1X Fixed Issues*

Bug ID	Description
77154	**Symptom:** If the **Use Server provided Reauthentication Interval** setting was enabled in an AP's 802.11X authentication profile, clients associated with that AP did not reauthenticate when the client roamed to a different AP. This issue is resolved by a change that allows the switch to store the session timeout reauthentication interval returned from the RADIUS server. **Scenario:** This issue occurred in AOS-W 6.1.2.4, when clients authenticating with a RADIUS server roamed between APs.
80841	**Symptom:** A switch configured to use both 802.1X and MAC authentication ignored the **eapol-start** request sent by client before the completion of the MAC authentication process, Improvements to how the key cache is managed during the MAC authentication process fix this issue in AOS-W 6.2.1.1. **Scenario:** When MAC authentication and 802.1X is configured and an **eapol-start** request from the client came between MAC authentication and 802.1X authentication, the 4-way key exchange was started instead of full 802.1X authentication. This issue was observed in switches running AOS-W 6.1.3.5.

Air Management - IDS

Table 109: *Air Management - IDS Fixed Issues*

Bug ID	Description
81073	**Symptom**: An Air Monitor (AM) stopped scanning when it had been up for more than 50 days. This uptime threshold was reached when the AM's milli-tick counter, which counts the uptime in milliseconds, rolled over and the counter returned to zero. **Scenario**: This issue was identified on AOS-W 6.1.3.2 and was not limited to a specific switch or AP model. This rollover is expected behavior and a side effect of the roll over caused the issue. A fix has been made to check for and correctly handle the rollover to avoid this issue.

AMON

Table 110: *AMON Fixed Issues*

Bug ID	Description
81759	**Symptom:** Upon upgrade to AOS-W 6.2.0.2, a switch rebooted unexpectedly due to an internal process (fw_visibility) crash. This issue is resolved in AOS-W 6.2.1.1. **Scenario:** This issue was identified on AOS-W 6.2.0.2 and not limited to any specific switch model.

Resolved Issues in AOS-W 6.2.1.0

The following issues were resolved in AOS-W 6.2.1.0:

3G/4G

Table 111: *3G/4G Fixed Issue*

Bug ID	Description
77928	**Symptom:** An AP failed to complete a DNS query when it was configured to use a UML290 USB modem uplink. Improvements to multicast IP address checks resolves this issue in AOS-W 6.2.1.0 **Scenario:** This issue occurred when a UML290 uplink was configured on an Instant AP that was provisioned to use a wired interface and a DNS host name for a VPN. Due to this issue, DNS host names could not be resolved on the IAP or its clients. This issue was identified on OAW-RAP3WN, OAW-RAP108 and OAW-RAP109 access points running AOS-W 6.2.0.0.

802.1X

Table 112: *802.1X Fixed Issues*

Bug ID	Description
77705 78658 78559	**Symptom:** Clients using WPA-TKIP encryption were unable to complete 802.1x authentication. Changes in how TX sequence numbers are reset resolves this issue. **Scenario:** This issue occurred on OAW-4550/4650/4750 Series switches running AOS-W 6.2.0.2.
79546	**Symptom:** An internal switch module stopped responding, causing the switch to unexpectedly reboot. The log file for the event listed the reason for the reboot as “datapath exception. Memory buffer improvements resolve this issue in AOS-W 6.2.1.0. **Scenario:** This issue occurred on OAW-S3 switches running AOS-W 6.1.3.7.

Air Management-IDS

Table 113: *Air Management-IDS Fixed Issues*

Bug ID	Description
76936	**Symptom:** Rogue APs operating in Greenfield mode were not contained by Air Monitors (AMs). Improvements to AP containment processes resolve this issue in AOS-W 6.2.1.0. **Scenario**: This issue was first identified in AOS-W 6.1.3.5, and was not limited to any specific switch or AP model.
76808	**Symptom:** Some internal processes on the switch were unusually busy, while overall CPU utilization remained within expected levels. AOS-W 6.2.1.0 introduces changes that prevent APs from sending excessive containment event messages to the switch, so these internal processes do not become overloaded. **Scenario**: This issue was triggered when the **wireless containment** parameter in the IDS General profile was set to **tarpit all-sta** or **tarpit-non-valid-sta**, and one or more IDS Protection features are enabled such that active containment occurred.

AP-Platform

Table 114: *AP-Platform Fixed Issues*

Bug ID	Description
76021	**Symptom**: A core file from an AP with a special character in the AP name included the special character in the core file name, causing TFTP dump servers to reject that file. AOS-W 6.2.1.0 resolves this issue by removing special characters from the core file name before it sends the file to the dump server. **Scenario**: This issue occurred when an internal process crashed on an AP, and a core file of troubleshooting data was sent to the dump server defined in the AP's system profile. This issue was seen on APs with one or more special characters in the AP name, and was not limited to a specific AP model.
77183	**Symptom:** OAW-AP61 associated with a OAW-4550/4650/4750 Series switch running AOS-W 6.2.0.1 unexpectedly rebooted. The log files on the switch listed the reason for the AP reboot as "watchdog timeout." Changes to channel reuse processing resolves this issue. **Scenario:** This issue occurred when the **RX Sensitivity Tuning Based Channel Reuse** setting in the dot11x radio profile was set to **dynamic**.
77645	**Symptom:** APs associated to OAW-4550/4650/4750 Series switch rebooted, forcing clients to reassociate. Changes in how the switch manages duplicate MAC addresses resolves this issue in AOS-W 6.2.1.0. **Scenario**: This issue occurred on OAW-4550/4650/4750 Series switch in a master-local topology where the APs failed over between two switches.

AP-Wireless

Table 115: *AP-Wireless Fixed Issue*

Bug ID	Description
77946	**Symptom:** AOS-W did not support mixed encryption modes for static-WEP and WPA-PSK-TKIP, or for dynamic-WEP and WPA-TKIP. This issue is fixed in AOS-W 6.2.1.0 and these combinations are now in the list of allowed modes. **Scenario:** When editing the SSID profile in the WebUI, the system displayed the error message "invalid opmode combination", even though dynamic-WEP WPA-TKIP was available for selection in the WebUI. This issue was observed in AOS-W 6.1 and later versions, and was not limited to any specific switch model.

Authentication

Table 116: *Authentication Fixed Issues*

Bug ID	Description
75665 75860	**Symptom:** A 3rd generation iPad running iOS 6.0.1 was incorrectly assigned to the default VLAN. Changes to how the switch manages PMKID data resolves this issue in AOS-W 6.2.1.0. **Scenario:** This issue occurred in AOS-W 6.1.3.5, when a Virtual AP was configured with both MAC authentication and 802.1x authentication, a VLAN derivation rule was configured on the MAC authentication server, and the derived VLAN was different from the default VLAN of the virtual AP.

BaseOS Security

Table 117: *BaseOS Security Fixed Issue*

Bug ID	Description
75754	**Symptom:** The user table showed that some 802.1X authenticated clients managed by an external XML-API server were using Web authentication, even though there was no captive portal authentication configured for those clients. This display issue is resolved in AOS-W 6.2.1.0. **Scenario:** This issue occurred on a switch configured with a 802.1X default role with an ACL that sent traffic through the GRE tunnel to a SafeConnect appliance. In this scenario, L3 authentication was managed by the SafeConnect XML API, which updated the user role to an L3-authenticated role.
76401 76403 82540 82060	**Symptom**: The internal switch module that manages handles user authentication stopped responding, preventing users from authenticating until the process automatically restarted. **Scenario**: This issue occurred on OAW-S3 switch module running AOS-W 6.2.0.2 in a master-local topology.

Switch-Datapath

Table 118: *Switch-Datapath Fixed Issues*

Bug ID	Description
75843 72359 73246 73256 74575 75700 75753	**Symptom:** Errors in the internal datapath module on a switch caused it to stop responding. The crash logs for this error listed the reason for the crash as **Datapath Timeout**. This issue is resolved in AOS-W 6.1.3.7 and AOS-W 6.2.1.0. **Scenario:** This issue occurred when aOAW-S3 switch experienced heavy traffic between the control plane module and the network.
77535 77537 77024	**Symptom:** Android, iOS, and Mac OS devices were incorrectly blacklisted, and the log files for the event listed the reason as IP spoofing. Improvements to the ARP-spoofing feature resolved this issue. **Scenario:** The iOS, Mac OS, and Android devices sent ARP packets to receive the MAC address of the gateway to all the networks. When the previously connected networks assigned these devices a leased out IP address, these clients were blacklisted.
76307	**Symptom:** A local switch crashed after a user added a VLAN ID in the master switch. Changes to how the switch decodes encrypted packets resolved this issue. **Scenario:** When a user added a VLAN ID to the master switch and executed the command `write-mem`, the local switch crashed due to an internal process failure. This issue was not specific to any switch or software version.
77484 78181 78667 78873 79682	**Symptom:** Under very high load conditions, the switch datapath module can prevent users from associating or prevent associated users from passing traffic. In most cases, the switch will automatically reboot to recover from this scenario. Improvements to this internal switch module resolves this issue. **Scenario:** This occurred on OAW-4550/4650/4750 Series switches running AOS-W 6.2.0.x.

