AOS-W 3.3.2.24

Release Notes

This document describes the new features and issues pertinent to the AOS-W 3.3.2.24 release.

See the *AOS-W 3.3.2 Software Upgrade Guide* for instructions on how to upgrade your OmniAccess Switch to this release.

What's New in This Release

AOS-W 3.3.2.24 is a patch release that addresses and provides solutions to a number of known issues. Those known issues are listed at "Issues and Limitations Fixed in AOS-W 3.3.2.24" on page 11.

Memory Monitor Enhancement

The memory monitor now saves up to 30 logs of debugging information. The logs rotate on a first-in first-out basis so that the most recent log contains the most current debug information. These logs include information on system memory, irregular application memory usage, large files in the ramdisk, large pending tx/rx queues, and memory block usage. This information is leveraged for technical support logs and nanny post-crash reports.

New CLI Commands

Table 1 list the new commands added to this release.

Table 1 *New CLI Commands for AOS-W 3.3.2.24*

Command	Description
`ids general-profile <profile-name> mon-stats-update-interval`	Allows you to control the time interval in seconds for AP to update the switch with stats for monitored devices. Minimum is 60. 0 is to disable stats propagation.
`show memory debug [verbose]`	Display detailed memory information to debug memory errors the controller. This command should only be used under the supervision of Alcatel-Lucent Technical Support.

License Interaction

The various licenses do require some equality and other important interactions.

- WIP being equal to AP/RAP recommended best practices.
  - All Aruba APs run WIP services, including RAPs. If the WIP licenses count is less than the AP/RAP count, then the number of AP's that are active will be equal to the WIP license count.
  - If the WIP license count is greater than AP/RAP count, there are no issue.

It is not possible to designate specific APs for WIP/non-WIP operations.

- Mesh
  - Outdoor mesh points or mesh portals consume one mesh license
  - If a mesh node is also configured for client service (i.e. advertises a BSSID), it consumes one AP license

RAPs consume only RAP licenses. An AP licenses is not needed nor consumed for the normal operations of RAPs.

In Previous Releases of AOS-W 3.3.2

Previous releases of AOS-W 3.3.2.x have introduced new software features for all Alcatel-Lucent OmniAccess Switches. This section describes new features and capabilities of AOS-W 3.3.2.x.

Voice

A number of voice optimization changes have were made in AOS-W 3.3.2.12 to help minimize packet loss and improve call reliability.

SIP Midcall Request Timeout

This feature was added in AOS-W 3.3.2.20 as a fix to bug #35288

This feature allows the switch to determine whether or not a call is still active in scenarios where a voice session does not exist, such as when a call is placed on hold. When enabled, if a client does not send responses for a mid-dialog requests, ALG will clear the status of the call and generate an ABORTED call record.

```
(config) #voip sip-midcall-req-timeout  <enable/disable>
```

CLI

SNMP Trap Versions

The feature was added in AOS-W 3.3.2.14.

A new command has been added to the CLI, allowing you to set the SNMP trap version that will be used by the remote trap receiver. This command has been added because the OmniVista 3600 Air Manager (OV3600) does not support SNMP version 3. For use with OV3600, you must select version 1 to avoid an SNMP queue overflow. The default setting is SNMP version 3.

The new command is as follows:

```
mobility-manager <IP of MMS server> user <username> <password>
trap-version {1|2c|3}
```

SNMP Queries Over IPsec Tunnel

This command was added in AOS-W 3.3.2.20 as a fix to bug #35902.

A command has been added to the CLI to force the use of the switch's IP address when sending SNMP responses. This will ensure that packets are sent to the tunnel interface.

```
(config) #snmp-server source switch-ip
```

voip-proxy-arp

The following CLI change was made in AOS-W 3.3.2.9.

The CLI command `voip-proxy-arp` has been changed to `broadcast-filter arp`. This change applies to both Virtual AP parameters as well as global firewall commands.

drop-mcast

The following CLI change was made in AOS-W 3.3.2.9.

The CLI command `drop-mcast` has been changed to `broadcast-filter all`. This command has been moved out of SSID profile and into Virtual AP profile to keep the `broadcast-filter` commands together. Additionally, this will no longer be tied to the voice license and is available in the base AOS-W.

Hardware

Software-Upgradable OAW-AP120 Series a/b/g APs

This feature was introduced in AOS-W 3.3.2.73.3.2.7.

The Alcatel-Lucent OAW-AP120 series wireless access points are now available in a/b/g variants. These models are upgradable via a software license to full IEEE 802.11n draft standard support. All OAW-AP120 series access points work only in conjunction with an Alcatel-Lucent WLAN Switch.

For more information, see the *Alcatel-Lucent OAW-AP120 Series Indoor Access Point Installation Guide*.

U-APSD Support

Support of Unscheduled Automatic Power Save Delivery (U-APSD) on the AP-120 Series was introduced in AOS-W 3.3.2.7.

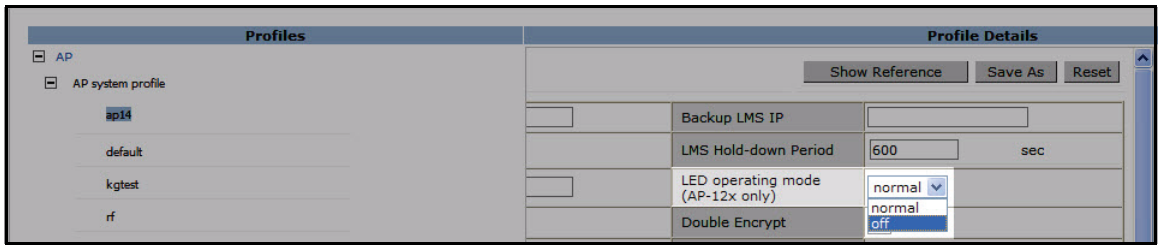
Disabling AP LEDs

AOS-W 3.3.2.8 introduces the ability to disable the LEDs on an AP when necessary. This is done through the CLI or the WebUI.


NOTE

This feature is available only on the OAW-AP120 Series.

To disable the LEDs through the WebUI, navigate to **Configuration > Advanced Services > All Profiles > AP > AP System Profile**. Select the desired AP from the list. When an AP is selected, the **Profile Details** menu appears. Locate the **LED operating mode (AP-12x only)** parameter and select "off" from the drop down menu, as shown below.



LEDs can also be disable through the CLI, while in configuration mode, using the following commands:

```
ap system-profile <profile-name>
led-mode {normal | off}
```

Platform

Port Session Behavior Change

Whenever port ACL is changed, the existing sessions on that port will not be deleted. Therefore, for deny rules to take effect, you need to bring down and up the port. The same applies for port channels.

This behavior change was added in AOS-W 3.3.2.9 and fixes Bugs #29754, 30478, and 32263.

PMKSA Cache Entry Age-out Timer

This feature was added in AOS-W 3.3.2.15.

A new command has been added to the CLI, allowing you to set a timer to age out old PMKSA cache entries. By default, this value is set to 8 hours but can be configured to anything from 1 hour to 2000 hours.

```
aaa authentication dot1x timer keycache-tmout <tmout>
```

Configuration Wizards

The Configuration Wizards were added in AOS-W 3.3.2.7.

This release of AOS-W introduces the implementation of three imbedded configuration wizards within the WebUI: the Switch Wizard, the WLAN Wizard, and the License Wizard. These three configuration wizards step you through various tasks via the Workflow pane within each wizard. Each wizard includes imbedded help that can be accessed by clicking the Help tab from within the wizard.

The following new wizards are accessible from the Configuration tab within the WebUI:

- Switch Wizard: Allows basic configuration of the switch, such as switch name, user admin and enable mode passwords, time settings, switch mode, VLANs and IP interfaces, and ports.
- WLAN Wizard: Allows creation and configuration of new internal and/or external WLANs associated with the “default” ap-group.
- License Wizard: Allows installation and activation of software licenses.


NOTE

Clicking Cancel from within the Switch and WLAN Wizards will return you to the top level page of the WebUI section from which you launched the wizard. Any configuration changes you have entered into the wizard until that point are cleared and not saved.

License Wizard changes are applied immediately, but complete license features will not take effect until reboot. Clicking Cancel does not undo any entered changes.

A-MSDU Support

This feature was introduced in AOS-W 3.3.2.7.

De-aggregation of MAC Service Data Units (A-MSDUs) is supported on the Alcatel-Lucent OmniAccess 4504, 4604, and 4704 WLAN Switches and the OmniAccess Supervisor Card III with a maximum frame transmission size of 4k bytes; however, this feature is always enabled and is not configurable. Aggregation is not currently supported.

Allow Only IP Addresses from Local Subnets

This feature was introduced in AOS-W 3.3.2.7.

You can now avoid manually adding the local subnets of each switch to the validuser ACL, making that ACL easier to manage. To do this, configure the firewall to allow only users with IP addresses in local subnets to be added to the user table using the following new command:

```
firewall local-valid-users
```

When you enable the `local-valid-users` option, the firewall examines any IP address that is denied by the validuser ACL. The default is disabled.

After you enable the `local-valid-users` option, change the validuser ACL to deny all IP addresses (the default is to allow all). In addition, make sure that DHCP is allowed. Finally, if you are using Remote APs, L2TP traffic must be allowed. Thus, the validuser ACL should be similar to:

```
ip access-list session validuser
any any svc-dhcp permit
any any svc-l2tp permit
any any any deny
```

Alcatel-Lucent does not recommend using the `local-valid-users` option with Mobile IP (29639).

Wireless

B/G Interference Immunity

This feature was added in AOS-W 3.3.2.11.

AOS-W 3.3.2.24 adds a new parameter to the `rf dot11g-radio-profile` command in the CLI. These parameters allow the user to set the interference immunity on 2.4 Ghz band. The default setting for this parameter is level 2, which is the same level the access point toleration is set in older releases.

When performance begins dropping due to interference in the band, the level can be increased to 5 for improved performance. However, increasing the level makes the AP slightly “deaf” to its surroundings, causing the AP to lose a small amount of range.

The levels for this parameter are:

- 0: no ANI adaptation
- 1: noise immunity only
- 2: noise and spur immunity
- 3: level 2 and weak OFDM immunity
- 4: level 3 and FIR immunity
- 5: disable PHY reporting

To adjust these parameters, use the following CLI commands:

```
rf dot11g-radio-profile <profile-name>
interference-immunity {Level-0 | Level-1 | Level-2 | Level-3 | Level-4 | Level-5}
```

Wi-Fi Multimedia Support for Remote APs

This feature was introduced in AOS-W 3.3.2.7.

This release introduces Wi-Fi Multimedia (WMM) support for remote APs. WMM is a Wi-Fi Alliance specification based on the IEEE 802.11e wireless Quality of Service (QoS) standard. WMM works with 802.11a, b, and g physical layer standards.

To enable WMM in an SSID profile using the WebUI, select the applicable SSID profile, then select the Advanced tab in the Profile Details section. Scroll down to the Wireless Multimedia (WMM) option, and select (check) the option. Click Apply.

To enable WMM in an SSID profile using the CLI:

```
wlan ssid-profile <profile>
   wmm
```

For more information, see the following chapters in the *AOS-W 3.3.2 User Guide*: "Configuring Remote APs" and "Configuring QoS for Voice."

Remote AP Operation on OAW-AP120 Series Access Points

AOS-W 3.3.2.7 introduced support for remote AP operation on AP-120 series access points.

