AOS-W 3.3.1.31

Release Notes

This document describes the new features and issues pertinent to the AOS-W 3.3.1.31 release.

NOTE

See the *AOS-W 3.3.1 Software Upgrade Guide* for instructions on how to upgrade your WLAN Switch to this release.

What's New in This Release

AOS-W 3.3.1.31 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 3.3.1" on page 9.

In Previous AOS-W 3.3.1 Releases

Previous releases of AOS-W 3.3.1 have introduced new software features for all OmniAccess Switches. This section describes new features and capabilities of AOS-W 3.3.1.

Hardware

AOS-W 3.3.1.31 supports the following new Alcatel-Lucent hardware products:

The Alcatel-Lucent OAW-AP120 series wireless access points support the draft standard of IEEE 802.11n / MIMO (Multiple-in, Multiple-out). These MIMO-capable, 802.11a/b/g/n wireless access points are available in versions with one or two radios and with integrated antennas or RP-SMA interfaces that support detachable antennas. The OAW-AP120 series access points work only in conjunction with an Alcatel-Lucent WLAN Switch.

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

Platform

AOS-W 3.3.1.31 introduces the following platform features:

Setup Wizard

The AOS-W 3.3.1 release introduces a browser-based Setup Wizard that steps you through the tasks of configuring the switch and installing software licenses.

To access the Setup Wizard, your switch must be running AOS-W 3.3.1 in factory-default mode. If you want to use the Setup Wizard, do the following after upgrading your switch to AOS-W 3.3.1:

From the WebUI:

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

From the CLI, execute the following commands:

```
write erase
reload
```

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

IPv6 Phase I

This release of AOS-W provides wired or wireless clients using IPv6 addressing with services such as firewall functionality, layer-2 authentication, and (with installation of the Policy Enforcement Firewall license) identity-based security. The Alcatel-Lucent switch does not provide routing or Network Address Translation to IPv6 clients in this release.

Clients can be wired or wireless and use IPv4 and/or IPv6 addressing. This release of AOS-W requires that the default gateway for the IPv6 clients be an external router that supports IPv6. The Alcatel-Lucent switch itself has an IPv4 address, and cannot route packets with IPv6 addresses. You can use the WebUI or CLI to display IPv6 client information.

IPv6 clients must be mapped to a VLAN that is bridged to an external router which provides IPv6 services to the clients. On the switch, you can configure IPv4 and IPv6 clients on the same VLAN.

For more information about IPv6 features supported in this release, see “IPv6 Client Support” in the *AOS-W 3.3.1 User Guide.*

Packet Mirroring for Layer-2 Traffic

This release allows you to mirror traffic based on MAC flow or Ethertype. You configure the mirroring option in either the MAC or Ethertype ACL and define the destination to which mirrored packets are sent in the firewall policy. If you configure both an IP address and a port to receive mirrored packets, the IP address takes precedence. Packets can be mirrored in multiple ACLs, so only a single copy is mirrored if there is a match within more than one ACL.

This enhancement provides additional troubleshooting and debugging capabilities to monitor and debug your network.

NOTE

This feature only mirrors non-IP traffic. To mirror IP traffic, configure the mirroring option in the session ACL. You also define the destination to which mirrored packets are sent in the firewall policy. To configure session ACLs, you must install the Policy Enforcement Firewall license.

To configure mirroring for Layer-2 traffic using the WebUI, navigate to the **Configuration > Security > Access Control > Policies** page. Edit an existing Ethertype or MAC ACL or create a new one, and select the mirroring option. To add the destination IP address or port, navigate to the **Configuration > Advanced Services > Stateful Firewall > Global Setting** page. At the Session Mirror Destination field, enter the valid IP address or the destination port.

To configure mirroring for Layer-2 traffic using the CLI:

```
ip access-list eth permit (<ethtype> [<bits>]|any} mirror
ip access-list mac permit {<macaddr> [wildcard>]|any|host <macaddr>} mirror
firewall session-mirror-destination {ip-address <ipaddr>|port <slot>/<port>}
```

Location API Management Role

This release introduces the location-api-mgmt role. This role permits access to location API information only.   This role does not allow the user to log in to the CLI nor does it allow the user to perform any action such as copying files or rebooting the switch.

> NOTE
>
> For backward compatibility with previous AOS-W releases, existing user roles that have access to location API information will continue to do so.