Table 118: *Switch-Datapath Fixed Issues*

Bug ID	Description
77814	**Symptom:** Errors in the internal control plane module caused OAW-4x04 Series or OAW-S3 switch to unexpectedly reboot. The switch log files listed the reason for the reboot as **watchdog timeout**. Changes to CPU register access has resolved this issue in AOS-W 6.2.1.0 **Scenario:** This issue occurred on OAW-S3 or OAW-4x04 Series switches in a master-local topology running AOS-W 6.1.x.
78326	**Symptom:** A local OAW-S3 switch unexpectedly rebooted. The log files on the switch listed the reason for the reboot as **Datapath timeout.** Changes to unicast forwarding checks prevent this issue from occurring in AOS-W 6.2.1.0. **Scenario:** This issue was triggered when a switch that receives GRE-type PPP packets has a user role that enables source NAT.
78593 79897	**Symptom:** A switch running AOS-W 6.2.0.1 stopped responding and reset. The switch crash logs lists reason for the reboot as **User Reboot**. Improvements to how core dumps are managed resolves this issue. **Scenario:** This issue was observed in OAW-4550/4650/4750 Series switch in a master-local topology.

Switch-Platform

Table 119: *Switch-Platform Fixed Issues*

Bug ID	Description
62096	**Symptom:** OAW-S3 switches unexpectedly rebooted, and the log files for the event listed the reason as “User pushed reset”. This issue is resolved in AOS-W 6.2.1.0. **Scenario:** This issue was observed on aOAW-S3 switch when there was high traffic between the control plane and the datapath.
75232	**Symptom:** An internal system error occurred in the OAW-S3 switch and APs failed to connect to the switch. **Scenario:** The issue was seen in large deployments, where the size of the config file was more than 360 KB and there were large number of references to one profile instance. Due to this there was an internal system error and the APs were unable to connect to the switch. This issue occurred in AOS-W 5.0.4.6 and is not specific to any switch model.
75411	**Symptom:** 10GE ports on OAW-4550/4650/4750 Series switches report sporadic packets being dropped with CRC errors. This issue is resolved in AOS-W 6.2.1.0. **Scenario:** This is an infrequent occurrence on these switches.
79385	**Symptom**: OAW-RAP5WN associated to OAW-4504XM switch failed to come up. The switch log files listed the reason as “AP-Group is not present in the RADIUS server.” Improvements to how remote AP route-cache entries are created resolves this issue in AOS-W 6.2.1.0. **Scenario**: The issue by a gateway failover, and was seen on a OAW-RAP5WN associated to a switch running AOS-W 6.2.0.2 in a redundant (active/standby) gateway topology.

IPSec

Table 120: *IPSec Fixed Issues*

Bug ID	Description
68035	**Symptom:** When site-to-site VPN was enabled between two switches, static routes were not removed from the routing table when site-to-site VPN went down. Improvements to the way switches add and delete static routes resolves this issue in AOS-W 6.2.1.0. **Scenario:** This occurred when site-to-site VPN was enabled and a static route was added to a remote subnet with an IPSec map.
76301	**Symptom:** An AP continually rebooted. The log files for the event listed the reason for the reboot as **Send failed in function sapd_keepalive_cb**. This issue is resolved in AOS-W 6.2.1.0 **Scenario:** This issue occurred on both campus APs (CAPs) and remote APs (RAPs) with IPSec tunnel to the switch.

Mesh

Table 121: *Mesh Fixed Issue*

Bug ID	Description
71371	**Symptom:** AOAW-AP85 configured as a mesh portal unexpectedly rebooted. The log files for the event listed the reason for the reboot as “kernel page fault.” This issue was caused by memory corruption, and is resolved in AOS-W 6.2.1.0 by changes to how internal switch modules restart. **Scenario:** This issue occurred in aOAW-AP85 mesh portal associated to an OAW-S3switch in a master-local topology.

RADIUS

Table 122: *RADIUS Fixed Issue*

Bug ID	Description
71836	**Symptom:** A switch sent incorrect class attributes to a RADIUS server, causing that server to show incorrect user statistics. Changes in how the switch sends class attributes in accounting requests has resolved this issue. **Scenario:** This issue occurred when multiple users with the same MAC address tried to connect to the switch using a wired connection.

Remote AP

Table 123: *Remote AP Fixed Issue*

Bug ID	Description
72454	**Symptom:** When a UML290 USB modem was provisioned as a remote AP (RAP) uplink with the **cellular_nw_preference** parameter set to **auto**, the RSSI value for the 3G/4G uplink was not fetched dynamically. This issue is resolved by changes in AOS-W 6.2.1.0 that enable an explicit dynamic RSSI check. **Scenario:** This issue was identified on RAPs with a UML290 modem uplink running AOS-W 6.1.3.3.

Station Management

Table 124: *Station Management Fixed Issues*

Bug ID	Description
74455	**Symptom:** Incorrect information was present in the CLI help for the local-probe-req-threshold CLI command, suggesting that the local probe response feature had to be enabled before setting the local probe request threshold. This additional help string is removed in AOS-W 6.2.1.0, as the local probe response feature is now enabled by default and this help message is no longer required. **Scenario:** This issue was not limited to any switch model, and appeared in the output of the **wlan ssid-profile <profile> local-probe-req-threshold ?** command.

WebUI

Table 125: *WebUI Fixed Issues*

Bug ID	Description
74227	**Symptom:** The **Monitoring** tab of the WebUI and the output from the **show ap active** command did not match. The WebUI showed more APs than were actually up and the output of **show ap active** displayed the correct number. This issue is resolved in AOS-W 6.2.1.0. **Scenario:** This occurred on master switches running AOS-W 6.1.3.2 or later if the bootstrap threshold in the ap system profile was set to over 40 minutes. In this instance, these APs were powered off when the switch attempted to send a configuration update. The APs failed to receive the update, and the switch marked the APs as down but did not update the AP database as well.
76348	**Symptom:** When an AP provisioned with a Fully Qualified Domain Name FQLN parameter using the format <*floor*>.<*building*>.<*campus*> was then reprovisioned, the AP provisioning page in the WebUI displayed the incorrect building value. This issue is resolved in AOS-W 6.2.1.0. **Scenario:** This issue occurred on APs provisioned with the FQLN parameter, and was not limited to any specific switch or AP model.
76335	**Symptom:** In the AOS-W 6.2.0.x **Dashboard** tab in the WebUI, the y-scale of the **Noise Floor** graph was inverted compared to previous versions of AOS-W. This has been changed in AOS-W 6.2.1.0, so -110 dBm is now shown at the bottom of the y-scale instead of the top. **Scenario:** This issue occurred on switches running AOS-W 6.2.0.x, and was not limited to a specific switch model.
79144	**Symptom:** OAW-AP105, OAW-AP92, and OAW-AP93 access points running AOS-W 6.2.x and later versions unexpectedly stopped responding and rebooted. This issue is resolved in AOS-W 6.2.1.0. **Scenario:** This issue occurred when the **spectrum monitoring** option was enabled in the AP's 802.11a or 802.11g radio profile, allowing the AP to operate as a hybrid AP that both serves clients and performs spectrum analysis on a single radio channel.

The following issues and limitations are observed in AOS-W 6.2.1.x releases. Applicable workarounds are included.

Known Issues and Limitations in AOS-W 6.2.1.9

The following issues and limitations observed in AOS-W 6.2.1.9. Applicable workarounds are included.

Air Management-IDS

Table 126: *Air Management-IDS Known Issues*

Bug ID	Description
109897	**Symptom**: The WMS and Database server reboots unexpectedly. **Scenario**: This issue is observed in OAW-4306 switches running AOS-W 6.2.1.7. **Workaround:** None.