DHCP Server Enhancements for Remote APs

In previous releases of AOS-W, the DHCP IP address pool for remote APs was predefined and not user-configurable. Beginning in AOS-W 3.3.2.7, you can define and configure the DHCP IP address pool for remote APs.

For more information, see "Configuring Remote APs" in the *AOS-W 3.3.2 User Guide*.

Secure Jack and Mesh

This feature was introduced in AOS-W 3.3.2.7.

You can configure the Ethernet port(s) on mesh nodes to operate in tunnel mode. Known as secure jack operation for mesh, this configuration allows Ethernet frames coming into the specified wired interface to be GRE tunneled to the switch. Likewise, Ethernet frames coming from the tunnel are bridged to the corresponding wired interface.

Unlike secure jack on non-mesh APs, any mesh node configured for secure jack uses the mesh link, rather than enet0, to tunnel the frame to the switch.

You configure secure jack operation in the wired AP profile.

To configure secure jack operation using the WebUI, select the applicable wired AP profile. Under Profile Details, select (check) Wired AP enable, and select tunnel from the Forward mode drop-down menu. Click Apply.

To configure secure jack operation using the CLI:

```
ap wired-ap-profile <profile>
   forward-mode tunnel
   wired-ap-enable
```

For more information, see "Configuring Secure Enterprise Mesh" in the *AOS-W 3.3.2 User Guide*.

PSK-Refresh for Remote APs

This feature was introduced in AOS-W 3.3.2.7.

Preshared key (PSK)-refresh allows you to refresh the PSK used by remote APs. By default, PSK-refresh is disabled. With PSK-refresh enabled, the switch accepts connections from remote APs using the previously configured PSK for the specified interval. After the interval elapses, that PSK expires and the switch uses the new PSK to authenticate remote APs. To enable PSK-refresh, you must:

1. Configure the amount of time in days or hours (known as the interval), to remember the previously configured PSK used in your remote AP deployment.

Alcatel-Lucent recommends configuring a large interval to prevent remote APs from being unable to authenticate and connect to the network.

2. Configure the global PSK. The IP address must be 0.0.0.0, and the netmask must be 0.0.0.0.

If you do not configure the global PSK, the PSK-refresh feature is invalid.

To enable PSK-refresh using the WebUI, navigate to the **Configuration > Advanced Services > VPN Services > IPSec** page. Scroll down to the IKE PSK-Refresh section and select (check) **Enable IKE PSK-Refresh**, select (check) the Interval Type (hours or days), and enter the Interval value (2-24 hours or 1-365 days). Click **Apply**. Review the IKE Shared Secrets section to ensure you have a global PSK configured.

To enable PSK-refresh using the CLI:

```
crypto isakmp psk-caching {days <interval> | hours <interval>}
crypto isakmp key <key> address 0.0.0.0 netmask 0.0.0.0
```

For more information, see "Configuring Remote APs" in the *AOS-W 3.3.2 User Guide*.

New Trap Versions

This feature was introduced in AOS-W 3.3.2.7.

A new version of the `adhocNetwork` trap, containing channel information, has been added. Also, new versions of the `adhocNetworkBridgeDetectedAP` and `adhocNetworkBridgeDetectedSta` traps, containing SNR information, have been added. The new traps will be generated along with the old versions (26518).

L3 Mobility

HA Discovery on Association

This feature was introduced in AOS-W 3.3.2.7.

In normal circumstances a switch performs a host address (HA) discovery only when it is aware of the client's IP address, which it learns through ARP or any L3 packet from the client. This limitation of learning the client's IP and then performing an HA discovery is not effective when the client performs an inter-switch move silently (does not send any data packet when in power save mode). This behavior is commonly seen in various handheld devices, Wi-Fi phones, etc., and delays HA discovery, eventually resulting in a loss of downstream traffic if any is meant for the mobile client.

Now, with the HA discovery on association feature, a switch can perform an HA discovery as soon as the client is associated. This feature can be enabled using the `ha-disc-onassoc` parameter in the `wlan virtual <ap-profile>` command. This feature is disabled by default. You can enable this on virtual APs with devices in power-save mode and requiring mobility. This option can also be polled for all potential HAs.

To use the CLI to set up HA discovery on association:

```
wlan virtual-ap default ha-disc-onassoc
```

Using VRRP IP in the HAT

This feature was introduced in AOS-W 3.3.2.7.

The HAT table now accepts the VRRP IP address as a candidate HA. Use either the switch's switch IP address or the VRRP IP address; otherwise, the switch will receive duplicate HA discovery requests from the FA.

Applying broadcast-filter arp to Virtual APs

This feature was introduced in AOS-W 3.3.2.7.

The `broadcast-filter arp` option in the `firewall` CLI command can be applied to virtual APs instead of using the option as a global firewall configuration.

The `broadcast-filter arp` option is available as part of the `wlan` CLI option in this release. If you are upgrading from a previous release, the `broadcast-filter arp` command will be disabled.

See the *AOS-W Command Reference Guide* for more information.

Configuring 802.11b Protection

This feature was introduced in AOS-W 3.3.2.7.

The current protection mechanism in 802.11b clients affects performance of various wi-fi phones. To avoid performance issues on the clients a new parameter, dot11b-protection is added to the rf dot11g-radio profile.

The dot11b-protection parameter can be used to enable or disable protection for 802.11b clients.

See the *AOS-W Command Reference Guide* for more information.

Redundancy

VRRP Interface Tracking add Parameter Removed

This feature was introduced in AOS-W 3.3.2.7.

The `add` parameter has been removed from the `vrrp tracking interface` command. When you upgrade, the add parameter is ignored. There is no change to the `sub` parameter (26552)

Adaptive Radio Management (ARM) 2.0

Support for ARM 2.5 was added in AOS-W 3.3.2.7.

Band Steering

Band steering actively guides faster 802.11a/n clients to the best available wireless channel. The result is better noise immunity, fewer sources of interference, and more available channels. If a client supports both 2.4GHz and higher speed 5GHz bands, this feature will automatically direct it to the 5GHz band for best performance.

Coordinated Channel Access

This coordinates access to a wireless channel, across all access points that share that channel, to overcome the challenges of densely populated deployments such as lecture halls, airport lounges, and conference centers.

Co-Channel Interference Mitigation

Access points with excess capacity reduce RF transmissions by reverting to air monitor mode.

Airtime Fairness

Scheduled access for dense deployments delivers equal access to all Wi-Fi clients. This feature works with all 2.45GHz and 5GHz Wi-Fi clients, regardless of its wireless chip manufacturer or standard operating system supplier.

Performance Protection

This feature prevents higher speed clients using 802.11n from being compromised by slower 802.11b/g clients.

Adaptive Radio Management (ARM) 2.5

Support for ARM 2.5 was added in AOS-W 3.3.2.12.

RX Sensitivity Tuning Based Channel Reuse

In some dense deployments, it is possible for APs to hear other APs on the same channel. This creates co-channel interference and reduces the overall utilization of the channel in a given area. RX Sensitivity Tuning Based Channel Reuse enables dynamic control over the receive (Rx) sensitivity in order to improve spatial reuse of the channel. The channel reuse mode is configured in an 802.11a or 802.11g RF management profile, and can operate in either of the following three modes:

- Static mode: The Clear Channel Assessment (CCA) is adjusted according to the configured transmission power level on the AP.
- Dynamic mode: The CCA thresholds are based on channel loads, and channel reuse is automatically enabled when the wireless medium around the AP is busy greater than half the time.
- Disable mode: Channel reuse is disabled.

Use the following CLI commands to adjust the RX sensitivity based on radio profile:

```
(config)#rf dot11a-radio-profile <profile-name>
(802.11a radio profile "<profile-name>") # channel-reuse {disable | dynamic |
static}
(802.11a radio profile "<profile-name>") # channel-reuse-threshold
```

Spectrum Load Balancing

Spectrum load balancing was updated with the release of ARM 2.5 in AOS-W 3.3.2.12.

The spectrum load balancing feature optimizes network resources by balancing clients across channels, regardless of whether the AP or the switch is responding to the wireless clients' probe requests. The switch determines the distribution of clients connected to each AP's immediate (one-hop) neighbors. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Alcatel-Lucent AP on another channel does not have any clients, load balancing will be enabled on that AP.

Spectrum load balancing is disabled by default, and can be enabled through an 802.11a or 802.11g RF management profile. The load balancing feature also requires that the 802.11a or 802.11g RF management profiles reference an ARM profile with ARM scanning enabled.

Use the following CLI commands to manage Spectrum Load Balancing:

```
(802.11a radio profile "<profile-name>") #spectrum-load-balancing
```

Spectrum Load Balancing (With ARM Disabled)

The feature was added in AOS-W 3.3.2.14.

An enhancement has been added to the spectrum load balancing (SLB) feature, allowing RF neighborhoods to be manually created in deployments in which ARM assignment and scanning are disabled. In deployments with scanning enabled, SLB works because the APs are able to find each other and create RF neighborhoods. But without scanning, RF neighborhoods are not formed.

To solve this limitation, a new parameter has been added to the CLI that allows RF neighborhoods to be manually created. SLB is enabled and SLB-domain is defined, APs belonging to that SLB-domain are used for load balancing.

```
rf dot11g-radio-profile <profile-name>
```

```
spectrum-load-bal-domain <spectrum load balancing domain name>
```

This command is also applicable to 802.11a radio profiles, not just 802.11g.

Security

Master-Local IPsec Key Configuration

This change was implemented in AOS-W 3.3.2.18.

Users must now manually configure a matching PSK on both the master and local switch before the devices can communicate with one another. Previously, this step could be avoided by using the default configuration of "`localip 0.0.0.0 ipsec <switch provided default psk>`." This default setting will no longer be automatically generated while going through the setup dialog.

Wired Containment of Rogue Devices

This feature was added in AOS-W 3.3.2.14.

Previously, Alcatel-Lucent APs on a trunk port supported wired containment of devices only on native VLANs. This feature has been enhanced to contain devices on tagged VLANs as well. New parameters have been added to the `show AP` command, allowing you to monitor this improvement.