To create a location API management role using the WebUI, navigate to the **Configuration > Management > Administration** page and click Add. Under Conventional User Accounts, enter a user name, password, and select location-api-mgmt from the Role drop-down menu. When you are finished, click **Apply**.

To create a location API management role using the CLI:

```
mgmt-user <username> location-api-mgmt <password> <password>
```

You are prompted to enter and confirm the password.

Using a third-party location appliance, you can gather information about the location of 802.11 stations. To log in to the switch using a third-party location appliance, enter **http[s]://<ipaddress>[:port]/screens/wms/wms.login**. You are prompted to enter your username and password (for example, the username and password associated with the location API management role). Once authenticated, you can use an API call to request location information from the switch, for example: **http[s]://<ipaddress>[:port]/screens/wms/wms.cgi?opcode=wlm-get-spot&campus-name=<campus id>&building-name<building id>&mac=<client1>,<client2>....**

VRRP Interface Tracking

This release supports VRRP interface tracking. If configured, you can track multiple VRRP instances to prevent asymmetric routing and dynamically change the VRRP master to adapt to changes in the network. VRRP interface tracking can alter the priority of the VRRP instance based on the state of a particular VLAN or Layer-2 interface. The priority of the VRRP instance can increase or decrease based on the operational state of the specified interface. For example, interface transitions (up/down events) can trigger a recomputation of the VRRP priority, which can change the VRRP master depending on the resulting priority. You can track a combined maximum of 16 interfaces.

> NOTE
>
> You must enable preempt mode to allow a switch to take over the role of master if it detects a lower priority switch currently acting as master.

To configure VRRP interface tracking using the WebUI, navigate to the **Configuration > Advanced Services > Redundancy** page and add a new VRRP instance or select an existing VRRP instance. At the Virtual Router page, configure the VLAN or port to track.

- To configure the VLAN, under Tracking VLAN, click New and enter the VLAN ID, enter a value to either add or subtract from the VRRP priority, and click Add.
- To configure the port, under Tracking Interface, click New and select a port from the drop-down list, enter a value to either add or subtract from the VRRP priority, and click Add.

To configure VRRP interface tracking using the CLI:

```
vrrp <id> tracking interface {fastethernet <slot>/<port>|gigabitethernet
<slot>/<port>} {add <value>|sub <value>}
vrrp <id> tracking vlan <vlanid> {add <value>|sub <value>}
```

Disable Local Management Accounts

This release introduces the option to disable local authentication of management accounts; however, you can log in with a local management account if the authentication servers are not available.

In previous versions of AOS-W, if the configured RADIUS or TACACS+ servers returned an invalid role, failed to authenticate the user, or the authentication request timed out, management users were authenticated by the local database.

In AOS-W 3.3.1, you can disable local database authentication for management users based on the results returned by the authentication servers. When enabled, locally-defined management accounts (for example, admin) are not allowed to log in if the user entry is not found in the authentication server. In this situation, if the RADIUS or TACACS+ servers return an error or fail to authenticate a user, local authentication is not used. If the authentication attempt times out, local authentication is used and you can log in with a locally-defined management account.

To disable local management authentication using the WebUI, navigate to the **Configuration > Management > Administration** page. Under Management Authentication Servers, check (select) the Local Authentication Mode checkbox.

To disable local management authentication using the CLI:

```
mgmt-user localauth-disable
```

To verify if local management authentication is enabled or disabled, use the following command:

```
show mgmt-user local-authentication-mode
```

RF Plan AP Status and Down AP Icon

This release introduces an AP status column and a down AP icon in the AOS-W RF Plan WebUI.

The status column displays the current status of each AP for the floor you are viewing within a live network.

- **Up:** AP is up (live). The corresponding AP icon on the floor map will display a live AP icon.

- **Down:** AP is down. The corresponding AP icon on the floor map will display with a red "X" over the AP icon symbolizing that the AP is down.

WebUI RF Plan Support

This release introduces planning of 802.11n high-throughput (HT) deployments, as described in D02.05 of the proposed IEEE 802.11n/MIMO (Multiple-in, Multiple-out) standard.

NOTE

In order for the WebUI RF Plan tool to import and read a standalone plan that incorporates 802.11n draft standard APs and was originally created in the Java-based standalone RF Plan tool, the plan must be exported out from the standalone tool using the Switch WebUI Format (version 3.0).