AP-Platform

Table 127: *AP-Platform Known Issues*

Bug ID	Description
107806	**Symptom:** When a wireless client associates with a bridge forwarding mode SSID, a few Gratuitous ARP (GARP) packets from the client have an incorrect VLAN tag ID. **Scenario:** On further investigation, when supporting mobility, the AP counterfeits a GARP request for the clients. The GARP request does not use the VLAN tag ID. This issue is observed in switches running AOS-W 6.2.1.7. **Workaround:** None.
109257	**Symptom**: Active access points on a local switch are displayed as down on the master switch. **Scenario**: This issue is observed in an OAW-S3 local switch running AOS-W 6.1.2.4 in a master-standby-local topology. **Workaround:** None.

Switch-Datapath

Table 128: *Switch-Datapath Known Issues*

Bug ID	Description
95706 100817 102229 103914 104137	**Symptom**: The OAW-4550/4650/4750 Series switch unexpectedly stops passing network traffic and does not respond to an ARP request. **Scenario**: This issue occurs in OAW-4550/4650/4750 Series switch on the dual personality ports 0/0/0 and 0/0/1, with auto-negotiation enabled by default. **Workaround**: Manually define the ethernet speed for each port in OAW-4550/4650/4750 Series switch.
98884 99817 101260	**Symptom**: A corrupt packet reaching an application may crash the application in the absence of validation. **Scenario**: This issue is observed on switches running AOS-W 6.2 or later. **Workaround**: Enable control plane security.

Switch-Platform

Table 129: *Switch-Platform Known Issues*

Bug ID	Description
101612	**Symptom:** A master switch reboots unexpectedly. The log file for the event listed the reason for the reboot as **kernel panic**. **Scenario:** This issue is observed in OAW-S3 switches running AOS-W 6.2.1.5. **Workaround:** None.
103165	**Symptom:** The **Arci-cli-helper** module crashes. **Scenario:** This issue is observed in OAW-4750 switches running AOS-W 6.2.1.4. **Workaround:** None.
109894 109896	**Symptom:** Multiple processes crash on a switch. **Scenario:** This issue is observed in OAW-4306 Series switches running AOS-W 6.2.1.7. **Workaround:** None.

Known Issues and Limitations in AOS-W 6.2.1.8

The following issues and limitations observed in AOS-W 6.2.1.8. Applicable workarounds are included.

AP-Datapath

Table 130: *AP-Datapath Known Issues*

Bug ID	Description
99655	**Symptom**: Gratuitous ARP triggers responses which cause station buffer overflow. **Scenario**: This issue is observed when a Gratuitous ARP packet is sent from a RAP to update the uplink switch/router MAC table. This causes devices in the same network to send ARP responses which leads to client MAC table overflow. This issue is observed in AOS-W 6.2.1.5. **Workaround:** None.

AP-Platform

Table 131: *AP-Platform Known Issues*

Bug ID	Description
98915	**Symptom**: OAW-RAP2WG fails to boot after upgrading the switch from AOS-W 6.1.3.4 to 6.2.1.7. **Scenario**: This issue occurs on a OAW-RAP2WG in a master-local topology and is caused by IPSec setup failure. **Workaround**: None.

BaseOS Security

Table 132: *BaseOS Security Known Issues*

Bug ID	Description
97460	**Symptom:** Station table entries for clients connected to an AP in split-tunnel forwarding mode do not age out. **Scenario:** Stale entries for stations using split-tunnel forwarding mode exist in the station table even after the stations have left. This can be verified by issuing the **show station-table** command on the switch's CLI. Those stale station entries display a long time (more than several days) on the **Age** column. **Workaround:** None.

Captive Portal

Table 133: *Captive Portal Known Issues*

Bug ID	Description
94675	**Symptom:** Clients attempting to log out of captive portal authentication can incorrectly receive the error message **User not logged in**. **Scenario:** This issue occurs in AOS-W 6.2.1.3, when a client that has completed captive portal authentication tries to log out of the captive portal. The switch user table shows the client is still authenticated and able to pass traffic. **Workaround:** None.

Configuration

Table 134: *Configuration Known Issues*

Bug ID	Description
94286	**Symptom:** When the user tries to upgrade a OAW-4306 Series switch to AOS-W 6.3.1.1 it fails with the following error: **Not enough flash/memory available (60 MB needed)**. **Scenario:** This issue occurs when a user tries to upgrade to AOS-W 6.3.1.1 and is caused by an invalid temporary file in the flash directory. This issue is observed on OAW-4306 Series switches. **Workaround:** This issue is resolved by deleting the invalid temporary file before upgrading to AOS-W 6.3.1.3.

Switch-Datapath

Table 135: *Switch-Datapath Known Issues*

Bug ID	Description
95706	**Symptom**: OAW-4550/4650/4750 Series switch unexpectedly stops passing network traffic. **Scenario**: This issue is triggered by a hardware error on OAW-4550/4650/4750 Series switch using auto-negotiated Ethernet speeds. **Workaround**: Manually define ethernet speeds for each port on the OAW-4550/4650/4750 Series switch.
100375	**Symptom**: The local OAW-4750 switch is unable to pass the packets in the Last in First Out (LIFO) mode and goes offline. **Scenario**: This issue is observed when the ingress NAE free LIFO buffers are zero and the SOS didn't lease the buffers at the same time. This causes the ingress NAE stall. This issue is observed in OAW-4750 switches running AOS-W 6.2.1.4. **Workaround**: Upgrade to AOS-W 6.2.1.6 to detect the reload issue on the switch.

Switch-Platform

Table 136: *Switch-Platform Known Issues*

Bug ID	Description
76059 85289 92255 93467 93827 95431 96293 96791 96827 98196 99287 99360 99362 99472 99568	**Symptom:** A switch reboots unexpectedly. The log files for the event listed the reason as **Reboot Cause: kernel panic**. **Scenario:** This issue is seen in OAW-4550/4650/4750 Series switch having a high density of IPv4 captive-portal users configured. This results in a high number of **httpd** processes running on the switch. This issue observed in AOS-W 6.2.0.0 or later versions. **Workaround:** None.
96115	**Symptom**: A local switch crashes unexpectedly and the log files for the event lists the reason for the reboot as Kernel panic. **Scenario**: This issue is observed in OAW-4650 switches running AOS-W 6.2.1.4. **Workaround**: None.

LLDP

Table 137: *LLDP Known Issues*

Bug ID	Description
100439	**Symptom:** Clients are unable to disable the 802.3 TLV power in the AP LLDP configuration. This results in PoE allocation issue on the switches. **Scenario:** This issue is observed in OAW-4550 switches running AOS-W 6.2.1.7. **Workaround:** None.

Remote AP

Table 138: *Remote AP Known Issues*

Bug ID	Description
99343	**Symptom:** RAP randomly reestablishes a GRE tunnel. **Scenario:** This issue is observed on a device connected to an untrusted RAP wired port that has the same IP address as another RAP's default gateway. **Workaround:** Include the RAP default gateway IP in valid user ACL. Enable enforce-dhcp.

WebUI

Table 139: *WebUI Known Issues*

Bug ID	Description
76432	**Symptom:** In the Client detail page, the trend is not displayed for Frame Rates To Client or Frame Rates From Client. **Scenario:** This issue is not limited to a specific switch model or release version. **Workaround:** None.
89070	**Symptom**: The switch WebUI fails to respond when you navigate to the **Monitoring > Clients** window, and attempt to view the status of a windows client that has been misclassified as an iPhone client. **Scenario**: This issue is observed in switches running AOS-W 6.2.1.3. It occurs only when viewing the status for misclassified clients. This issue does not occur when viewing status information for Windows clients that are correctly classified. **Workaround**: None

Known Issues and Limitations in AOS-W 6.2.1.7

The following issues have been reported in AOS-W 6.2.1.7 and are being investigated.

Switch-Platform

Table 140: *Switch-Platform Known Issues*

Bug ID	Description
94304	**Symptom**: A switch running AOS-W 6.2.1.2 unexpectedly rebooted. Log files for the event listed the reason for the reboot as **Control Processor Kernel Panic**. **Scenario:** This issues occurs on switches running AOS-W 6.2.1.2 or later. **Workaround:** None

Known Issues and Limitations Prior to AOS-W 6.2.1.7

The following issues and limitations were observed in releases prior to AOS-W 6.2.1.7. Applicable workarounds are included.