VLAN Gateway mapping is displayed in the output of `show ap monitor wired-mac ap-name <ap-name> enet-mac <enet-mac>`.

```
Wired MAC Table
---------------
mac                ip            age
---                --            ---
00:0b:86:51:2f:70  10.15.69.80   3m:3s
00:17:e0:01:97:e7  10.15.69.254  3m:6s
00:22:15:cb:0c:7e  10.15.69.50   1m:5s
00:0b:86:f0:32:50  10.15.69.52   3m:6s
00:0b:86:41:1d:40  10.15.69.1    2m:7s
00:0b:86:cd:cf:70  10.15.31.99   1m:33s
00:1b:fc:ed:15:a3  10.15.69.205  3m:2s
00:1a:1e:c0:9a:ea  -             4s
00:30:48:5d:5d:52  10.15.69.200  3m:2s
00:0b:86:61:10:a8  10.15.31.110  33s
00:0b:86:61:13:00  10.15.69.36   9s
00:17:e0:01:97:df  10.15.31.254  2s
00:17:e0:01:97:e1  10.15.33.254  1m:53s
00:0b:86:61:23:00  10.15.69.253  2m:13s
00:17:e0:01:97:e2  10.15.34.254  1m:51s

Wired MAC Table: Gateway MACs
-----------------------------
mac                ip            age     tagged
---                --            ---     ------
00:17:e0:01:97:df  10.15.31.254  3m:24s  No
00:17:e0:01:97:e1  10.15.33.254  1m:53s  Yes
00:17:e0:01:97:e2  10.15.34.254  1m:51s  Yes

Wired MAC Table: Gateway VLAN Info
----------------------------------
vlan  gw-mac             gw-ip
----  ------             -----
533   00:17:e0:01:97:e1  10.15.33.254
534   00:17:e0:01:97:e2  10.15.34.254

Config Wired MAC Table
----------------------
mac
---
```

A count of tagged packets processed and learned VLANs is displayed in the output of `show ap monitor debug status`.

```
WLAN Interface
--------------
bssid              scan    monitor  probe-type  phy-type  task   channel  pkts
-----              ----    -------  ----------  --------  ----   -------  ----
00:0b:86:5c:f7:08  enable  enable   sap         80211a    tuned  153      254357
00:0b:86:5c:f7:00  enable  enable   sap         80211b/g  tuned  6        1106455

Wired Interface
---------------
mac                ip            gw-ip         gw-mac             status  pkts  macs  gw-macs  tagged-pkts  vlan
---                --            -----         ------             ------  ----  ----  -------  -----------  ----
00:0b:86:cd:cf:70  10.15.31.251  10.15.31.254  00:17:e0:01:97:e0  enable  210   16    3        103          2
```

Additionally, logs at the info level indicate "tagged wired containment," as well as "tagged gateway MACs."

Issues and Limitations Fixed in AOS-W 3.3.2.24

This release contains all fixes up to and including those in AOS-W 3.3.2.7. The following issues and limitations have been fixed in the AOS-W 3.3.2 release:

Table 2 *Fixed in AOS-W 3.3.2.24*

Bug ID	Description
27944	When a destination alias is added, it is correctly displayed in the summary screen.
35349	The AP Status LED on the front of switches now works correctly.
35727	PMK cache memory leak is fixed.

36212, 38287	When the system clock is changed on a switch, the following warning message is displayed to inform the user that the switch must reboot:
	`WARNING: Changing the system clock will require a reboot of the controller.`
	This message is followed by another message asking the user:
	`Are you sure you want to continue(y/n): y`
	`Switch Real Time Clock is changed. The controller must be rebooted now.`

36327, 36723	An fpcli memory leak has been fixed.
36652, 36960	Unexpected switch behavior caused by a datapath exception has been fixed.
37027	VRRP flapping, which results in AP bootstrapping when running `show inventory` has been fixed.
37675	The WebUI no longer returns a blank page when viewing a policy with a large number of rules.
37783	The default ap-inactivity-time has been increased to 20 sec. This reduces the message flow to WMS on master due to discovery of APs with low RSSI by AM or by an AP on its home channel.
38073	SSLCipher settings of web server have been modified such that LOW, MEDIUM and HIGH cipher aliases are cumulative. LOW=LOW+MEDIUM+HIGH, MEDIUM=MEDIUM+HIGH and HIGH=HIGH. This allows webserver to allow strongest SSL cipher according to configuration settings.
38569	Japanese characters display and print properly in the Poicy Text section of the Guest Access tab.
38661	Memory leak related to Auth timers is now fixed.

Table 3 *Fixed in AOS-W 3.3.2.23*

Bug ID	Description
33737	An auth process crash, sometimes accompanied with the error message “Module Authentication is busy,” that occurs when a new access list is added to the switch has been fixed.
35285	Idle wireless VPN users are no longer deleted from the auth table when ICMP response from the inner IP address is returned on a different ingress tunnel.
36736, 36796, 37076, 37307	An issue in which the tar was unable to archive the core files with long filenames has been fixed. The size of the file name, including paths, is limited to 100 bytes and this was previously exceeded for the arci-cli-helper on non-legacy platforms.
36746	Descriptions of the 10GB ports added in the CLI are preserved across reboots.
36810	When using XML-API, passwords may have trailing spaces.
37247	An auth module crash caused by an inconsistency of the ACE table between auth and datapath has been fixed.
37250, 37260	An issue in which STM is unable process messages from connected APs, resulting in the APs never coming up and continually rebooting, has been fixed.
37643	An auth process crashe caused by user entries cached in a local db tied to a VPN user role that no longer existed on the switch has been fixed.
37703, 37499	Clients can now succesfully authenticate against configured 802.1x profiles and the associated auth module crash has been fixed.

Table 4 *Fixed in AOS-W 3.3.2.22*

Bug ID	Description
31976	When a halt command is issued on an OAW-S3 or 4X04 Series WLAN switch, the Power LED is solid green, the Status LED is solid red, and any active LEDs are off.
32097, 35616	An authorization memory leak was causing unexpected behavior when executing the `show memory auth` command. The memory leak has been fixed.
36183	Encrypted H323 traffic was not handled correctly (denies in the datapath) and has now been corrected.
36380	A switch malfunction when auto-provisioning memory was not freed when the master switch sends requests to an LMS has been fixed.
36459, 36947, 36997, 37032, 37827, 28508	Datapath timeout issue have been fixed.
36477	Packet drops and multicast issues caused for clients behins a RAP caused by TX failures on the switch has fixed.
36675	When the link is lost on a GigE port an Alcatel-Lucent 4324, the 4324 does not have to be power-cycled to reestablish the link

Table 4 *Fixed in AOS-W 3.3.2.22*

Bug ID	Description
36817	The asterisk(*) is no longer accepted in usernames and passwords used for LDAP authentication.
36819	When seven or more clients are connected to a single OAW-AP125, clients are no longer disassociating and associating when additional clients are added.
36844, 37131	A kernal panic issue on S3 or 4X04 Series switches has been fixed.
36864, 36958	The traps wlsxAccessPointIsUp and wlsxAccessPointIsDown now disply the coreect information in the correct fields.
37139	User counts displayed by `show user-table` and `show aaa state configuration` now correctly display the same number of users.
37183	When VLAN Pooling is enabled, IPv6 router advertisements (RA) are sent via unicast to ensure that clients see the RA of a spcific VLAN only.

Table 5 *Fixed in AOS-W 3.3.2.21*

Bug ID	Description
23154, 27433	The local switch's hostname is no longer incorrectly changed to the host IP address, defined in the netdestination command on the master, after the switch is rebooted.
26303	Certificate validity times are now handled properly with respect to the local time.
29022	User credentials in an internal DB of a switch, created using a MAC address with a colon as a delimiter, can now be successfully modified when done through the WebUI.
33362, 35170, 35576, 36562	A flash backup can be completed successfully, when enough free space is available, using the `backup flash` command.
34243	The crash.tar file is no longer corrupted when extracted using the WebUI.
34679	When a switch is being used as a DHCP server (to provide option 252), an extraneous space is no longer added by the switch to the option 252 URL.
34975, 37034, 36814	An auth crash occuring in handle_tunnel_id_update has been fixed.
35857, 36558, 36735, 36875, 37022, 37040	The STM module no longer unexpectedly restarts on the switch when band-steering is enabled.
36249	Saving a switch configuration with a large number of netdestination entries no longer causes an auth malfunction.
36508	OAW-AP125s can send CTS-to-self when 11g protection is active and any g-tx-rates are selected.

Table 5 *Fixed in AOS-W 3.3.2.21*

Bug ID	Description
36560	SAPM no longer tries to generate a config message for an AP that has been marked for full reconfiguration.
36731, 36760, 36759	The command `show ap association` has been improved to be more effcient.
36752	IPv6 multicast frame (converted to unicast) are no longer leaked to the client when using VLAN pooling and battery boost is enabled.
36915	Clock drift has been adjusted to eliminate VRRP flaps caused by missed heartbeats from the master switch.

Table 6 *Fixed in AOS-W 3.3.2.20*

Bug ID	Description
30707, 33778, 33777, 36010	Unexpected switch behavior caused by a datapath exception due to a double free issue has been fixed.
32803, 35350, 35134	An auth hang issue due to frequent RAND number generation has been fixed.
33890	A new parameter type netmask was added to support subnet mask 240.0.0.0. This parameter type validates that the netmask added is a valid IP address.
35774	The switch no longer hangs during SCP file transfer after 504 copies. However, any copies after 503 will fail because the system runs out of memory.
35939	Additional debug code has been added to AOS-W to capture more information in the event that similar unexpected switch behavior, such as that reported in this bug, occurs in the future.
36220	The VAP registration queue is no longer getting stuck, resulting in active APs no longer being incorrectly displayed as inactive in the CLI.
36642	OAW-AP12x does no longer turns back on immediately after converting to APM mode.

Table 7 *Fixed in AOS-W 3.3.2.19*

Bug ID	Description
20274, 35673	Whenever VRRP changes state, tunnel(s) configured with VRIP as dstip or srcip gets a notification and oper state is modified. If keepalives are turned on, vrrp has no effect on tunnels.
33964, 34274, 35723	The Captive Portal login screen preview is now correctly displayed in the Maintenance tab.
34192, 36017	Unexpected switch behavior caused by a datapath timeout has been fixed.

Table 7 *Fixed in AOS-W 3.3.2.19*

Bug ID	Description
34759, 35330	An unexpected switch behavior caused when an RFprotect sensor radio's sap_info is registered but not associated with a sap_info_radio_t has been fixed.
35107	RF plans are no longer lost after rebooting the switch.
35118	AMs can now obtain the correct VLAN ID, allowing the AM to successfully DoS traffic from a rogue AP.
35299	The protocol field of tagged frames is now parsed correctly and the age-out mechanism for the has table has been corrected, allowing AMs to reliably contain rogue APs.
35393	The "blacklist-on-failure" feature now works successful for machine-auth.
35894, 35895	A RAP failure caused by an inability to handle kernal paging requests has been resolved.
35916	An AP-125a/b/g can be configured, managed, and used as an RFprotect sensor.
35362, 33072, 35080	Memory is now correctly freed after the client sends a deauth and dissociates from the AP.
35540	1000Mbps speed and full duplex can now be hardcoded for GE ports on the S3.

Table 8 *Fixed in AOS-W 3.3.2.18*

Bug ID	Description
25202	AOS-W upgrades, via the WebUI, on hardware platforms with 128MB flash memory now work correctly.
33501	MPDU spacing has been changed to 8us to improve performance of Intel clients.
34031, 34649	An issue in which a delay in displaying the Captive Portal authentication screen is shown as 1.8 million seconds has been fixed.
34093, 35328, 35810	The packet offset and length received from the kernel will now be validated, which will prevent the SAPD from crashing.
34356, 35217	SAPD is now notified whether the LMS address is a VRRP address. Therefore, if SAPD detects a "broken tunnel" (as indicated by ICMP errors) and the LMS is VRRP, SAPD rebootstraps to the same address. Otherwise, SAPD will move to the backup LMS.
34362	STM is now notified of the association cleanup when a client roams away from FA/HA.
34389	AMSDU + AESCCM is disabled on all legacy (non-XLR) platforms.
34484	The "Invalid Source MAC Address" error message no longer appears on a Cisco switch while passing an IPsec tunnel reply from a local to a master switch.
34661, 35114, 35225, 35545	An issue in which the number of times the backup switch became the VRRP master incremented, causing all APs to reboot, has been fixed.