OAW-AP120 Series Support

Support of the 802.11n draft standard comes in unison with the release of Alcatel-Lucent's OAW-AP120 Series of Indoor Access Points, which are 802.11n draft standard compliant APs. These APs can now be planned for in this release of RF Plan.

WebUI RF Plan Changes/Modifications

The following areas of the WebUI RF Plan application have been modified to support 802.11n (HT) planning (refer to the *AOS-W 3.3.1 User Guide* for complete details):

- Building Specifications Overview Page
- AP Modeling Parameters Page
- AM Modeling Parameters Page
- Floors Planning Page (including Deployed Floors Page)
- AP Planning Page
- AM Planning Page
- Area Editor Dialog Box (includes new 802.11n Zone)
- Suggested Access Point Editor Dialog Box
- Suggested/Deployed Access Points and Air Monitors Table
- Coverage Map Selections (HT Mode, Rates, Channels)

Supported Planning

This version of the WebUI RF Plan tool will aide you in the planning of legacy and/or 802.11n draft standard compliant deployments. The term legacy refers to Alcatel-Lucent APs that are not 802.11n draft compliant and support 802.11a and/or 802.11b/g networks only.

This version of WebUI RF Plan supports planning of the following deployment types:

- Legacy Deployments:

  RF Plan allows you to plan for legacy environments. Legacy refers to Alcatel-Lucent APs that are not 802.11n draft compliant and support 802.11a and/or 802.11b/g networks only. Planning for these environments works in the same way as previous versions of RF Plan.
- 802.11n Deployments:

  This version of RF Plan now supports planning of network environments that wish to utilize Alcatel-Lucent's OAW-AP120 series of indoor access points, which are 802.11n draft compliant. RF Plan supports the planning of these APs in the following capacity: 802.11a/n, 802.11b/g/n, or 802.11a/b/g/n.

NOTE

802.11n only deployments are not supported at this time.

- 802.11n Hotspot Deployment within an Existing Legacy Environment:

  This version of RF plan allows you to plan for an 802.11n hotspot deployment within an existing legacy environment. This type of environment requires that legacy AP/AM locations be fixed at the building level. If you set and fix the location of legacy APs prior to planning for the 802.11n APs, the legacy APs will not move when you initialize/optimize the 802.11n AP locations.
- 802.11n Hotspot Deployment and New Legacy Environment:

  This version of RF Plan allows you to plan for a new deployment that will utilize an 802.11n hotspot and 802.11a and/or 802.11 b/g support outside of the hotspot.

  To plan for this type of deployment, start by planning your 802.11n hotspot. When you initialize and optimize the APs planned for the hotspot, the 802.11n APs will be placed within the hotspot area. However, the same AP type will also be placed outside of the hotspot area with 802.11n support disabled. RF Plan will deploy APs outside of the hotspot area based on the 802.11a and/or 802.11b/g rates defined by the system. For the system to define 802.11a and/or 802.11b/g rates, the system looks at the defined 802.11n rate and the distance covered by the defined rate; it then selects corresponding 802.11a and/or 802.11b/g rates based on the distance covered. Since the APs outside of the 802.11n hotspot area utilize 802.11a/b/g rates only, you can deploy legacy APs in their place if desired.

Security

Master-Local IPsec Key Configuration

This change was implemented in AOS-W 3.3.1.30.

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.

Certificate-Based Site-to-Site VPN Interoperability

This release supports certificate-based site-to-site VPN interoperability with a Cisco IOS router. The configuration is similar to configuring VPN settings between Alcatel-Lucent switches, with the following requirements:

- On the Alcatel-Lucent switch, configure a fixed lifetime under the IKE policy:

  ```
  crypto isakmp policy 1
    auth rsa-sig
    lifetime 86400
  ```

  The site-to-site VPN capabilities of AOS-W have been enhanced for this feature. You can define multiple IPSec maps for the same peer VPN device. These maps must have unique Destination-networks that do not overlap. These maps can have overlapping Source-networks.
- On the Cisco IOS router, configure the ISAKMP identity to be Distinguished Names (DN):

  ```
  crypto isakmp identity dn
  ```

  This is required for the Cisco router to send the Subject-name of the certificate as the IKE-ID.?(This is standard behavior for most vendors' routers and is expected by the switch.) This allows AOS-W to validate the digital signature during IKE Main mode negotiation.