802.1X

Table 141: *802.1X Known Issues*

Bug ID	Description
74663	**Symptom:** Clients are not able to reauthenticate after rebooting or logging off the network. **Scenario**: This issue is observed on a client running Windows 7 with machine authentication, and connected to a Cisco phone. This issue only occurs when the eapol-logoff feature that handles EAPOL-LOGOFF messages is enabled in the switch's 802.11X authentication profile. **Workaround:** Disable the **Handle EAPOL-Logoff** setting in the 802.11X authentication profile (This setting is disabled by default).

AMON

Table 142: *AMON Known Issues*

Bug ID	Description
94570	**Symptom:** The **Dashboard** tab of the switch WebUI can display the incorrect user role for clients. **Scenario:** This issue occurred in AOS-W 6.2.1.4, when clients connected to a remote AP configured to use split-tunnel forwarding mode. **Workaround**: View client role information on the **Monitoring** tab of the switch WebUI, or issue the command **show user-table** in the command-line interface.

AP-Wireless

Table 143: *AP-Wireless Known Issues*

Bug ID	Description
75564	**Symptom**: An internal process in an OAW-AP135 running AOS-W 6.1.3.3 restarts, causing that AP to unexpectedly reboot. **Scenario:** This issue can occur if the **Collect Stats** parameter is enabled in the WMS General profile, and the **Monitored Device Stats Update Interval** parameter in the IDS General profile is set to a non-zero value. **Workaround**: Set the **Monitored Device Stats Update Interval** in the IDS General profile to 0, its default value.
69424 75874 78978 78981 79891 80054 87250 88619 88620 88989 89537 91689 93455 93811 94396	**Symptom:** When upgraded to AOS-W 6.2, an OAW-AP125 crashed and rebooted. **Scenario:** This issue was observed when upgrading to AOS-W 6.2 from AOS-W 6.1.3.2 and later in any deployment with an OAW-AP125. **Workaround:** None.

AP-Platform

Table 144: *AP-Platform Known Issues*

Bug ID	Description
58011	**Symptom**: OAW-4306G switch reboots unexpectedly after enabling the internal AP. **Scenario**: This issue is observed in OAW-4306G switches running AOS-W 5.0 or later. The internal AP is disabled when OAW-4306G switch upgrades to AOS-W 6.2.1.x. **Workaround**: None. **Duplicate Bugs:** 60846, 60850, 61100 , 61196, 61537, 61539, 61540, 63004 , 64156, 64517 , 64524, 64526 , 66118, 66128 , 66133, 66135 , 66185 , 66596 , 66659, 67435, 67670, 67671, 67673, 67871, 67872, 67977, 67978, 67980, 68875, 68889, 68934, 68937, 72069, 74142, 75366, 75368, 75369, 75370 , 75539 , 75703 , 79854
89741 88763 89538 92872 92876 95060	**Symptom**: OAW-AP125 access points unexpectedly rebooted. **Scenario:** This issue was observed in OAW-AP125 access points associated to OAW-4550/4650/4750 Series, OAW-6000, or OAW-4604 switch running AOS-W 6.2.1.3. **Workaround**: None.
89916	**Symptom**: OAW-AP125 access points unexpectedly rebooted, and log files for the event indicate that the APs reboot because they are out of memory. **Scenario**: This issue is observed OAW-AP125 access points associated to a local switch running AOS-W 6.2.1.x. **Workaround**: None.
93955	**Symptom**: Windows Surface Pro does not allow traffic with MPDU aggregation disabled. **Scenario**: This issue occurs on OAW-AP105 running AOS-W 6.2.1.2. **Workaround:** Enable MPDU aggregation.

Air Management -IDS

Table 145: *Air Management - IDS Known Issues*

Bug ID	Description
93516	**Symptom:** An AP incorrectly reported an Overflow IE detection warning. **Scenario**: This issue occurs when an AP associated to a switch running AOS-W 6.2.1.2 in a master-local topology incorrectly detects its own MAC address as a device sending malformed IE. **Workaround**: None.

Authentication

Table 146: *Authentication Known Issues*

Bug ID	Description
55867	**Symptom:** The client is placed in the VLAN provided by 802.1X default role, instead of the VLAN defined by the Vendor Specific Attributes (VSA). **Scenario:** This issue is observed in switches where the role-based VLAN derivation is configured for a machine role and 802.1X default role, with a RADIUS server sending the VLAN through the VSA. The client is placed in the VLAN provided by the 802.1X default role, because the VLAN provided by the 802.1x default role overrides the VLAN sent through the VSA.This issue is found in switches running AOS-W 6.0.0.0 and later with 802.1X configured and machine authentication enabled. **Workaround:** Remove the VLAN from the 802.1X authenticated role and machine authentication.
81517	**Symptom**: The switch log files are being flooded with the error *Datapath-UserRem (IPv4/L2) failed: mac=<switch-mac-addr>*. **Scenario**: This issue occurred in AOS-W 6.2.0.0 on anOAW-S3switch and anOAW-AP93 remote AP operating in split-tunnel forwarding mode and configured to support captive portal authentication. **Workaround**: None

BaseOS Security

Table 147: *BaseOS Security Known Issues*

Bug ID	Description
85453	**Symptom:** An internal switch process (resolvewrap) stops responding at random intervals when a RADIUS authentication server is configured with a host name. **Scenario:** This crash does not have any impact on the AOS-W operation as the resolvewrap process is used only for resolving the host name configured for authentication server periodically. If host-name resolution fails due to a crash then subsequent attempts to resolve the host name are successful. **Workaround:** If this crash is observed continually, use an IP address is used instead of a host name in the server authentication profile.
76424	**Symptom:** Issuing the CLI command **aaa user delete all** on OAW-4550/4650/4750 Series switch managing over 14,000 users causes internal switch process modules that manage AP management, user association and user authentication to become busy and cause the switch to become unresponsive. **Scenario:** This issue occurred on OAW-4550/4650/4750 Series switch running AOS-W 6.2.x.x. **Workaround:** Delete fewer users at a time.
79467	**Symptom:** User table entries for users that disconnect from the network are not correctly aging out and getting removed from the switch user table. **Scenario**: This issue was observed on OAW-4750 local switch running AOS-W 6.2.0.2 in a master/local topology. **Workaround**: None.

Table 147: *BaseOS Security Known Issues*

Bug ID	Description
81243	**Symptom**: When an AP boots up, the switch log files display the message *AP-Group is not present in the RADIUS server for username=<mac address>; AP will take the ap-group as provisioned in the AP*. **Scenario:** This message appears when an AP boots, and although it does not indicate a problem with the boot process, the current wording of the message can be confusing. The error message is not limited to any specific AP model or software version. **Workaround**: No workaround is needed since this error message does not indicate a functionality issue.
86867	**Symptom**: When a user role and an ACL configured as the ip access-group on an AP or remote AP (RAP) interface have the same name, the AP/RAP traffic is assigned the user role ACL instead of the ip access-group ACL. **Scenario**: This issue was observed on a switch running AOS-W 6.2.1.2. **Workaround**: Do not create an ACL for the IP access-group that has a name matching that of any user-role in the configuration.
95546	**Symptom**: The OAW-4550 switch reboots frequently and the log files for the event display the reason for the reboot as **Datapath Timeout**. **Scenario**: The trigger of this issue is not known. This issue is observed in OAW-4550 switches running AOS-W 6.3.1.2. **Workaround**: None.

Switch-Datapath

Table 148: *Switch-Datapath Known Issues*

Bug ID	Description
82402 84212 86636 87552 89437 90466 91280 93591 94721 94727 95074 95624 95643 95644	**Symptom**: A switch unexpectedly rebooted. The switch log files listed the reason for the event as **Nanny rebooted machine - httpd_wrap process died**. **Scenario**: This issue occurs on a switches running AOS-W 6.2.x.x. **Workaround**: None.
84585 92227 92228 92883	**Symptom**: Traffic can fail to pass a network with heavy traffic (such as high levels of packet replication), and AES-CCM or one another encryption/decryption modes is enabled. **Scenario**: This issue was identified on OAW-4550/4650/4750 Series switch connected to 2000 APs when Gratuitous ARP messages were replicated and sent to clients. **Workaround**: None
90923	**Symptom**: When VLAN 1 on the switch uses source network address translation (NAT) for all traffic routed from VLAN 1, and the uses a different uplink VLAN to connect to remote and campus APs, the APs on the come up with ID flags, indicating that the APs are inactive and have not downloaded a configuration. The APs are not be operational in this state. **Scenario**: This issue occurs in AOS-W 6.2.x.x in deployments using control plane security **Workaround**: Issue the command interface vlan 1 no ip nat inside to disable NAT for all traffic routed from VLAN 1.