Table 8 *Fixed in AOS-W 3.3.2.18*

Bug ID	Description
34841	Previously deployed APs no longer incorrectly appear on the suggested APs list.
34843	The OAW-AP125 now works correctly with the Avaya Cajun P33T switch.
35128	An SNMP engineboot count mismatch has been fixed.
35327	A crash in the ISAKMPD module, caused by a memory leak, has been fixed.
35339	The 40MHz channel is now supported in the country code IN (India).
35362, 33072, 35080	Memory is now correctly freed after the client sends a deauth and dissociates from the AP.
35540	1000Mbps speed and full duplex can now be hardcoded for GE ports on the S3.

Table 9 *Fixed in AOS-W 3.3.2.17*

Bug ID	Description
29842	Error messages and auth modules crashes no longer occur when `show acl acl-table` or `show running-config` is run.
33682	A crash caused by the “via” pointer being accessed, without being validated, has been fixed.
34039	Management authentication to an external authentication server is now reliable.
34219	Policy rules are now correctly displayed in both the WebUI and the CLI.
34404	Lowering of ARM maximum TX power successfully takes effect after the adjustments are made.
34434, 34432	Controllers no longer incorrectly mark the DSCP bits in the GRE packet of Cisco PVST+ to a non-zero value.
34630	The nd of vlan_list array is no longer written off, fixing the stm crash when `show ap essid` is used.
34804	A number of error messages related to missing XML files no longer appear in the console log.
34977	nUserAPBSSID for wireless clients is now reported correctly by switches with OKC enabled.
34986	VOIP rtcp-inactivity configuration is successfully saved after a reboot.
35100	AIFS for Spectralink VIEW phones is now correctly set to 2.
35248	Additional debug code has been added to the existing packet tracing tool.

Table 10 *Fixed in AOS-W 3.3.2.16*

Bug ID	Description
32733, 34348, 34482	Rx descriptors were not self linked anymore causing overruns in short rx packets. The intr code was processing them as fatal but the BH would not treat it as fatal, causing a code lock on just processing overruns. Therefore, beacons were not prepared in right time slots. This code fixes overruns and adds to limit to Rx Desc processing in each pass so that beacons can really go out.
34931	With this fix, only new 64-bit tx/rx counters are read when constructing a statistics message for STM. Now, stations that are not associated to the AP are not included, so the error message will not be generated.
35091	Captive Portal pages now display the correct default images.

Table 11 *Fixed in AOS-W 3.3.2.15*

Bug ID	Description
26819	Client-IDs are now correctly sent in DHCP discover, request, and renew packets.
31190	EO2SA phones successfully handover when wpa-fast-handover is enabled.
32527	An issue in which the datapath session for three-way party calls was being dropped after several seconds has been fixed.
33149, 33442, 28868	The method by which an AP synchronizes its time with a switch has been enhanced. The time is provided by the switch once per minute, instead once every hour. Previously, the potential gap in this synchronization could cause the AP's keep-alive message to be delayed, causing the AP to age out.
34181	ACL names containing spaces are now successfully copied when configurations are pushed to local switches.
34222	When tspec enforcement is enabled and ADDTS for voice (UP 6 or 7) is received from non-voice client, stm no longer crashes due to a lack of null pointer checks.
34263	The RADIUS server group is saved when sending an accounting start message, ensuring the that accounting stop message is correctly sent to the RADIUS accounting group, instead of the authentication group.
34327	Fixed a Captive Portal problem where the local switch may not intercept Captive Portal requests if the configuration is too large.
34657	Double free of nodes no longer occurs for action frames not in powersave mode.

Table 12 *Fixed in AOS-W 3.3.2.14*

Bug ID	Description
30165, 31702	An issue in which H-323 phone calls are established and maintained but eventually fail when attempting to attach to a new call server has been fixed.
31423	An issue in which the an S3 in slot 0, in a fully populated chassis (four M3s) crashes causing an S3 in slot 2 to reboot has been fixed.

Table 12 *Fixed in AOS-W 3.3.2.14*

Bug ID	Description
32153	When logging level is set to informational for the system log, PoE messages are no longer shown. PoE messages appear when the logging level is set to debugging.
32154	RF plan data shown in the GUI now correctly matches the data shown in the CLI.
33519	An issue in which roaming VoIP phones retain their in-call status on their related switch until the STM process or the switch is restarted has been fixed.
33712, 32906	An issue where the Captive Portal logon wait screen appears, despite CPU usage being low, has been fixed.
33789	An issue in which the configuration manager crashes while exporting an RF plan, causing the switch to restart, due to low memory has been fixed.
34016	Use of an snmpget for CPU load OIDs now correctly returns the requested OID.
34111	A rule, with an action marked as reject, in the firewall policy does not reappear after being deleted, once the configuration is saved.
34129	When a RAP fails to reconnect, it will now continue sending PADI packets until it reboots after four (4) hours, and will continue to do the same after rebooting.
34257	The 5 GHz band has been enabled for you use in Thailand (TH).
34324	When an XML-API 'user authenticate' request is sent and the corresponding radius request times out, the XML-API returns random response. This issue has been fixed.
34470	An issue in which a Captive Portal configuration error occurred when sending an XML-API call has been fixed.

Table 13 *Fixed in AOS-W 3.3.2.13*

Bug ID	Description
28781, 33748	The commands `mgmt-user webui-cacert`, `mgmt-user localauth-disable`, and `mgmt-user ssh-pubkey` are not deleted from the config file on an image upgrade.
29905, 31026, 31013, 33624, 33761	This fix addresses the rare case of datapath timeout caused by data corruption due to memory underruns on packet transmission, while handling high volume of flooded traffic.
30116	The trim-fqdn option now works when the credentials are in the format of "domainusername" against LDAP and TACAS servers.
31112	An issue in which APs rebooted under a heavy load of small packets has been fixed.
31707, 33267	When an AP changes from AP to APM mode, the error message `an internal system error has occurred at file ncfg_cmn_util.c function ncfg_get_item_display_string line XXX error Internal error` are no longer displayed.
31797	When upgrading RFProtect, the sensor name is maintained from version to version.
32009	A number of improvements have been made to increase RAP stability.
32121, 32203	A switch reboot issue due to low memory in configurations using Captive Portal and a high number of users has been resolved.
32195	When using **Save Configuration** in the WebUI on a master switch, configuration changes are not lost when pushed to local and redundant masters.

Table 13 *Fixed in AOS-W 3.3.2.13*

Bug ID	Description
32394	When a configuration is pushed from a Master switch to a Local switch, a time computation message now shows up in the switch's system log.
32607	Users will now see the correct Captive Portal logon page, based on the cp-profile, instead of the default.
33072	An AP reboot issue caused by decreasing amounts of free memory has been fixed.
33388	HT-40 MHz channels now work correctly for country code IL (Israel).
33496	An issue in which delays in 802.11 association response caused Polycom/Nortel 6120 to lose voice connectivity while roaming has been fixed.
33655	An AP crash issue, which occurred when certain unusual frame sequences appear during heavy bursts of traffic, has been fixed.

Table 14 *Fixed in AOS-W 3.3.2.12*

Bug ID	Description
28275, 28279, 28280, 30147, 32183	An issue where PAPI sessions from a local switch are not reaching the master has been fixed.
29709	VRRP advertisements are sent at the configured interval on the S3, 4504, 4604, and 4704 switches.
30927	If Radius accounting is enabled, the Radius accounting stop message is sent to the correct server group after switching to a new VAP.
31672, 31364, 31365	UAPSD statistic reporting has been fixed; resolving the issue involving high radio reset counts.
31702, 30060, 30165	Session updates no longer fail when a unidirectional deny session exists.
31830	In the WebUI, details for channels 100 to 140 are correctly displayed under Monitoring > Air Monitor > Channel.
32070	An issue where ARM multi-band assignment was causing ESSIDs to not appear on APs after changing bands has been fixed.
32258	An issue where 802.11a radios were shown as having an HT-20 channel width, despite being configured a HT-40, has been fixed.
32568	In ARM, when single-band mode-aware is enabled for a single-radio AP, ARM no longer attempts to change the band unexpectedly.
32750	Wired users are now correctly directed to the Captive Portal logon page when connected through an untrusted trunk port.
32931	An issue where APs were not scanning after bootup has been fixed.

Table 15 *Fixed in AOS-W 3.3.2.11*

Bug ID	Description
23706	AOS-W now provides SNMP support for fan and power supply status.
27401	Fan failures are now reported correctly.
27796	Issues with ssh mgmt authentication using public keys has been fixed.
28144	R-values are now calculated and displayed correctly.
28348	5 GHz channels are enabled for Russia and Thailand.
28627, 30095	AP-61 performance has been improved when confronted with non-802.11 interference.
29528	All members of a port channel will successfully come back up after a reboot.
29627, 27502, 29124, 31251, 30947	APs will now recognize that RF Plan information has been removed and will instead use the correct configuration settings instead.
30703	Channels 149 - 165 have been enabled for use indoors in Macau.
30875	The “show ap association” command now displays the correct, up-to-date AP status.
30925	The logging message for adding a user through XML provides correct IP addresses.
30983	The issue where APs reboot due to HT clients sending HTcap IE to an AP that is not HT capable has been fixed.
31104, 31631	The issue where clients have trouble decrypting broadcast/multicast frames from an AP has been fixed.
31202, 32215	TotalAPCount and TotalSTACount, which are displayed in “show wms counters,” always show positive values.
31481	AP’s will not reboot if the switch probe contains an unsupported rates element.
31546	When adding an user via the XML API, a MAC address must be specified if the user does not exist in the user table.
31706	Medium time is now computed correctly for Nokia N902il phones.
31726	The method used to distribute PUBSUB_SERVICE_ALG information has been improved to ensure that ALG information is published correctly.
31908	The MAC address does not need to be specified if the user exists in the user table.
32100	Issues where the H323 ALG was failing have been fixed.
32137	High priority traffic is now correctly given higher precedence than low priority traffic.
32192	A mismatch between the TID on a frame and the driver’s interpretation of the TID has been fixed.
32353, 32159, 31898, 30222, 31788, 31987, 32491, 32679, 32157, 30011	A crash in the auth module, followed by slow connectivity, has been resolved.

Table 16 *AOS-W 3.3.2.10*

Bug ID	Description
32126	The WebUI now correctly displays the expected information under **Monitoring > Switch > Access Points**.

Table 17 *AOS-W 3.3.2.9*

Bug ID	Description
26668, 28087	The “halt” command no longer reboots the switch.
27102, 31696	When performing an SNMP Get, the switch will return the correct OID.
27944	When a destination alias is added, it is correctly displayed in the summary screen.
29589	A switch will no longer reboot due to a control processor exception.
29754	Performing a “write mem” on a local switch no longer causes APs terminating on that switch to become unresponsive.
30397	In a Master/Master redundancy deployment, the “show switchinfo” command correctly displays the master’s IP address instead of 0.0.0.0.
30795	APs manually classified as rogue correctly appear that way in the WebUI.
30853, 30920	The issue where crashes in Auth and STM were followed by slow dot1x authentication has been fixed.
30963, 30239	The AP-125 now successfully transmits buffered frames if the client polls the AP with QoS-Null with PS bit set.
31232	Nokia E-series phones now work correctly when stateful SIP processing is enabled.
31274	Voice troubleshooting now works correctly from the WebUI.
31480	The issue where APs were rebooting every hour after rebooting to 3.3.2.7 has been resolved.
31545	The issue where use of the command “show ipc statistics app-name <any valid argument>” causes a memory leak has been fixed.
31672, 31364, 31365	The issue where radio resets were abnormally high has been fixed.