Wireless

AOS-W 3.3.1 introduces the following wireless features and capabilities:

AP Maintenance Mode

You can configure APs to suppress traps and syslog messages related to those APs. Known as AP maintenance mode, this new setting in the AP system profile is particularly useful when deploying, maintaining, or upgrading the network. AP maintenance mode is disabled by default. If enabled, APs stop flooding unnecessary traps and syslog messages to network management systems or network operations centers during a deployment or scheduled maintenance.

To configure AP maintenance mode using the WebUI, navigate to the **AP Configuration** page, select either the AP group or specific AP, and then select the AP system profile. Under Profile Details check (select) the Maintenance Mode checkbox to enable AP maintenance mode, or clear (deselect) the Maintenance Mode checkbox to disable AP maintenance mode.

To configure AP maintenance mode using the CLI:

To enable AP maintenance mode:

```
ap system-profile <profile>
      maintenance-mode
```

To disable AP maintenance mode:

```
ap system-profile <profile>
      no maintenance-mode
```

Viewing AP maintenance mode information

To view the maintenance mode status of APs, use the following commands:

```
show ap config
show ap debug system-status
```

On the local switch, you can also view maintenance mode status using the following commands:

```
show ap details
show ap active status
show ap database
```

For more information see “AP Maintenance Mode” in the *AOS-W 3.3.1 User Guide*.

Configurable WMM AC to DSCP Mapping

The IEEE 802.11e standard defines the mapping between Wi-Fi Multimedia access categories (WMM ACs) and the Differentiated Services Codepoint (DSCP) tags. In previous AOS-W releases, WMM AC to DSCP mapping used the fixed mapping defined by the IEEE 802.11e standard. Beginning with AOS-W 3.3.1.31, you can use the WMM AC mapping commands to customize the mapping between WMM ACs and DSCP tags. You apply and configure WMM AC mappings to a WMM-enabled SSID profile.

NOTE

The user-configured mapping only takes effect when WMM is enabled for the SSID profile.

To configure WMM mapping using the WebUI, navigate to the applicable SSID profile in the **Virtual AP** profile. Under **Profile Details**, select the Advanced tab. Scroll down to the Wireless Multimedia (WMM) option to enable WMM. After enabling WMM, modify the DSCP mapping by entering the desired value in the DSCP mapping for voice, video, best-effort, and background fields. Click **Apply**.

To configure WMM mapping using the CLI:

```
wlan ssid-profile <profile>
   wmm
   wmm-be-dscp <best-effort>
   wmm-bk-dscp <background>
   wmm-vi-dscp <video>
   wmm-vo-dscp <voice>
```

For more information, see “Optional Configurations” in the “Configuring QoS for Voice” chapter in the AOS-W 3.3.1.31 User Guide.

IEEE 802.11n Draft Standard Support

This release introduces core 802.11n high-throughput (HT) functionality, as described in D02.05 of the proposed IEEE 802.11n/MIMO (Multiple-in, Multiple-out) standard.

MIMO technology, an imminent IEEE standard of 802.11n, is an unlicensed band Wi-Fi ODFM modulation technology, operating in the 2.4-2.5 GHz and 5 GHz bands, that leverages multiple 802.11 radios on a single radio chip (up to three), simultaneously transmitting and receiving to improve RF signal integrity. This enhanced signal integrity dramatically reduces the effects of multi-path and increases both the usable coverage area as well as overall wireless throughput.

NOTE

Support of the 802.11n draft standard comes in unison with the release of Alcatel-Lucent’s OAW-AP120 Series of Indoor Access Points, which are 802.11n draft standard compliant APs.

The following items from the 802.11n draft standard are supported in this release of AOS-W:

- Spatial Multiplexing with two streams
- A-MPDU aggregation/de-aggregation

- Block Acknowledgements
- 40 MHz Channel Operation in both 2.4 GHz and 5 GHz bands
- Short Guard Interval in 40 MHz Operation
- MIMO Power-Save

New Profiles/Commands

Configuration of HT functionality is split into two new profiles, the high-throughput radio profile, and the high-throughput SSID profile. The radio profile contains parameters that apply to all SSIDs on a given radio. The SSID profile contains parameters applicable to a specified SSID.