Switch-Platform

Table 149: *Switch-Platform Known Issues*

Bug ID	Description
69277	**Symptom:** The Point-to-Point Tunneling Protocol (PPTP) VPN connection is lost when a user tries to connect to the PPTP server using a Windows 7 client as the VPN client, then switches to split-tunnel forwarding mode. **Scenario:** This issue is seen in AOS-W 6.1.3.2. **Workaround:** None.
74428 88758	**Symptom:** On the dual-personality RJ45 ports 0/0/0 and 0/0/1, if the port speed is forced from/to 1 Gbps to/from 10/100 Mbps when traffic is flowing, traffic forwarding on the port can stop in an unintended manner. **Scenario:** This issue has been observed in OAW-4550/4650/4750 Series switch running AOS-W 6.2.x.x in configurations or topologies where traffic is flowing. The trigger is unknown. **Workaround:** Change the speed on the port by shutting the port., changing the speed on the port, then opening the port.
76220	**Symptom:** A switch crashes due to a virtual AP configuration change. **Scenario:** In a high traffic deployment, when a virtual AP with active client associations is removed from an AP group, a race condition may trigger a switch crash. **Workaround:** Before removing a virtual AP profile from an AP group, wait for all active associated clients to disassociate or time out. Use the **show ap association** command to verify the virtual AP client association status.
84597 83623	**Symptom**: Campus APs may not come up properly in a topology where a firewall between the AP and switch only allow communications from certain IP address through the firewall. The issue occurs if the AP communicates to the switch using the VRRP address, and this is communication is allowed through the firewall, but the control plane security feature causes the switch to communicate to the AP using its switch IP as its source IP address, which fails to pass the firewall. **Scenario**: This issue is not limited to any specific switch model or software version, and can occur in networks. Switch are using VRRP redundancy, there is a firewall between the switches and the campus AP, and the campus AP terminates at the VRRP IP **Workaround**: In the event that only the VRRP to AP communications are allowed, allowing the switch-ip address through the firewall may resolve this issue.
86903	**Symptom**: AnOAW-S3 switch module may not consistently respond to ping messages for the first 1-2 minutes after that module reboots. **Scenario**: This issue occurs if the management port on anOAW-S3 switch module running AOS-W 6.2.1.2 is connected to a VLAN that sees very low levels of broadcast or multicast traffic (less than 1 packet/second). This issue is not seen with OAW-S3 switch modules connected to VLANs with higher levels of traffic. **Workaround**: None.
93005	**Symptom**: The switch WebUI and CLI stops responding. The log files list the reason for the event as a crash in the internal process that manages the command-line interface. **Scenario**: This issue was observed in OAW-4750 switch running AOS-W 6.2.1.x in a master-local topology. **Workaround**: None.
93011	**Symptom**: Users may be unexpectedly logged out of the switch WebUI. **Scenario**: This issue was observed in AOS-W 6.2.1.4, when users accessed the switch using the WebUI. **Workaround**: Access the switch through the command-line interface..

DHCP

Table 150: *DHCP Known Issues*

Bug ID	Description
91099	**Symptom**: Clients connected to the wired port on a remote AP occasionally fail to get an IP address. This issue is under investigation, and the root cause is not yet identified. **Scenario:** This issue occurred in OAW-4550/4650/4750 Series switches running AOS-W 6.2.1.1, and was triggered when the switch failed to send DHCP offers to the AP via a GRE tunnel. **Workaround:** None.

IDS

Table 151: *IDS Known Issues*

Bug ID	Description
90630	**Symptom**: Log messages incorrectly warn of a blocked ACK DoS attack from a valid client. **Scenario**: This issue was identified in OAW-6000 switch running AOS-W 6.2.0.2 in a master-local topology. **Workaround**: None.

IPSec

Table 152: *IPSec Known Issues*

Bug ID	Description
75891	**Symptom:** When an idle user times out, the switch does not send a ping request before aging out the user. The user is aged out immediately. This applies to VPN and VIA-VPN users as well. When the users age out, the VPN tunnel will also go down. **Scenario:** This occurs on switches running AOS-W 6.2.x.x, when there is no data for the user during the ageout time period. For VPN and VIA-VPN users, if the IPSec tunnel does not have any data for the configured user ageout time, the user will age out and the tunnel will be deleted. **Workaround:** Increase the value of the user ageout time. The default value is five minutes. This issue can also be avoided if you ensure that there is always some data sent from the user.

Master-Redundancy

Table 153: *Master-Redundancy Known Issues*

Bug ID	Description
70343	**Symptom**: Custom captive portal pages are not synced between a master and standby switch when set up to do so. **Scenario**: For all software versions, when the standby becomes the master, the custom captive portal page will no longer show up during CP authentication. The **database synchronize** command only copies database files and RF plan floor plan backgrounds. **Workaround**: None
75367	**Symptom**: Enabling web-server debug logging using the CLI command **logging level debugging system subcat webserver** does not take effect until you restart the HTTPD process. **Scenario**: This happens on all switch models running AOS-W3.x, 5.x and 6.x software versions when web-server debug logging mode is enabled. **Workaround**: Restart the HTTPD process in order to enable debug logging.

Mobility

Table 154: *Mobility Known Issues*

Bug ID	Description
58883 60328	**Symptom:** In a Layer-3 IP mobility enabled network, when the client moves from a Home Agent network to a Foreign Agent network, the IPv4 address of the client changes. This prevents the client from sending traffic. **Scenario:** Layer-3 IP mobility does not work when IPv6 packet processing is enabled on the switch. This issue is found in switches running AOS-W 6.2.x.x.. **Workaround:** Do not issue the **router enable** command along with the **ipv6 enable** command in the switch.
92453	**Symptom**: Users connecting to an AP or switch with IP mobility enabled are unable pass any traffic **Scenario**: This issue was first identified in AOS-W 6.2.1.3, and is not specific to any switch model. This issue is triggered when client roams between an ESSID with IP mobility enabled and an ESSID with IP mobility disabled. **Workaround**: Clear the IP mobile host entry using by issuing the CLI command **clear ip mobile host <client-mac-address>**. After clearing the client IP mobile host entry, the client is able to pass traffic.

Remote AP

Table 155: *Remote AP Known Issues*

Bug ID	Description
83002	**Symptom**: A wireless client connected to a backup virtual AP configured in bridge forwarding mode is unable to get an IP address from an assigned VLAN. **Scenario**: This issue occurred when the switch upgraded to AOS-W 6.2.x.x. **Workaround**: Once the AP connects to the switch, remove the virtual AP profile from the ap-group/ap-name configuration, then return the virtual AP profile to the ap-group/ap-name settings.

Station Management

Table 156: *Station Management Known Issues*

Bug ID	Description
72194	**Symptom:** When VLAN pooling is used with the assignment type EVEN, the user VLAN changes when the client roams from AP to AP, but the IP address remains the same until a release/renew is executed on the client device. **Scenario:** This issue occurs on any switch model with the VLAN mobility and preserve VLAN features enabled. When these features are enabled, the bridge table of the switch keeps user entries for 12 hours. This issue occurs when the STM module (an internal process) of the switch does not find the entry in the bridge lookup result. **Workaround:** Disable VLAN mobility and the preserve VLAN feature.
90390	**Symptom**: IP phones connected to the wired port on a remote AP get disconnected. **Scenario**: This issue was identified in AOS-W 6.2.1.x, and is triggered when GRE tunnels from the wired port get dropped. **Workaround**: Reboot the remote AP to restore connectivity to the IP phones.
91224	**Symptom:** An AP unexpectedly reboots. The switch log files list the reason for the event as **Unexpected stm (Station management) runtime error**. **Scenario:** This issue occurred on OAW-S3 switch modules running AOS-W 6.2.1.4 in a master-local topology.

Startup Wizard

Table 157: *Startup Wizard Known Issues*

Bug ID	Description
72740	**Symptom:** The Switch Wizard, Campus AP Wizard, and Remote AP Wizard display a blank page when the LDAP server attributes contain special characters. **Scenario:** This issue occurs on switches running AOS-W 6.2.x.x when the LDAP server attributes contains special characters. **Workaround:** Ensure that the LDAP server attributes do not have special characters.
77057	**Symptom:** In the **Remote APWizard**, the Split Tunnel role configuration requires an additional ACL to automatically generate roles. **Scenarios:** This issue occurs on switches running AOS-W 6.2.x.x if the **svc-dhcp permit** rule is missing in the access list of **$APGROUPNAME_default_role** in the **Remote AP Wizard**. Due to this, the IP addresses cannot be assigned to the clients. **Workaround:** Add the **any any svc-dhcp permit** ACL rule under the ACL in position 1.
81063	**Symptom:** The Authentication port configuration cannot be applied to the LDAP server. **Scenario:** This issue occurs on switches running AOS-W 6.2.x.x when an invalid command is sent to the switch from **Campus AP** or **WLAN Wizards**. **Workaround:** Manually configure the authentication port for the LDAP server under **Configuration > Security > Authentication > Servers > LDAP**.