Table 18 *AOS-W 3.3.2.8*

Bug ID	Description
21507, 24164, 25844	The issue where APs are not receiving information from WMS and MMS servers has been fixed.
25611, 29956	DST NAT correctly works for wired clients.
29106	User roles specified in user_add are now correctly added.

Table 18 *AOS-W 3.3.2.8*

Bug ID	Description
29308	The following show commands have been added to “show tech-support:” • show ap mesh active • show ap mesh topology long
29430	An issue in which and Auth crash occurs while debugging a RAP has been addressed.
29536	The low memory condition caused after upgrading from 3.1.1.x to 3.3.2.x has been fixed.
29571	The Server derivation rule no longer fails to match when the added VSA is an integer type.
30196	All clients are able to communicate with network after successfully authentication.
30291, 30810	The issue preventing the upload of a graphic file for use with guest provisioning or update the policy text has been resolved.
30324	An S3 crash issue accompanied by a datapath timeout error has been addressed.
30364	An issue causing an STM crash after upgrading 3.3.2.5 has been fixed.
30595	Switches now correctly decode AARP packets.
30612	Users can now be more easily tracked through a switch’s log files.
30637, 21671, 21672, 29851	The issue in which the CP and DP user tables are out of sync has been addressed.
30705	Correctly creating a new Reg Domain through the Web UI no longer results in errors.
30720, 30053	A database sync failure issue has been fixed.
30739, 30793	Clients connecting through a TKIP or mixed mode WPA/WPA2 SSID now successfully acquire an IP address from the DHCP.
30768	A RAP datapath timeout issue has been fixed.
30866	The issue where the WMS database continues to grow, not matter the limit, has been addressed.
30883	Vista clients are now able to get an IP address from a DHCP server when 802.1p priority is configured.
31009	An issue where the instrumentation required to dump the correct register becomes set during a kernel panic has been addressed.
31239	The issue in which improved background scanning in APs has caused APs, which have been discovered on other channels during scanning, to be aged out faster.

Table 19 *AOS-W 3.3.2.7*

Bug ID	Description
30166, 30144	The issue in which APs did not transmit packets due to a transmission descriptor failure has been resolved.
30175, 30627, 30714	When the band steering table becomes full, multiple entries will age-out to avoid lookup/replace at every insertion when the table is full.
30668	A memory leak in the STM module has been addressed.

Table 19 *AOS-W 3.3.2.7*

Bug ID	Description
10148	Fast ethernet port detection problems on client devices equipped with a GigE NIC have been fixed.
23265	The issue in which Intel-based Macs using WPA2-AES and WPA-TKIP authentication are unable to associate with their networks has been fixed.
24275, 27610, 29521	The AP provisioning page now correctly displays the number of APs per page, as set by the user.
25069, 24818	When a new Captive Portal certificate is uploaded, the changes now take effect immediately.
25706, 25847, 23558, 29043, 28935, 27891	The issue involving background scanning interfering with location tracking has been fixed.
26328, 23297, 24643	JPG files with spaces in the file name can now be uploaded for use with the RF Planner.
27234	The issue with a user not appearing the user table and being unable to send traffic, despite receiving an IP address, has been fixed.
27646	The base MAC address is no longer required to create a working heat map in the RF Planner.
27787, 27847	The issue with AP impersonation detection has been fixed.
28498, 30042	The security logs created by the switch display correct and valid source and destination IP addresses.
28615	The “show acl hit” CLI command now correctly displays the statistics.
29106	A new AAA profile called default-xml-api has been created. This profile will be used if the XML-API is used to communicate with the switch regarding users that have not yet associated.
29135	The issue with Air Monitor not getting packets and causing ARM to not scan properly has been fixed.
29368	The RF Plan now correctly shows an AP's assigned channel.
29427	The issue in which external antenna is not enabled when the RAP, configured for external antenna, is unable to connect to the switch has been fixed.
29459	The issue in which a RAP is unable to connect to the switch resulting in the antenna gain not being set and the default at 0 has been fixed.
29510	Password modifications are now correctly retained between reboots.
29552, 29943	Statistics for stations that are not associated are no longer saved and allocated memory is freed.
29559	The issue resulting in WMS configuration changes made on the master switch not being saved on the local has been fixed.
29640	Location issues caused by invalid RSSI data have been fixed.
29853	The issue in which the response packet from the switch does not match the expectations of the server has been fixed.
29978	The issue causing CPU load to reach 100% due to MUX tunnel authentication conflict has been fixed.

Table 19 *AOS-W 3.3.2.7*

Bug ID	Description
30146	Clients now receive an IP address from the DHCP server when connecting to an 802.1X VAP with bootstrap-threshold value other than the default.
30181, 30400	Logs.tar files can now be extracted without issue.
30199	The issue with show ap association command returning no data has been fixed.
30266	The issue resulting the STM consuming CPU resources has been fixed.
30326	The AP12x Series now work correctly with Alcatel-NOE phones.
30431	Stateful 802.1x now works on Linux-based Radius servers.
21571	Certificates that do not have a trailing new line can be uploaded using the WebUI.
24117	Issues with 802.11g interference causing low throughput for clients attached to 802.11a has been fixed.
25228	The issue with 1% packet lost during the TKIP P1 key not being ready has been fixed.
25412	Re-provisioning issues with APs have been fixed. Now, an AP is populated with static IP.
25917	Broadcast and multicast from a SRC-NAT subnet is now allowed.
26812	Mobility trail information for wireless clients is now available.
26676	Retry issues with the Cisco phone can now be reduced using the 'single-chain-legacy' configuration setting in HT Radio Profile. You should, however, enable this setting only if the retries are very high.
26885	The default value for idrequest period is now set to 3 seconds.
26886	The WLAN switch will now send an EAP-request when a 802.1x authentication is aborted due to a station timeout.
27465	A high CPU usage issue preventing users from authenticating has been fixed.
27582	Management users can now be authenticated by the internal local-userdb using the WebUI. You can select the following roles from the WebUI (Configuration->Security->Authentication->Servers-> Internal DB): • root • guest-provisioning • network-operations • read-only • location-api-mgmt To enable this feature using the WebUI, go to the Configuration -> Management -> Administration page and select Server-group as ‘Internal’.
27596	The permanent bridge MAC warning message has been removed.
27876	The raw packet capture is now enabled in OAW-AP125 with support for PPI header format which can now carry more 802.11n specific information.
28001	The MAX ERIP data is now available for APs in Europe region.
28141, 28090	The CPU spike and low memory issues have been fixed.
28204	Now the algorithm received in the AUTH message from client's AUTH request is sent including the list of unsupported algorithms.

Table 19 *AOS-W 3.3.2.7*

Bug ID	Description
28913	The time taken to generate a 4096 key is longer than the default timeout value of the CLI command. The button to view the key is enabled only after the timeout value.
29137	The issue with panic caused by the sequence re-association request, association request, re-association response, association response message from APs have been fixed.
27081	The issue with tunnel entries not being deleted after a clean-up has been fixed.
29045	When GRE tunnel parameters are changed, static routes that use that tunnel are lost. This issue has been fixed.”
29310	Issue with radio profiles not getting copied during upgrade has been fixed.
29314	Issues with multiple APs reboot or re-configuration causing crypto stalls have been fixed.
29317	Switch crash issues due to datapath exception have been fixed.
29400	If the web server (or Captive Portal) certificate configuration is invalid, the switch will fall back and use the default certificate. This will cause browsers to notify a mismatch between the certificate name and IP address.
29469	The process to build RF neighbourhood information is now optimized and hence reduces association delays.
29816	CPU spike issues in the switches have been fixed.
29563	Issues with clients not being able to get an IP address when connecting to open SSID has been fixed.
29878	Issues while upgrading to 3.3.1.18 has been fixed. The default interval between EAP identity requests is now set to 30 seconds.
29898, 29957, 29885, 29914	Multiple issues with switches crashing due to datapath timeout error has been fixed.
21897	The issue with a Microsoft Vista client behind NAT device not being able to connect to the switch has been fixed.
26589	Stateful firewall global setting parameters are displayed properly in Firefox and IE browsers. The edit box for configuring Monitor Ping Attack (per sec) in the Configuration > Advanced Services > Stateful Firewall > Global Settings page works correctly in Firefox and IE browsers.
26653	A new parameter has been added to fix the Apple connectivity issue due to WPA2 key-exchange delay. See the “What's New in 3.3.1.10" section of the AOS-W 3.3.1.10 release notes for more information.
27041, 29232	The age out of entries is now correctly displayed in the 'show ap active' and 'show ap association remote' command.
27654, 27173	Throughput performance issues with WPA2-AES and WPA2-PSK have been fixed.
27594	Crash issues with OAW-AP125 when connected to enet with mis-match port setting have been fixed.
27627	The issue with client entries not being removed in spite of the timeout value set in sta-inactivity-timeout has been fixed.
27648	The issue with incorrect temperature alerts on M3s have been fixed.
27772	The issue with a local switch not forwarding ARP packets when voip-proxy-arp is disabled or not used VRRP has been fixed.

Table 19 *AOS-W 3.3.2.7*

Bug ID	Description
27896	The 802.11a channel is now enabled for Ecuador (EC) country code.
27957	The breadcrumbs text on the Security > Authentication > Advanced page now displays the correct information.
27734, 27724, 28999, 28028	Multiple auth module crash issues have been fixed.
28356	Issue with AMAP protocol not working with OAW 4308 WLAN switch has been fixed.
28580	Issue with Supervisor Card III crashing during to datapath timeout has been fixed.
29398, 28658	The issue with Nanny module crash causing the switch to reboot has been fixed.
28672	The issue with VRRP failure not happening between local switches has been fixed.
28962	The switch now retains the static IP of the L3 GRE tunnel interface after a reboot.
22929	The connectivity issue with a wired device connected to enet1 has been fixed.
23306	Extraneous error message generated during AP boot up has been fixed.
23487, 24725	You can now use the VRRP address (VIP) as a multiplexer server address to terminate multiplexors.
25206, 27429, 26193, 28094	The 4504, 4604, or 4704 and Supervisor Card III switches no longer occasionally drop packets during traffic floods.
25805	If the cp-redirect-address is disabled, a DNS query is now forwarded to the appropriate DNS server correctly.
25966, 28346	STM now sends the AP-State message in batches when there are large numbers of BSSIDs
26461	When a running configuration is copied via FTP, the configuration file is copied to a directory if it is specified. By default, the configuration file is copied to the root directory.
26986, 16085, 16092	Using the show log crypto command on a switch no longer occasionally crashes the switch
27287	When an AP provisioned with server IP is updated to use a server name, the WebUI displays only the server IP instead of the server name after a reboot. This issue has been fixed.
27345	Datapath timeout causing switch to crash has been fixed.
27415	The Captive Portal proxy can now be connected to port 80 in the base operating system.
27522	When WMM is enabled on a virtual AP (VAP) and the channels are busy, the wireless client drops incoming calls. This issue is fixed.
27544	An issue with 4324 switch causing it to crash frequently has been fixed.
27623	The issue with 'write mem' command sometimes causing the switch to crash has been fixed.
27645	Auth crash issues have been fixed
27657	The temperature display for OAW-AP12x has been removed.