- rf ht-radio-profile
- wlan ht-ssid-profile

Modified Profiles/Commands

The following profiles/commands have been modified to support 802.11 (HT) configuration and operation:

- ap enet-link-profile
- ap regulatory-domain-profile
- ids dos-profile
- ids unauthorized-device-profile
- rf arm-profile
- rf dot11a-radio-profile
- rf dot11g-radio-profile
- wlan ssid-profiles
- wlan virtual-ap

Troubleshooting and Display Commands

The following commands have been extended or added to show information about 802.11 (HT) configuration and operation:

- show ap configuration
- show ap debug received-config
- show ap association
- show ap bss-table
- show ap debug system-status
- show ap debug radio-stats
- show ap debug client-stats
- show ap debug client-table
- show station-table
- show user-table
- show ap ht-rates bssid

Issues and Limitations Fixed in AOS-W 3.3.1

The following issues and limitations have been fixed in the 3.3.1 release:

Table 1 *AOS-W 3.3.1.31*

Bug ID	Description
32803, 35350, 35134	An auth hang issue due to frequent RAND number generation has been fixed.

Table 2 *AOS-W 3.3.1.30*

Bug ID	Description
33992, 34564, 34577	A datapath session timeout issue on the OAW-6000 switch 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.
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 3 *AOS-W 3.3.1.29*

Bug ID	Description
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.

Table 4 *AOS-W 3.3.1.28*

Bug ID	Description
22199, 24868, 33952, 33069	With this fix, when certificate configurations are pushed from the master to a local, which does not have the corresponding certificates, the local will mark associated profiles as invalid.These invalid profiles will become valid once the correct certifcates are loaded on the local switches. Invalid status can be seen by using the `show profile-errors` command.
30116	The `trim-fqdn` option now works when the credentials are in the format of "domainusername" against LDAP and TACAS servers
31423	An issue in which the an S3 in slot 0, in a fully populated chassis (four S3s) crashes causing an S3 in slot 2 to reboot has been fixed.
33712, 32906	An issue where the Captive Portal logon wait screen appears, despite CPU usage being low, has been fixed.

Table 5 *AOS-W 3.3.1.27*

Bug ID	Description
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.

Table 6 *AOS-W 3.3.1.26*

Bug ID	Description
28498, 30042	An issue in which logged ACL hits contained incorrect information has been fixed.
29588	A slow memory leak, which only affects configurations configured for VPN, has been resolved
32121, 32203	A switch reboot issue due to low memory in configurations using Captive Portal and a high number of users has been resolved.
32353, 30222, 31788, 31987, 32491, 32679, 32159, 31898, 32845	A crash in the auth module, followed by slow connectivity, has been resolved.
32607	Users will now see the correct Captive Portal logon page, based on the cp-profile, instead of the default.
32750	Wired users are now correctly directed to the Captive Portal logon page when connected through an untrusted trunk port.
33388	HT-40 MHz channels now work correctly for country code IL (Israel).

Table 7 *AOS-W 3.3.1.25*

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.
29106	A new AAA profile called default-xml-api has been created. This profile is selected if the XML API is used to communicate with the switch regarding users that have not yet associated.
30925	The logging message for adding a user through XML provides the correct IP addresses.
30927	If Radius accounting is enabled, the Radius accounting stop message is sent to the correct server group after switching to a new VAP.
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.

Table 7 *AOS-W 3.3.1.25*

Bug ID	Description
31702, 30060, 30165	Session updates no longer fail when a unidirectional deny session exists.
31908	User_add and user_query work correctly for existing users, even when a MAC address is not specified.
32483, 32739, 32759	A number of enchancements have been made to track down, monitor, and prevent memory leaks' reducing the number of reboots caused by low memory.

Table 8 *AOS-W 3.3.1.24*

Bug ID	Description
25350, 32123, 31929	Enabling spanning-tree protocol (STP) on the OAW-AP70 no longer causes RX errors or drop increases on eth0.
26665, 27749, 27677	The issue where client devices are receiving Key 2 MIC failures when attempting PMK caching, with OKC enabled, has been fixed.
26954, 25473	HT IEs sent in probe responses are now based on information about the VAP, not taking into account client info from the probe request.
27796	Issues with ssh mgmt authentication using public keys has been fixed.
28348	5 GHz channels are enabled for Russia and Thailand.
31202, 32215	TotalAPCount and TotalSTACount, which are displayed in "show wms counters," always show positive values.