WebUI

Table 158: *WebUI Known Issues*

Bug ID	Description
55981	**Symptom:** When a user views the Spectrum UI with saved preferences from a newer version of AOS-W, the UI will display charts incorrectly. **Scenario:** Downgrading from a newer version of AOS-W, such as from 6.2.x.x to 6.1.x.x with saved Spectrum preferences, will cause the Spectrum UI to display charts incorrectly. This is due to the difference between the Spectrum UI in 6.2.x.x and previous versions. **Workaround:** Use the command **ap spectrum clear-webui-view-settings** on the switch to delete the saved preferences.
66521	**Symptom:** Two **Apply** buttons are displayed in the WebUI when adding users to the internal database. **Scenario:** While creating a new user in the WebUI, two **Apply** buttons appear in the **Configuration > Security > Authentication > Internal DB** page due to incorrect labeling of the buttons. This issue is not limited to a specific switch model. **Workaround:** Use the **Apply** button at the top to add a new user. Use the **Apply** button at the bottom to apply any user list changes.
75836	**Symptom:** An incorrect label is displayed on the **AP Details** page on clicking the AP Name hyperlink on the **Client and Performance** page of the WebUI **Dashboard**. **Scenario:** This issue occurs on switches running AOS-W 6.2.x.x. When the users navigate to the **AP Details** page from the **Client and Performance** page of the WebUI **Dashboard,** the client filter is applied instead of the AP filter. **Workaround:** None.

Table 158: *WebUI Known Issues*

Bug ID	Description
75857	**Symptom:** An incorrect label is displayed on the **WLAN Details** page when the WLAN hyperlink is selected from the **Client** page. **Scenario:** This issue occurs on switches running AOS-W 6.2.x.x, when WLAN detail page is navigated from Client page, Client filter gets applied instead of the WLAN filter. **Workaround:** None.
76836	**Symptom:** A Javascript error occurs when trying to view the trend on the **WLAN Summary** page. **Scenario:** This issue occurs on switches running AOS-W 6.2.x.x, when the trend is performed on the Client entry hyperlink or distribution charts of Frame rates in **Default** or **Tx/Rx Stats** section. A blank screen with JS error is seen in Firebug. **Workaround:** None.
77274	**Symptom:** An error occurs when creating an access control list using the WebUI when the **invert** option is enabled in **netdestination**. **Scenario:** This issue occurs on switches running AOS-W 6.2.x.x, where an error occurs while creating the ACLs with netdestination created with invert option. **Workaround:** None.
77542	**Symptom:** The OAW-4306 Series switch is unable to upgrade from a local file. **Scenario**: For the local file upgrade to be successful, the switch must have at least 75 MB of free memory. When upgraded to AOS-W 6.2.x.x, the OAW-4306 Series switch has only 77 MB of free memory remaining. And when the browser UI is launched, the free memory is decreased to 75 MB. In this case, the local file upgrade will fail. It is recommended that you do not use the local file upgrade function in the switch has less than 80 MB of free memory. **Workaround:** None. Use the USB, TFTP, SCP, or CLI option to upgrade instead.
79146	**Symptom:** The SSID does not display properly if the SSID name contains special characters. **Scenario:** This issue occurs on switches running AOS-W 6.2.x.x, when the cursor is placed on the WLAN. **Workaround:** Do not configure an SSID name with special characters.
80260	**Symptom:** Users cannot add use the WebUI to add a netdestination to a whitelist or blacklist in the **Captive Portal** profile. **Scenario:** This issue occurs on switches running AOS-W 6.2.x.x, where the whitelist and blacklist details do not contain any data on the **Configuration** > **Security** > **Authentication** > **L3 Authentication** > **Captive Portal Profile** page in the WebUI. **Workaround:** None.
92770 94692	**Symptom**: The **Advanced Services** > **Stateful Firewall** > **Global Settings** section of the WebUI do not correctly display settings defined in the following fields: • Monitor Ping Attack (per sec) • Monitor TCP SYN Attack rate (per sec) • Monitor IP Session Attack (per sec) **Scenario**: This issue is triggered when AOS-W 6.2.1.4 incorrectly overrides the configured values for the **Monitor ping attack**, **Monitor TCP SYN attack**, and **Monitor IPv6 sessionsattack** features. **Workaround**: None.
95269	**Symptom**: The switch WebUI does not display all entries in the remote AP whitelist. **Scenario**: This issue is observed in AOS-W 6.2.1.4, when the remote AP whitelist contains more than 100 entries. **Workaround**: View the remote ap whitelist by accessing the command-line interface in enable mode, and issuing the command **show whitelist-db rap**.

WMM

Table 159: *WMM Known Issues*

Bug ID	Description
68503	**Symptom**: The switch chooses an incorrect WMM priority (background instead of best-effort) in the downstream traffic. When same DSCP value is mapped to two different access categories, the lower of the two is used for the downstream traffic. **Scenario**: This issue is observed on switches running AOS-W 6.2.x.x or earlier in Tunnel and D-Tunnel modes. **Workaround**: None.

Issues Under Investigation

The following issues have been reported in AOS-W 6.2.1.9 and are being investigated.

Base OS Security

Table 160: *Base OS Security Issues Under Investigation*

Bug ID	Description
109895	**Symptom:** A OAW-4306 switch fails to respond and reboots with the reboot cause **Nanny rebooted machine - udbserver process died**.

Maximum DHCP Leases Per Platform

Exceeding the following limits may result in excessive CPU utilization, and unpredictable negative impact on switch operations:

Table 161: *Maximum DHCP Lease Per Platform*

Platform	Maximum
OAW-4550/4650/4750 Series	5000
OAW-S3	512
OAW-4504XM	512
OAW-4604	512
OAW-4704	512
OAW-4306 Series	512

This chapter details 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

- Beginning with AOS-W 6.2.0.0, the default **NAS-port-type** for management authentication using MSCHAPv2 is **Virtual** instead of **Wireless**. If your configuration uses the NAS-port-type in any derivation or access rules, this value will change for management user requests from the switch. This behavior is in line with IEEE RFC 2865. There is no change in behavior for management authentication using PAP.
- Beginning with AOS-W 6.2.0.0, you cannot create redundant firewall rules in a single ACL. AOS-W will consider the 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 your pre-6.2 configuration contains an ACL with redundant firewall rules, on upgrading, only the last rule will remain.

  For example, in the below ACL, both ACE entries could not be configured in AOS-W 6.2.x.x. Once the second ACE entry is added, the first would be overwritten.

```
(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
```

- AOS-W 6.2.x.x is supported only on OAW-4550/4650/4750 Series, OAW-S3, OAW-4604, OAW-4704, OAW-4306 Series, and OAW-4504XM switches.

  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 89).
- For OAW-4306 Series and OAW-4550/4650/4750 Series switches, the local file upgrade option in the 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 exceeds limit** and the upgrade fails. All other upgrade options work as expected.
- Upon upgrading to AOS-W 6.2.x.x, the internal AP of the OAW-4306G switch is disabled. The switch then operates as OAW-4306G switch.
- OAW-4504XM switches with 1GB memory can be upgraded to AOS-W 6.2.x.x. The OAW-4504XM switch with 512MB of memory does not support AOS-W 6.2.x.x.

Important Points to Remember and Best Practices

Ensure a successful upgrade and optimize your upgrade procedure by taking the recommended actions listed below. 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 during the upgrade, such as configuration changes, hardware upgrades, or changes to the rest of the network. This simplifies troubleshooting.
- Know your network. 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 issuing 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 over 30 MB of data.
- 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 are not valid options.
- Always upgrade the non-boot partition first. If problems occur during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.
- Before you upgrade to the current version of AOS-W, assess your software license requirements and load any new or expanded licenses you require. For a detailed description of these new license modules, refer to the "Software Licenses" chapter in the 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:

- Issue 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.
- Issue the **show storage** command to confirm that there is at least 60 MB of flash available for an upgrade using the CLI, or at least 75 MB of flash 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 issue the **halt** command before power cycling.