Table 19 *AOS-W 3.3.2.7*

Bug ID	Description
27680	Customized Captive Portal users are redirected properly when the initial authentication fails.
27688	When Captive Portal is used for VPN users, a DNS response to the client is now received through the tunnel properly.
27705	Retrieving the switches CPU load via SNMP was inaccurate, this issue is resolved.
27732	The WebUI will now escape the dot (.) character in the AP Name, floor name, building name, and campus name when sending FQLN using the “provision-ap fqln <FQLN>” CLI command.
27748	The issue with APs not rebooting after a network outage has been fixed.
27775	The issue with Supervisor Cards (SC1 or SC2) in slot 0 and Supervisor Card III in slot 1 resolving to the same base MAC address has been fixed.
27841	The issue with not being able to add more than two Gigabit Ports under port channel interface has been fixed.
27850	If the logging level for the web server was set to debug, the log file size grew uncontrollably causing the system to reboot. This issue has been fixed.
27882	IDS features are disabled properly when WIP license is not installed.
27929	STM crash issues have been fixed.
27949	VLAN assignment from RADIUS server now works properly when user is authenticated with LEAP
27965	The issue with S3 crashing has been fixed.
28007	The issue with not being able to set expiry time for a user in the internal DB has been fixed.
28502	The issue with clients not connecting to WPA-PSK-TKIP VAP if there is a Cisco 3560 as a L3 gateway between an AP and master switch has been fixed.
28061, 28223, 19977	The issue with the switch reboot resulting in kernel panic has been fixed.
28228, 27965	Switch reboot during network flood has been fixed.
27776, 26750	Enabling the `ids-high-setting` in the IDS profile for an OAW-AP125 no longer occasionally causes the AP to crash under a high load.
27734	A cause of MAC auth module crashes when both MAC and 802.1x authentication are enabled has been resolved.
27696	Installing a new OAW-AP125 a/b/g in a network running AOS-W 3.3.1.8 (or earlier) no longer occasionally causes other APs in the network to reboot.
27514	Disabling rogue AP classification now works as expected (all interfering APs are classified as rogues).
27477	When an AP changes channels, the switch now sends the appropriate trap group.
27405	The switch now correctly reports the power-saving state of the phone on re-association.
27404	APs now immediately recognize that a phone has transitioned back to active mode from power save mode.
27302	Long Captive Portal profile names no longer cause the switch to crash.
27211	You can now properly add a management user via the WebUI after upgrading from AOS-W 3.2 (or earlier).

Table 19 *AOS-W 3.3.2.7*

Bug ID	Description
27163	You can now correctly create an AP regulatory domain profile with a different country code than the switch, when the switch has a restricted country code.
27118	The wlsxVoiceCdrBufferThresholdReached has been changed from a periodic trap to a single trap so that the trap is no longer generated as frequently.
27106, 26558	The hyphen (-), period (.), underscore (_), and at (@) characters can now be used in a guest user name.
27105	The issue with multiple auth manager crashes has been fixed.
27087	Mesh links no longer occasionally fail due to the mesh portal aging out the station.
27066	Dynamic WEP keys are now correctly maintained when there is more than one VAP.
27015	The auth manager crashing when the client certificate has multiple subject alt name fields has been fixed.
26957	The issue with STM crashing on the master switch has been fixed.
26954	Atheros-based 802.11n NICs now connect consistently using HT rates.
26904, 27382, 27587	APs connected to a 4504, 4604, or 4704 switch or Supervisor Card III using TKIP encryption now correctly forward multicast and broadcast traffic after the P1key is rekeyed.
26896	The issue with a delay in creating a mesh link between two OAW-AP70s has been fixed.
26812	The association trail for mobile devices is now available. The `show ip mobile trail [<Host IP Address> | <Host Mac Address>]` command can be used to view the trail info. Please refer the *AOS-W 3.3.2 CLI Reference Guide* for more information.
26786	The issue with the Report tab not displaying the 802.11n HT information about clients has been fixed. A new column, HT Type, has been added in the Report tab. The data in this column can be sorted and provide information on clients based on the following HT Types: Active Interfering Clients Active Valid Clients Top Talker Clients
26772	After upgrading from AOS-W 2.5, users with certain chipsets (Intel 3945ABC) could not connect to a bridged SSID. This has been fixed.
26760	The issue with the WebUI (**Monitoring > Network > All Access Points**) displaying the wrong number (0-zero) of clients associated with an AP has been fixed.
26734	User firewall state is now reported correctly in the client status page under **Monitoring -> Switch -> Clients**.
26727	The issue with incorrect or no information on the Phy type of an AP in the WebUI has been fixed.
26703	The issue with the switch dropping IPSec packets in quick mode if there is a NAT device in between has been fixed.
26689	The issue with `httpd` not starting after an image is loaded to the switch has been fixed.
26677	Synching the configuration no longer results in APs failing over to the LMS (and thus disconnecting clients).
26665	The issue with Intel clients getting Key 2 MIC failures when attempting PMK caching with OKC enabled has been fixed. PMK caching and OKC can now co-exist.
26647	The issue with user entries of the disconnected VPN users still persisting in the user table has been fixed.

Table 19 *AOS-W 3.3.2.7*

Bug ID	Description
26647	The issue with user entries of the disconnected VPN users still persisting in the user table has been fixed.
26576	The issue with the WebUI not allowing you to disable re-authentication of roles that were previously set with a re-authentication interval has been fixed.
26565	Remote AP ACLs corresponding to newly created user-roles used by offline (backup/always mode) virtual APs are now correctly programmed.
26529	The inter-process communication not happening after an upgrade from AOS-W 3.3.1.4 has been fixed.
26489	The number of clients listed on the **Switch -> Summary** page now matches the number listed on the **Switch -> Clients** page.
26462	The `user_add` XML-API command can now be used in systems that have VLAN interfaces defined with a non /24 netmask.
26426	The watchdog timer issue on the OAW-AP85 has been fixed.
26425	Derivation rules have been fixed on port channels. Auth manager is notified of a new wired connection on a port channel.
26396	The issue with the Auth Manager crashing has been fixed.
26383	A RAP with dynamic WEP and a bridged VAP now encrypts broadcast traffic properly.
26348	The issue with active probe-req and Auth messages during a call has been fixed.
26268	The issue with the Captive Portal login page not displaying after upgrading to AOS-W 3.3.1.5 has been fixed.
26249, 26252	The time difference issue on the 4504, 4604, and 4704 platform has been fixed.
26202	The issue with high CPU utilization in the CLI mode has been fixed.
26171	The issue with the `tar logs` command causing the switch to freeze has been fixed.
26164	The issue with auth manager crashes while verifying the client certificate, when EAP-TLS offload is enabled, has been fixed.
26132	The issue with mesh points not working with JPX country code has been fixed.
26074	Stateful firewall for IPv6 is disabled by default. To enable the stateful firewall for IPv6 use the `ipv6 firewall enable` command.
26067	The issue with RAPs not working after downgrading from AOS-W 3.3 to AOS-W 2.5.x has been fixed.
26035, 26036, 26037, 26039, 26186	The issue with the crash of the STM module caused by SIP-TCP messages of large size has been fixed.
26021	The id-request period in a dot1x profile can now be set to a value higher than 30 seconds.
26009, 26888	Customized Captive Portal redirection now works properly.
25991	The issue with `mgmt-user radius` not authenticating based on calling station-id and nas-port-id has been fixed. When a RADIUS server is used to authenticate management users, the caller ID attribute in the RADIUS request will use the incoming IP address, with 0.0.0.0 as the serial console.
25987	The issue with DB sync between the master switches when the RF Plan is included has been fixed.

Table 19 *AOS-W 3.3.2.7*

Bug ID	Description
25977	When a user logs into the switch, the user auth assigns a new role and VLAN. The new role contains the VLAN configuration but the VLAN role is not assigned to a station. This has been fixed. The user role VLAN is now correctly assigned to a station.
25976	The user counts displayed on the **Monitoring -> Switch -> Switch Summary** and **Monitoring -> Switch -> Clients** pages now match the output of the `show user` command.
25911	The issue with LEAP 802.1x authentication not working with an IBM access client with the Atheros driver has been fixed.
25896	If the URL sent by MMS uses a different IP address than the one assigned in the switch, the following error message will be displayed: MMS server [a.b.c.d] in sync request is different than the active MMS server
25848	You can no longer enter the space or question mark (?) characters for the enable password (previously you could enter those characters even though they were not accepted).
25821	The issue with an OAW-AP70 not working after upgrading from AOS-W 2.5.6.2 to AOS-W 3.1.1.12 with the country code JP3 has been fixed.
25808	The issue with the database failing to synchronize has been fixed.
25800	The issue with the bandwidth-contract not limiting the rate of downlink multicast traffic sent from the switch to an AP has been fixed.
25773	The log message #399816, which occurs after upgrading from AOS-W 3.1 to AOS-W 3.3 is now a debug message. These messages can typically be ignored.
25771	The issue with the initial role not being assigned to user on MAC authentication failure has been fixed. The following behavior is implemented: When the MAC auth fails, L3 authentication using Captive Portal is performed. Dot1x will not be attempted. L3 authentication using Captive Portal can be performed if Captive Portal is configured. When the MAC auth fails in the base OS, the user is given the AAA profile initial role instead of the “denyall” role. An L3 authentication can still be performed. The `max-authentication-failure` option in the MAC auth profile is removed from the WIP license.
25743	The issue with the admin user role in the CLI changing to an snmp user role after a switch reboot has been fixed.
25677	The out of memory issue causing the switch to reboot has been fixed.
25586	The issue with traffic not moving across the master/local tunnel has been fixed.
25579	The `show user-table verbose` output now displays the correct current user VLAN.
25536	A TACACS authentication bug has been fixed.
25533, 25549	An issue with the CPU running at 100% utilization has been fixed.
25525, 25410	The issue with the switch removing SIP sessions that are offered but not answered and blocking subsequent RTP packet flow causing call disconnection has been fixed.
25438	The issue with auth manager processing the logon user-role ACLs in spite of the ACLs being removed has been fixed.
25350	STP BPDUs are no longer occasionally dropped when STP is enabled on an OAW-AP70.
25348	The issue with the broken AP Configuration page in the WebUI is fixed.
25345	The issue with clients not being able to authenticate in a LEAP setup using Cisco ACU version 4.x has been fixed.
25337	Disabling a trap using the `snmp-server trap disable` command no longer generates error messages warning that the trap is disabled.