Table 9 *AOS-W 3.3.1.23*

Bug ID	Description
23706	AOS-W now provides SNMP support for fan and power supply status.
26528	STM requests for basic system information, which declares an AP as "up," continue until they are successful.
27102, 31696	When performing an SNMP Get, the switch will return the correct OID.
27401	Fan failures are now reported correctly.
29528	All members of a port channel will successfully come back up after a reboot.
29589	A switch will no longer reboot due to a control processor exception.
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.
30247	The WebUI now displays the correct number of APs, matching the number shown in the CLI.
30853, 30920	The issue where crashes in Auth and STM were followed by slow dot1x authentication has been fixed.

Table 9 *AOS-W 3.3.1.23*

Bug ID	Description
30875	The “show ap association” command now displays the correct, up-to-date AP status.
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.
31481	AP’s will not reboot if the switch probe contains an unsupported rates element.
31545	The issue where use of the command “show ip statistics app-name <any valid argument>” causes a memory leak has been fixed.

Table 10 *AOS-W 3.3.1.22*

Bug ID	Description
23501, 29302	An auth crash issue caused by the NULL pointer being returned by a function call has been fixed.
25611, 29956	DST NAT correctly works for wired clients.
29308	The following show commands have been added to AOS-W: ● show ap mesh active ● show ap mesh topology long
29368	The issue where the RF Planner incorrectly shows “some APs assigned to the wrong channel” 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.
30324	An S3 crash issue accompanied by a datapath timeout error has been addressed.
30595	Switches now correctly decode AARP packets.
30668	A memory leak in the STM module has been addressed.
30705	Correctly creating a new Reg Domain through the Web UI no longer results in errors.
30768	A RAP datapath timeout issue has been fixed.
30720, 30053	A database sync failure 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.

Table 11 *AOS-W 3.3.1.21*

Bug ID	Description
25221, 26550	The issue with the Master switch showing APs down when they are actually up has been fixed.

Table 11 *AOS-W 3.3.1.21*

Bug ID	Description
29536	The low memory issue caused after upgrading to 3.3.1.15 has been fixed.
30637, 21671, 21672, 29851	The issue in which the CP and DP user tables are out of sync has been addressed.
30739, 30793	Clients connecting through a TKIP or mixed mode WPA/WPA2 SSID now successfully acquire an IP address from the DHCP.

Table 12 *AOS-W 3.3.1.20*

Bug ID	Description
10148	Fast ethernet port detection problems on client devices equipped with a GigE NIC have been fixed.
22669	The issue with the MUX tunnel dropping between the master and the remote (local) switches has 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.
24979, 29931	Installation of an Outdoor Mesh license no longer triggers the message “licensemgr” to appear in the error logs.
25069, 24818	When a new Captive Portal certificate is uploaded, the changes now take effect immediately.
25548, 27554	Packet capture now works correctly with 802.11 and QOS.
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
27876, 25548	PPI headers are now supported.
28615	The “show acl hit” CLI command now correctly displays the statistics.
29135	The issue with Air Monitor not getting packets and causing ARM to not scan properly 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.
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.
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.

Table 12 *AOS-W 3.3.1.20*

Bug ID	Description
30181, 30400	Logs.tar files can now be extracted without issue.
30199	The show AP association command now returns data instead of being blank.
30431	Stateful 802.1x now works on Linux-based Radius servers.

Table 13 *AOS-W 3.3.1.19*

Bug ID	Description
21571	The issue where a certificate, which lacks a newline at the file, cannot be uploaded has been fixed.
24117	The issue with chronic g-radio interference saturating the CPU and reducing a-radio throughput has been fixed.
25412, 29449	A Remote AP issue where the AP's static IP was being overwritten by the Inner IPSec address during reprovisioning has been fixed.
25917	Multicast and broadcast from a SRC-NAT subnet is now allowed.
26202, 28364	The display issue in the CLI showing CPU utilization of 100%, while in shell mode the CPU is normal, has been fixed.
26812	Association trail information is now displayed correctly in both the WebUI and CLI.
27329, 27417	The issue in which the AP is using its highest rate to transmit EAP frames while the client is using the lowest rate has been fixed.
28001	Maximum EIRP for European countries can now be reached.
29255	VPN L2TP tunnels are now deleted whenever the connection is terminated.
29310	When upgrading from AOS-W 3.1 to 3.3, AP radio profiles are now copied over.
29314, 29367	The issue involving multiple AP reboots and AP reconfigurations causing crypto stalls has been fixed.
29317	A switch crash issue caused by a datapath exception has been fixed.
29469	The issue resulting in excessive association processing delay under high system load has been fixed.
29563	The issue with guest clients not receiving an IP address when connecting to an open SSID has been fixed.
29816	The CPU spike issue on the switches has been fixed.
29878	The default time between EAP identity requests has been reverted to 30 seconds from Patch 3.3.1.18.
29898, 29914, 29957, 29885	Multiple switch crash issues due to datapath timeout error has been fixed.