If the output of the **show storage** command indicates that insufficient flash memory space is available, you must free up additional memory. Any switch logs. crash data, or and 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 memory before upgrading:

- **Crash Data:** Issue 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 88 to copy the **crash.tar** file to an external server, then issue 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 88 to back up the flash directory to a file named **flash.tar.gz**, then issue the **tar clean flash** command to delete the file from the switch.
- **Log files:** Issue 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 88 to copy the **logs.tar** file to an external server, then issue 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 on 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 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**.

BackUp 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. Enter **enable** mode in the CLI on the switch, and enter the following command:

   ```
   (host) # write memory
   ```
2. Use the **backup** command to back up the contents of the Compact Flash file system to the flashbackup.tar.gz file.

   ```
   (host) # backup flash
    wait while we tar relevant files from flash...
    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> <remot
   e 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 Alcatel-Lucent 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 88.

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 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.
4. If all the switches cannot be upgraded with the same software image and reloaded simultaneously, use the following guidelines:
   a. Remove the link between the master and local mobility switches.
   b. Upgrade the software image, then reload the master and local switches one by one.
   c. Verify that the master and all local switches are upgraded properly.
   d. Connect the link between the master and local switches.

Upgrading to 6.2.x.x

Install Using the WebUI

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash available for an upgrade using the WebUI.

Upgrading From an Older Version of AOS-W

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 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 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 version of AOS-W on page 90 to install the interim version of AOS-W, then repeat step 1 to step 11 of the same procedure to download and install AOS-W 6.2.

Upgrading From a Recent version of AOS-W

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

- 6.0.1.0 or later
- 5.0.3.1 or later (If you are running AOS-W 5.0.3.1 or a later 5.0.x.x review, review Upgrading With OAW-RAP5 and OAW-RAP5WN APs on page 91 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 the customer support site.
2. Upload the new software image(s) to a PC or workstation on your network.
3. Log in to the AOS-W WebUI from the PC or workstation.

4. 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.
5. Select the downloaded image file.
6. In the **partition to upgrade** field, select the non-boot partition.
7. In the **Reboot Switch After Upgrade** option field, 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.
8. In **Save Current Configuration Before Reboot** field, select **Yes**.
9. Click **Upgrade**.
10. When the software image is uploaded to the switch, a pop-up 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).
11. When the reboot process is complete, log in to the WebUI and navigate to the **Monitoring > Switch > Switch Summary** page to verify the upgrade.

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

1. Login to the WebUI to verify all your switches are up after the reboot.
2. Navigate to **Monitoring > 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 88 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 91. 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 Access Points by executing the **show ap image version** command.
2. If the flash (Provisioning/Backup) image version string shows the letters *rn*, 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 omit 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 6.2.1 and upgrade its production software image.

Install Using the CLI

CAUTION

Confirm that there is at least 40 MB of free memory and at least 60 MB of flash available for an upgrade using the CLI. For details, see Memory Requirements on page 88.

Upgrading From an Older version of AOS-W

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.

- For 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 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 version of AOS-W on page 92 to install the interim version of AOS-W, then repeat step 1 to step 7 of the procedure to download and install AOS-W 6.2.

Upgrading From a Recent version of AOS-W

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

- 6.0.1.0 or later
- 5.0.3.1 or later (If you are running AOS-W 5.0.3.1 or a latest 5.0.x.x, review Upgrading With OAW-RAP5 and OAW-RAP5WN APs on page 91 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).
3. Execute the **ping** command to verify the network connection from the target switch to the SCP/FTP/TFTP server:

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

   or

   ```
   (hostname)# ping <tftphost>
   or
   (hostname)# ping <scphost>
   ```

4. Use the **show image version** command to check 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**.

   ```
   (hostname) #show image version
   ```

5. Use the **copy** command to load the new image onto the non-boot partition:

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

   or

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

   or

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

   or

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

NOTE

The USB option is only available on the switches.

6. Execute the **show image version** command to verify the new image is loaded:
   ```
   (hostname)# show image version
   ```
7. Reboot the switch:
   ```
   (hostname)# reload
   ```
8. Execute the **show version** command to verify the upgrade is complete.
   ```
   (hostname)# show version
   ```

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

1. Login to the command-line interface to verify all your switches are up after the reboot.
2. Issue the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Issue the **show ap database** command to 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 88 for information on creating a backup.

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 the current version of AOS-W to 5.0.3.2, changes made to WIPS in 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 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. Backup your switch. For details, see Backing up Critical Data on page 88.
2. Verify that the control plane security is disabled.
3. Set the switch to boot with the previously-saved pre-6.2 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:
   - Restore pre-6.2 flash backup from the file stored on the switch. Do not restore the current version of the flash backup file.
   - If you installed any certificates while running the current version of AOS-W, you need to reinstall the certificates in the downgraded AOS-W version.

Downgrading Using the WebUI

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

1. If the saved pre-upgrade 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 pre-upgrade configuration file.
   b. For **Destination Selection**, enter a filename (other than default.cfg) for Flash File System.
2. Set the switch to boot with your pre-upgrade configuration file by navigating to the **Maintenance > Switch > Boot Parameters** page.
   a. Select the saved pre-upgrade configuration file from the **Configuration** File menu.
   b. Click **Apply**.
3. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > 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 pre-upgrade 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 sections describe how to use the CLI to downgrade the software on the switch.

1. If the saved pre-upgrade 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 pre-upgrade configuration file.

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

3. Execute the **show image version** command to view the partition on which your previous software image is stored. 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 6.1.3.2. Partition 1, the default boot partition, contains the AOS-W 6.2.1.8 image:

```
#show image version
---------------------------------
```

```
Partition               : 0:1 (/dev/ha1)
Software Version        : AOS-W 6.1.3.2 (Digitally Signed - Production Build)
Build number            : 33796
Label                   : 33796
Built on                : Fri May 25 10:04:28 PDT 2012
----------------------------------

Partition               : 0:1 (/dev/hda2) **Default boot**
Software Version        : AOS-W 6.2.1.8 (Digitally Signed - Production Build)
Build number            : 43609
Label                   : 43609
Built on                : Fri May 09 20:41:56 PDT 2014
```

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

This chapter discusses the steps required to migrate your existing switches to OAW-4550/4650/4750 Series switches.

For information about migrating to the OAW-4550/4650/4750 Series Switch, visit service.esd.alcatel-lucent.com.

Migrating to the OAW-4550/4650/4750 Series Switch

You must complete the following tasks to complete the migration process:

- Back up the switch data from your existing switch.
- Upgrade your network to AOS-W 6.2.x.x. This ensures that the image on your new switches matches the image of the rest of the switches in your network.
- Back up the switch data from your upgraded, existing switch.
- Transfer existing licenses to your new switch.
- Install your new switch.
- Install the backed up data on your new switch.
- Apply transferred and new licenses.
- Reload your switch.
- Update port-related configuration.
- Confirm that your new switch operates as expected.

Important Points to Remember

- The OAW-4550/4650/4750 Series switches use a different port number scheme than other switches. Ports on the OAW-4550/4650/4750 Series OAW-4550/4650/4750 Series are numbered **slot/module/port**. Other switch ports are numbered **slot/port**.
- Not all Alcatel-Lucent switch models support AOS-W 6.2. The following switches support AOS-W 6.2:
  - OAW-4550/4650/4750 Series
  - OAW-S3
  - OAW-4504XM, OAW-4604, and OAW-4704
  - OAW-4306 Series

Beginning in AOS-W 6.2, the OAW-4306G switch's internal AP is disabled. Additionally, upon upgrade, the OAW-4306G will appear as OAW-4306G-1 and the OAW-4306G-8 will appear as OAW-4306G-9 in AOS-W.

- You can complete this migration process on a switch-by-switch basis if your replaced switches support AOS-W 6.2. The entire deployment does not need to be completed at the same time.
- When replacing a master switch, replace the backup master first.
- If you are migrating to OAW-4550/4650/4750 Series switch from a switch not listed above, contact Alcatel-Lucent support.

Backing Up Your Data Before Upgrading to 6.2

Back up your switch data before upgrading to AOS-W 6.2. To back up your switch data, complete the steps in the following sections:

Back Up the Flash File System in the WebUI

1. Click on 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.
6. 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.

Back Up the Flash File System in the CLI

1. Enter **enable** mode in the CLI on the switch, and enter the following command:

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

2. Use the **backup** command to back up the contents of the Compact Flash file system to the flashbackup.tar.gz file.