Table 19 *AOS-W 3.3.2.7*

Bug ID	Description
25336	The issue with the switch crashing during an upgrade from AOS-W 3.3.1.0 to AOS-W 3.3.1.1 has been fixed.
25299	An OAW-AP70 RAP no longer crashes when over 20 MB of traffic passes upstream.
25266	The out of memory issue during an upgrade causing the switch to reboot has been fixed.
25263	The `aaa server-group` name 32 character limit is now properly enforced.
25244	The issue with the command `show datapath user` looping when an IPv6 and IPv4 user are on the same hash chain has been fixed.
25238	IPv6 packets with a source address of ::1 are now forwarded correctly.
25226	The firewall logging and ping issues during a switch reboot have been fixed. The ping command is not activated during the reboot.
25221, 26550	The master switch and MMS now display the correct AP status after a reboot.
25196	The `show user-table unique` command now outputs the correct number of unique users.
25164, 23722	Unicast DHCP replies are now correctly forwarded.
25162	S3 and 4504, 4604, or 4704 switches now fully support VRRP pre-emption.
25134, 25092	The Startup Wizard now behaves properly if there are any configuration errors when you click the Finish button.
25132	After upgrading Alcatel-Lucent switches to AOS-W 3.3.1, APs now properly utilize max-power settings, if allowed by Adaptive Radio Management (ARM).
25114	Adhoc containment for 802.11a/b/g APs is functional in the 5 GHz band.
25107	Changes to the default speed and duplex mode for a port in the Setup Wizard are now properly applied.
25094, 25577, 26641	The issue with not being able to save an RF Plan after updates has been fixed.
25057, 25438	Users no longer temporarily get assigned to the logon role instead of the initial role in the AAA profile.
25043	Without active AP licenses on the S3 and 4504, 4604, or 4704, you can now provision a remote AP.
25017	Adhoc network detection will trigger interfering ap detection against the adhoc network devices if `detect-adhoc` is disabled.
25015, 25058	The switch rebooting due to low memory has been fixed.
24995	If the user moves the port on which the Setup Wizard is connected from VLAN 1 to a new VLAN, the web browser window no longer hangs after the user clicks the Finish button.
24951	Wireless containment on the OAW-AP124 and OAW-AP125 802.11n access points is now supported.
24950	The issue with random reboot of APs has been fixed.
24942	The month, day, and year in the Setup Wizard Date & Time drop-down menus now reflect changes made with the calendar icon.
24864, 25306	The issue with the switch crashing after a huge log file is pasted into an SSH session has been fixed. You can terminate the SSH session to restore the switch without rebooting.

Table 19 *AOS-W 3.3.2.7*

Bug ID	Description
24846	Multicast data packets are no longer sent on a mesh-p VAP that has no associated children (a leaf-node).
24818	In IE, the issue with the user not being redirected to the actual URL after displaying the CP page has been fixed.
24778	You can now configure the role-based reauthentication interval from the mobility switch CLI.
24752	If you enable Cisco-style PoE on an unused port, the port LED no longer turns amber.
24749	The 40 MHz channel can now be enabled against the “KR” country code for the OAW-AP124 and OAW-AP125.
24729, 25982, 25983	The issue with incorrect AP entries in the WebUI has been fixed.
24727	The list of associated clients now matches the client count on the **Monitoring -> Switch -> Switch Summary** page.
24726	AP uptime is now reported correctly via SNMP.
24677	An error message is now displayed when you try to assign more VAPs than are supported by each radio on the AP.
24596, 24288	APs connected to switches with different time stamps failed to detect that the GRE tunnel was down during failover tests. This issue has been fixed.
24589, 24978	The Cisco 7921 IP phone no longer loses synchronization with the AP.
24522	The issue with irregular RADIUS stop messages being sent before the session has ended has been fixed. The following behavior is implemented: The switch sends the Rad-acct-terminate cause 28 only when L2 mobility is ON and when the station entry is aged out. The switch sends Rad-acct-terminate cause idle-timeout when L2 mobility is OFF, and when the user is inactive. The Rad-stop message is not sent if the user is still active on the switch (provided the user is detected via the user idle detection mechanism).
24520	Intel 2200 b and g clients now connect properly to bridged SSIDs.
24428	When all of the servers in a server group time out, the next authentication attempt no longer waits until the “dead timer” expires.
24346	The native VLAN ID and ap-group are now correctly programmed on “always” mode virtual APs before the remote AP connects to the switch.
24343	Group-based ACLs now work properly on the enet1 port of a RAP.
24330	Failed captive-portal authentication attempts always show the customized background.
24322, 25865, 26056	SVP phones using the g radio no longer constantly re-associate.
24306	Read only users can now export reports as expected.
24298, 25001, 26656	The switch rebooting due to a watchdog time-out has been fixed.
24286	The issue with users in the L3 table not being removed after the idle time-out period has been fixed.
24272	Outbound calls from a Nokia E65 using SIP no longer experience up to a 25 second delay before a call begins.

Table 19 *AOS-W 3.3.2.7*

Bug ID	Description
24234, 23496	During a mobility switch upgrade from 3.1.1.7, TFTP now operates as expected.
24219	The WebUI now displays the correct VLAN information under the Association State on the **Monitoring > Clients > Status** page.
24178	The switch's DHCP server may not send a DHCP NAK when the client roams from a different layer-3 subnetwork and tries to renew its old IP address on the new VLAN. When this happens, the client is unable to obtain the IP address on the new subnetwork. This issue has been fixed. The switch now sends a NAK if a client requests a wrong IP not serviced by the switch.
24148	Atheros 11n chipset installed clients do not associate at the 54 Mbps 802.11 rate after `stm kick-off station` command or after OAW-AP124/OAW-AP124 channel change.
24061	You can now properly view the status of RADIUS and LDAP servers.
24042	Changing the IPSec key on a master/local deployment with VRRP enabled no longer causes a loss of connectivity until the master switch is rebooted.
24017	When using an 802.11e-capable device with TSPEC, the AP now responds properly to an ADDTS request.
23977	The incorrect rogue AP report in the WebUI has been fixed. Two additional links, "Active Disabled APs" and "All Disabled APs," have been added for providing the correct information.
23957	The association table of the OAW-AP80M configured for static WEP no longer fills up with invalid entries over time.
23949	PPPoE now works properly on remote APs operating in split-tunnel mode.
23907, 25922	Xsec opmode SSIDs for the OAW-AP124 and OAW-AP125 are now supported.
23897, 24397	If the standby master switch is configured with the primary master IP, the standby master switch takes longer to boot. This is fixed.
23893, 26927	Bandwidth contracts now work properly on the S3 and 4504, 4604, and 4704 platforms.
23719	After changing the IP address of a master switch, local switches now correctly re-build their IPSEC tunnel to the master.
23690	APs will only show up under the WebUI "unprovisioned" page if the following is true: The AP is using external antennas and no gain values have been provisioned. The AP's group does not exist on the switch. The AP has the same name as another AP which is up. For this reason, most APs such as the OAW-AP61 or OAW-AP65 will never show up as "unprovisioned."
23631	LDAP authentication now differentiates between server unreachable and user unauthorized.
23501	The issue with the switch rebooting due to auth manager crash has been fixed.
23430, 24733	The issue with an AP crashing with WMM is enabled has been fixed. Now, new clients can associate to the AP.
23328	A memory leak due to an extremely large WMS database has been resolved.
23327	A blacklisted client no longer remains blacklisted for a maximum of 3600 seconds, even when the block time has been set to zero.
23306	Internal errors caused when an AP upgrades an image have been fixed.
23281, 24147	VLAN assignment is now always correct during MAC authentication. Workaround: Disable dos-prevention if this problem is observed.

Table 19 *AOS-W 3.3.2.7*

Bug ID	Description
23236	A RAP configured with a static IP address now responds properly to ARP requests.
23202, 27168	Remote APs now fail over to the backup LMS more quickly.
23175	RF Troubleshooting (RFT) functionality on the OAW-AP124 and OAW-AP125 is fully supported.
23141, 23976, 25811	The RAP watchdog timeout issue while attaching clients has been fixed.
22960, 22945, 25220, 25250	Local bridging on enet1 now works for OAW-AP70 access points that are not remote APs or Mesh nodes.
22916	A user authenticating through the Captive Portal via VPN is now assigned the proper role. When the user logs out from Captive Portal, the VPN tunnel is deleted as well.
22900, 25213	The issue with the `show user-table station` command failing has been fixed. The command now works with a large number of stations.
22832	The output of the `show station-table` command now displays the AP name based on the BSSID.
22668	APs now always get the correct FQLN from RF Live.
22654	The issue with incorrect output in the `show user-table` command has been fixed. The command now displays the AP name as `N/A` if no AP is found. When an AP entry exists, the actual AP-Name is displayed.
22636	All search options under **Monitoring -> Clients -> Search** now produce results.
22579, 22603	AP kernel logs are now visible in the output of the `show log ap-debug` command. Switch kernel logs are now visible in the output of the `show log system` command.
22475	Per-SSID bandwidth contracts on the OAW-AP124 and OAW-AP125 are now supported.
22227	L3 mobility across mobility switches that are configured with VRRP redundancy now work as expected.
22199, 24868	AAA FastConnect for EAP-TLS no longer fails if the authentication profile is configured before the CA certificate is loaded.

21437	The following CLI command and the WebUI page now display the current power level and maximum power level instead of the configured power level.
	CLI command updates:
	`show ap active`
	`show ap bssid-table`
	`show ap details`
	`show ap mesh active`
	`show ap arm state`
	WebUI updates:
	The WPA2 Pre-authentication row is removed
	The Power Level information under the profile in the **Switch > Access Points** page is updated.

21240, 24210, 24767, 25159	When upgrading S3 and 4504, 4604, or 4704 switches from AOS-W 3.2.0.x to 3.3.2, note the following, the clock no longer occasionally moves forward 3 hours.
21118	The logging level of message 501050 has been changed from informational to debugging. This message is not meaningful to end users.

Table 19 *AOS-W 3.3.2.7*

Bug ID	Description
20864, 24882, 24685, 26025	The state of APs terminated on the local mobility switch is now always reported the same on the master mobility switch.
20463, 24628, 24679	If a parameter in the Wired AP profile is modified, it now takes immediate effect. If you connect the mesh portal to a trunk port on the switch and the trunk native VLAN of that port has a value other than the default of 1, you are no longer required to set the native VLAN in the AP system profile to that value.
20456	L3 roaming of wireless clients with static IP addresses across switches is now supported. Host Address (HA) discovery for mobile users who perform silent roam is done on-association.
20274	The issue on the order in which the VRs and GRE tunnels are set up has been fixed. If the VR in backup mode, the GRE tunnel will be brought down. If, however, the VRRP is in admin shutdown mode, the GRE tunnel will remain in active state.
19977, 21057, 22702, 23309, 24758, 26403, 27520, 27523	Several causes of occasional switch crashes have been fixed.
19931	TACAS+ authentication now works properly with TACACS version 2.3.6 (and later) on Sun servers.
19602	The AP no longer need to be rebooted after WMM is disabled for Spectralink Voice Protocol to work with an acceptable retry rate.
18849, 19805, 21020, 22378, 23117, 23353, 23227, 23704, 23738, 23838, 23884, 24074, 24218, 24746, 24088, 24883, 25099, 25232, 25251, 25254, 25278, 25759, 25656, 25879, 26034, 26071, 26076, 26196, 26245, 26246, 26687	Several issues with the switch rebooting due to a datapath timeout have been fixed.

Known Issues and Limitations in AOS-W 3.3.2.24

The following are known issues and limitations for this release of AOS-W. Where bug IDs or workaround are applicable, they are included.

When upgrading S3 and 4504, 4604, or 4704 switches from AOS-W 3.2.0.x to 3.3.2.7, note the following:

Unless NTP is used, the system clock might move forward 3 hours. Provision the system clock manually after the upgrade. Temporary licenses must be reinstalled after the clock change.

Make sure that licenses installed on the system are enabled after the upgrade by navigating to the **Maintenance** tab on the WebUI or use the show license command on the CLI; if not, re-install the licenses and reboot the system WITHOUT saving your configuration.

AOS-W 3.3.2.7 does not support OAW-AP52 access points. If you have OAW-AP52s installed in your network, you should continue to run AOS-W 2.x.