```
(host) # backup flash
 wait while we tar relevant files from flash...
 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:

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

Upgrading Your Network

Before attempting upgrade any of your switches, read the Upgrade Procedures on page 86. If you are migrating from switches that do not support AOS-W 6.2, best practices are to upgrade to the latest supported build of your current version of AOS-W before beginning the migration process.

Table 162 provides a brief overview of the steps required to upgrade to AOS-W 6.2.1.9.

Table 162: *AOS-W 6.2 Upgrade Path Overview*

Version	Step 1	Step 2
3.x, earlier than 3.4.4.1	Upgrade to the latest 3.4.5x	Upgrade to 6.2
RN-3.x	Upgrade to the latest 5.0.4.x	Upgrade to 6.2
5.x, earlier than 5.0.3.1	Upgrade to the latest 5.0.4.x	Upgrade to 6.2
6.0.0.x	Upgrade to the latest 6.0.2.x	Upgrade to 6.2
6.2.0.x, 6.1.x.x, 6.0.1.x, 6.0.2.x, 5.0.3.1 (or later 5.0.3.x), 5.0.4.x 3.4.4.1 (or later 3.4.x), 3.4.5.x	Upgrade to 6.2	—

Backing Up Your Data After Upgrading to 6.2

After completing the upgrade to AOS-W 6.2, back up your switch data and configuration once more before continuing. It is recommended that you rename your backup file and transfer to an external storage device.

Transferring Licenses

To transfer existing licenses from one switch to another:

1. Open a browser, navigate to https://licensing.alcateloaw.com, and log in.
2. Navigate to **Certificate Management > Transfer certificate** and select the licenses you want to transfer.
3. All the certificates active on the switch of the license certificate you have selected will be displayed. Select all the certificates you would like to transfer.
4. Enter the serial number of the new switch and click **Transfer**. When the transfer is completed successfully, you will receive a new set of activation keys.

The selected certificates must be compatible with your new switch. If not, you will not be able to complete the transfer. You will receive the following error message: **This certificate is not compatible with your system!**

If the destination switch does not exist, you will receive the following error message: **This system does not exist**. If you receive this error, ensure that you entered the serial number correctly. Once you have verified that the serial number you entered was correct, contact Alcatel-Lucent Technical Support.

Installing Your New Switch

For instructions and additional information about installing your OAW-4550/4650/4750 Series switch, refer to the *Alcatel-Lucent OAW-4550/4650/4750 Series Switch Installation Guide* and *AOS-W 6.2 Quick Start Guide* included with your device. For the latest version of these document, visit service.esd.alcatel-lucent.com and click the **Documentation** tab.

After installing your OAW-4550/4650/4750 Series, verify that it is running the latest version of AOS-W 6.2. If not, it is recommended that you upgrade your switch.

Installing Backed Up Switch Data

Follow the instructions below to install backed up switch data. Do not modify your configuration before reloading the switch.

OAW-4550/4650/4750 Series switches use a different port numbering scheme than other switches. Ports on the OAW-4550/4650/4750 Series are numbered **slot/port/module**. Other switch ports are numbered **slot/port**. Once you've loaded your old configuration onto OAW-4550/4650/4750 Series switch, you will no longer be able to connect to the switch over the network. Additionally, all ports will become untrusted. You must connect to your new switch using a serial connection to reconfigure port settings.

To install your existing configuration and switch data onto your new switch, complete the following steps.

Restore the Flash File System in the WebUI

1. Navigate to the **Maintenance > File > Copy Files** page.
   a. For **Source Selection**, specify the server to which the flashbackup.tar.gz file was previously copied.
   b. For **Destination Selection**, select **Flash File System**.
   c. Click **Apply**.
2. Navigate to the **Maintenance > File > Restore Flash** page.
3. Click **Restore** to restore the flashbackup.tar.gz file to the flash file system.

4. Install licenses before you reboot your switch. Do not modify your configuration until after the switch reloads.

Restore the Flash File System in the CLI

1. Enter **enable** mode in the CLI on the switch.
2. Transfer the flashbackup.tar.gz file from its external location to the switch's flash using the commands that follow according to your preferred method.

```
copy ftp: <ftphost> <srcfilename> flash: flashbackup.tar.gz
copy tftp: <tftphost> <srcfilename> flash: flashbackup.tar.gz
copy scp: <scphost> <username> <srcfilename> flash: flashbackup.tar.gz
copy usb: partition <partition-number> <srcfilename> flash: flashbackup.tar.gz

restore flash
```

3. Install licenses before you reboot your switch. Do not modify your configuration until after the switch reloads.

Applying Licenses

After you have installed your new switch and brought it up, you can apply and back up any new or transferred licenses.

Applying the Software License Key in the WebUI

1. Log in to your switch's WebUI.
2. Navigate to the **Configuration > Network > Switch** select the **License** tab.
3. Copy the software license key, from your email, and paste it into the **Add New License Key** field. Click **Add**.
4. Reboot your switch to enable the new license feature.

Applying the Software License Key in the License Wizard

1. Log in to your switch's WebUI.
2. Launch the License Wizard from the **Configuration** tab and click the **New** button.
3. The License Wizard will step you through the activation process. Click on the Help tab within the License Wizard for additional assistance.
4. Reboot your switch to enable the new license feature.

Backing Up Licenses in the WebUI

1. Log in to your switch's WebUI.
2. Navigate to the **Configuration > Network > Switch** and select the **License** tab.
3. Scroll to the bottom of the page and click **Export Database**.
4. Enter the file name of the file to export and click **OK**.
5. Copy the backup file from the external server or USB storage device to the compact flash file system using the file utility in the **Maintenance > File > Copy Files** page.

Backing Up Licenses in the CLI

1. Use the license export <filename> command to create a license backup.

```
(host) #license export licensebackup.db
Successfully exported 1 licenses from the License Database to licensebackup.db
```

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

```
(host) copy flash: licensebackup.db ftp: <ftphost> <ftpusername> <ftpuserpassword> <remote dir
ectory>
(host) #copy flash: licensebackup.db usb: partition <partition-number> licensebackup.db
```

Reload Your Switch

After restoring flash and transferring licenses, you must reboot your switch before continuing.

Establishing Network Connectivity

Due to the difference in port numbering schemes between the OAW-4550/4650/4750 Series and older switch platforms, your OAW-4550/4650/4750 Series switch will not have network connectivity and all ports will become untrusted after installing your previous switch's configuration in data. All previous switch models used a **slot/port** number scheme; the OAW-4550/4650/4750 Series uses **slot/module/port**. To establish network connectivity, you must manually reconfigure your switch interfaces.

Slot and module will always be 0 and 0 on the OAW-4550/4650/4750 Series switch. The first two ports on the OAW-4550/4650/4750 Series, 0/0/0 and 0/0/1 are combination ports and can be used for management, HA, and data traffic. Ports 0/0/2 through 0/0/5 can only be used for data traffic. Keep this in mind when reconfiguring your ports.

Connecting to the Switch

Since your OAW-4550/4650/4750 Series switch does not have network connectivity, you must directly connect to it using a serial port connection. Once connected, you will receive a login prompt. Login using your configured credentials.

After you restore the flash and rebooting, all inherited port configurations are be lost. This can include, but is not limited to, trusted settings, port channel, and port monitoring settings. The following commands are affected by this new port numbering scheme and must be considered when reconfiguring your ports:

```
interface gigabitethernet <slot/port/module>
   trusted

interface range gigabitethernet <slot/port/module>

interface port-channel gigabitethernet
   add <slot/port/module>
   delete <slot/port/module>

interface gigabitethernet port monitor <slot/port/module>

interface vlan <vlan-id>
   ip igmp proxy gigabitethernet <slot/port/module>
```

Verifying Switch Operation

Once you have completed the tasks described above, verify that your switch and the expected APs come up and are active.

Verifying Migration in the WebUI

1. Log in into the WebUI to verify all your switches are up after the reboot.
2. Navigate to **Monitoring > 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 would expect.
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.

Verifying Migration in the CLI

1. Log in into the CLI to verify all your switches are up after the reboot.
2. Use the command **show ap active** to determine if your APs are up and ready to accept clients.
3. Issue the command **show ap database** to verify that the number of access points and clients are what you would expected.
4. Test a different type of client for each access method that you use, and in different locations when possible.
5. Backup all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing Up Your Data Before Upgrading to 6.2 on page 97.