Table 20 *Known Issues and Limitations*

Bug ID (if any)	Description
23929	Direct SNMP GET requests have been discontinued, despite the fact that an SNMP profile can still be configured under the AP system profile.
27834	Apple Macintosh laptops running OS X are unable to roam when OKC is enabled. To work around this, disable OKC (it is enabled by default).
27873	With some clients, client authentication can sometimes take from 30 seconds to 2 minutes.
27565	RF Plan imports do not always work with Firefox.
25351	PEF rules do not always pause ARM scanning.
26643	Some AP models do not display the master switch IP and the DHCP assigned IP in the AP boot message log.
24956	Wired 802.1x on OAW-4308 trunk port is not supported.
27069	When “enfore machine authentication” is enabled for 802.1x clients, the master switch(s) track the authentication state of every device on the master. However, if the master goes down, there is no place to check if a client passed machine authentication and thus impacts user connectivity. A workaround is enable the local switch’s internal database to store machine authentication states.
27613	The UI displays only one firewall ACL with a “time range” parameter.
25265	Valid user ACLs are not supported for IPv6 addresses.
25787	If the `best-effort-acm` parameter is set to 1, Cisco 7921g phones cannot associate. To work around this, set the `best-effort-acm` parameter to 0 (which is the default value).
27669	If a roaming client has difficulty maintaining connectivity, set the dot1x key retry count to 5 using the `aaa authentication dot1x wpa-key-retries 5` command.
27371	An error is generated in RF Plan when you create a new building in the main campus the first time after a WMS reinitdb. The new building is created and you can ignore the error. To work around this reload the browser.

Table 20 *Known Issues and Limitations*

Bug ID (if any)	Description
27309	After applying the upgrade license to allow AP-120 series a/b/g APs to support 802.11n, the affected APs must be rebooted for the change to take effect.
27498	Clients using a Linksys WPC600N 802.11n NIC are unable to pass traffic on 40 MHz channels over a back-up virtual AP. Clients are able to associate and get an IP address via DHCP, but cannot pass traffic. To work around this, use the 20 MHz channels for the back-up VAP.
27340	If a client connects via VPN using a different SSID (for example, if the client loses their wireless connection), the client is categorized as a new user. Thus, until the earlier entry ages out, the client is seen as two discrete users, each counting toward the total for your VPN license. To force an L2TP user entry to age out, use this command for the inner IP address: aaa user logout Use this command for the outer IP address: aaa user delete You cannot force a PPTP user entry to age out.
26898	RF Plan currently supports planning for the AP-124 only in the 20 MHz channel.
26699	You cannot use the native Windows XP L2TP IPSec dialer if you install the Alcatel-Lucent dialer. To work around this, uninstall the Alcatel-Lucent dialer and reboot Windows.
25109	ACL new hits and total hits may show incorrect values for “redirect src-nat” enabled session ACLs.
25031	When users select a different server group for the authentication server group, the mobility switch webUI will display a message; this message can be ignored.
25022	The **`show auth-tracebuf`** command may not work as expected after “user debugging” is enabled and then disabled.
24761	Enabling port mirroring on a 1 Gbps port to a 100 Mbps port is not supported on M3 and 3000 series Alcatel-Lucent switches. Port mirrors should be disabled whenever not in use in order to prevent performance impact on these type of mobility switches.
24748	Not able to add channels to the regulatory domain using the mobility switch webUI. Workaround: Use the mobility switch CLI to add channels to the “ap regulatory-domain” configuration.
24601	The mobility switch WebUI may show the number and state of APs and AMs incorrectly. Workaround: Use the **`show ap active`** command in the local mobility switch CLI to monitor AP states that are terminated on the mobility switch.
24108	The WebUI and the CLI prevents configuration of an AP-70 to use internal antennas for one radio and external antennas for the other radio.
24063	For APs that discover the master switch using DNS, switch discovery fails if the DHCP server returns more than one domain name.
23929	APs do not respond to SNMP queries even though SNMP has been enabled.
23880	Radius uptime may reset to 0:0:0 after a few minutes of high load of 802.1x authentication; no service outage will be observed.
23859	Forced classification of “suspect-unsecure AP” to “interfering AP” may fail. Workaround: Change state of the AP to classification type “unsecure” and then re-classify as “interfering”.
23792	Some packet loss might be observed on AP-70 eth1 port.
23736	Wired rogue AP containment does not work properly if multiple VLANs have been trunked to an AP. The AP will only perform wired-side rogue containment for an AP on its own VLAN.

Table 20 *Known Issues and Limitations*

Bug ID (if any)	Description
23735	Single-radio APs may take an excessive amount of time to detect rogue APs on their non-preferred band, due to the amount of time it takes the internal radio to change between 2.4 GHz and 5 GHz bands. Workaround: Use dedicated air monitors or deploy dual-radio access points.
23713	Checkbox selections may get lost after WebUI auto refresh.
23669	SNMP total AP count will not include APs that do not have VAPs enabled. Workaround: Use the `show ap active` command on the mobility switch to monitor the total AP count.
23437	In some cases voice call admission control load balancing may not function correctly. Workaround: Retry call request or association on the voice client.
23297	Spaces in filenames are not allowed for floorplan images uploaded to RF Plan.
23275	MAC authentication may not immediately take place if a user account is recently added to the internal local database. Workaround: Retry after 5 minutes if the MAC authenticated user was missing from the database during the first try.
23234	The WebUI does not properly permit resetting of custom captive portal pages to factory defaults.
23220	The following SNMP MIBs incorrectly report zero at all times: wlanAPFrameReceiveErrorRate, wlanAPFrameFragmentationRate, wlanStaFrameReceiveErrorRate, wlanStaFrameFragmentationRate.
22925	The AP-124 and AP-125 might fail to boot up across a 100 MB half duplex link.
22678	The “%” character may not be used in a password in the local user database.
22672	An SSID configured for xSec and WMM will not function properly. This combination should not be used in this release.
22524	When configuring passwords and keys in the WebUI, non-alphanumeric characters (for example,%, ^, &) are silently discarded, resulting in incorrect passwords being stored. Workaround: Use the CLI to configure passwords and keys that contain non-alphanumeric characters.
22346	If the switch reboots while a call is in progress, the “show voice call-cdrs” command may show incorrect data for the call after the switch is back up. For example, the direction and called party information may be incorrect.
22283	Extensive amount of syslog messages may be observed after changing the role of the mobility switch from master to local. Workaround: Before changing the role of the mobility switch from master to local, use the `clean wms-db` command on the mobility switch.
22203	The switch cannot authenticate users with special UTF-8 characters in their username.
22190	L2 ACLs (MAC and Ethertype) only work if the user table has any entry for the station. L2 ACLs do not work in an untrusted station has not sent an IP frame, but an L2 frame.
21820	Disconnected calls are not reported as such in the output of the `show ap association voip-only` and `show voice sip client-status` commands. The calls are properly disconnected and this is a benign problem with the output.
21673	The WIP module may be logging “Signature Match Detected. SignatureName=Null-ProbeResponse” for some mesh nodes during the time the mesh nodes are starting up. This message is harmless.
21633	It is not possible to provision the antenna type for outdoor APs using AOS-W. This provisioning must be done from MMS.

Table 20 *Known Issues and Limitations*

Bug ID (if any)	Description
21338	The WIP module may be logging “Disconnect Station Attacks” for mesh nodes incorrectly. If this occurs, disable detection of “Disconnect Station Attacks”.
20603	Users using WZC or MACbook 802.1x supplicant fail authentication with Steel-Belted Radius servers or the internal database if both AAA FastConnect (EAP termination) and trim FQDN are enabled.
20242	When an AAA profile is configured with a reauthentication interval and AAA FastConnect is enabled, reauthentication may fail. Workaround: Disable reauthentication.
20214, 22187	Changing a bandwidth contract while a large number of users are active on the system and subject to that bandwidth contract may result in the message “Module Authentication is busy. Please try later”. Workaround: Change the bandwidth contract when there are a low number of active users on the system.
20143, 23778	Wired authentication support on ENET1 of an AP-70 remote access point is not supported if “split-tunneling” is enabled.
20134	An “sapd” error message may be seen on switchs terminating remote APs that states “An internal system error has occurred at file messenger.c function msgr_papi_send_status_callback line 1590 error”. This error message is harmless.
17857	When `logging level debug system` is set during system bootup or during a VRRP failover, APs may take a long time to come up. Workaround: Only set `logging level debug system` during an active debugging session. Turning off debugging restores normal operation.
17784	The default behavior of Windows XP may cause AP load balancing not to function correctly by allowing any Windows XP station to associate to an AP after three minutes.
17701	The `show memory fpapps` command does not work on the S3 and the OAW-4504, 4604, and 4704.
17688	To deny access to a specific switch when traffic travels across another switch in the same master-local topology, ACLs must be added to the user’s session ACL. Port ACLs are bypassed.
17394	When you first display the Reports page in the WebUI in an Internet Explorer version 7 browser window, a warning message about allowing scripting appears.
16046, 16565	A wired client connected to an OAW-4304 or OAW-4324 fails 802.1x authentication. The message “Dropping EAPOL packet” appears in the logfile of the OAW-4304/4324. Workaround: Configure the MUX client as master and disable 802.1x.
14119	The mobility switch does not perform NAT for traffic originated by the mobility switch itself, such as RADIUS requests, syslog, and SNMP. Workaround: Put a loopback or VLAN interface on a public subnet. If that is not possible, configure the WAN VLAN interface IP address to be the same as the switch IP address.
12732	Load balancing does not work properly when local probe responses are enabled.
8684	When a mobile client is on a foreign network in a mobility domain, multicast traffic is not tunneled back to the home network.
	The Ethernet port on the AP-124 and AP-125 may not function as expected in 10 Mbps mode.
	This release does not support the secure enterprise mesh functionality on the AP-124 and AP-125.
	This release does not support FCC DFS on the AP-124 and AP-125.
	ETSI DFS is supported but not yet fully certified on the AP-124 and AP-125 at this time.

Table 20 *Known Issues and Limitations*

Bug ID (if any)	Description
	If local management authentication is enabled and you are unable to log into the switch, use password recovery to log into the switch to disable local management authentication. For information about password recovery, see “Resetting the Admin or Enable Password” in the *AOS-W 3.3.1 User Guide*.
	The AP-80M uses only approved outdoor channels; however, the administrator can configure any channel using the CLI and the WebUI. If this occurs, the AP-80M randomly selects a valid outdoor channel.
	In multi-switch networks, save your mesh cluster configuration before provisioning the mesh nodes. To save your configuration in the WebUI, at the top of any page click **Save Configuration**. To save your configuration in the CLI: `write memory`

Documents in This Release

New revisions of the following documents are available with this release:

- *AOS-W 3.3.2 User Guide*
- *AOS-W 3.3.2 Command Line Interface Reference Guide*
- *AOS-W 3.3.2 Quick Start Guide*
- *AOS-W 3.3.2 MIB Reference Guide*
- *AOS-W 3.3.2 Software Upgrade Guide*

The documentation library is updated continuously. You can download the latest version of any of these documents from:

https://service.esd.alcatel-lucent.com

For More Information

To contact Alcatel-Lucent, refer to the information below:

Web Site Support	
Main Site	http://www.alcatel-lucent.com/enterprise
Support Site	https://service.esd.alcatel-lucent.com
Support Email	support@ind.alcatel.com
Telephone Numbers	
North America	1-800-995-2696
Latin America	1-877-919-9526
Europe	+33 (0) 38 855 6929
Asia Pacific	+65 6240 8484

www.alcatel-lucent.com

26801 West Agoura Road
Calabasas, CA 91301