Table 14 *AOS-W 3.3.1.18*

Bug ID	Description
22003	Incorrect CPU load values has been fixed.

Table 14 *AOS-W 3.3.1.18*

Bug ID	Description
25228	The issue with 1% packet lost during the TKIP P1 key not being ready has been fixed.
25352	SNMP switch logging: A log message has been re-classified as debug (earlier informational) to prevent the logs rotating quickly.
26885	In 802.1X the default time between the re-transmitted EAP requests has been reduced to 3 seconds (from 30 seconds in previous releases). To change this time: aaa authentication dot1x <profile> timer idrequest_period 3
26886	After the maximum number of EAP requests are retransmitted, the switch now sends an EAP failure message to the client instead of failing silently. To change the maximum number of EAP requests: aaa authentication dot1x <profile> max-requests 3
27465	A high CPU usage issue preventing users from authenticating has been fixed.
27852	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.
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.
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 reassociation request, association request, reassociation response, association response message from APs have been fixed.

Table 15 *AOS-W 3.3.1.17*

Bug ID	Description
27896	The 802.11a channel is now enabled for Ecuador (EC) country code.
27648	The issue with incorrect temperature alerts on S3s have been fixed.
27041, 29232	The age out of entries is now correctly displayed in the 'show ap active' and 'show ap association remote' command.
25724	Misleading log messages related to localdb have been eliminated.
27734, 27724, 28999, 28028	Multiple auth module crash issues have been fixed.

Table 16 *AOS-W 3.3.1.16*

Bug ID	Description
24961	Performance issues with two APs connected on the same channel has been fixed.
26396, 27259, 27762, 28662	Several auth crash issues have 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.
26686, 27654, 27173	Throughput performance issues with WPA2-AES and WPA2-PSK have been fixed.
26734	The WebUI now correctly reports the firewall processing of client traffic.
27594	Crash issues with AP 125 when connected to enet with mis-match port setting have been fixed.
27623	The issue with 'write mem' command sometimes causing the switch to crash has 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.
27772	The issue with a local switch not forwarding ARP packets when voip-proxy-arp is disabled or not used VRRP has been fixed.
27957	The breadcrumbs text on the Security > Authentication > Advanced page now displays the correct information.
28061, 28223, 19977	An issue with kernel panic during boot time has been fixed.
28534	Issue in configuring the link profile has been fixed.
28580	Issue with S3 crashing during to datapath timeout has been fixed.

Table 17 *AOS-W 3.3.1.15*

Bug ID	Description
22916	The user role now changes to the Captive Portal role after the user successfully authenticates in Captive Portal via VPN.
23487, 24725	You can now use the VRRP address (VIP) as a multiplexer server address to terminate multiplexors.
24401, 25362, 22647	The user table entries are deleted properly after the IPSEC SA / L2TP tunnel has timed out.
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.

Table 17 *AOS-W 3.3.1.15*

Bug ID	Description
27654, 27173	Throughput performance issues with WPA2-AES and WPA2-PSK have been fixed.
27688	When Captive Portal is used for VPN users, a DNS response to the client is now received through the tunnel properly.
27087	Error in classifying frames into the correct WMM category has been fixed.
27106	An e-mail address that contains the @, hyphen, period, underscore special characters can be used as the guest username.
27645	Auth crash issues have been fixed.
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.
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
28007	The issue with not being able to set expiry time for a user in the internal DB has been fixed.

Table 18 *AOS-W 3.3.1.14*

Bug ID	Description
22960	The issue with local bridge on ENET1 not working for AP's has been fixed.
23306	Extraneous error message generated during AP boot up has been fixed.
24818	The issue with custom Captive Portal welcome page redirection not working after upgrading to 2.5.6.0 has been fixed.
25206, 27429	Packet drops to control path during flood has been fixed.
26552, 27040	The issue with the priority value not being restored for tracked interfaces has been fixed.
26685	The issue with a busy master switch is dropping DB SYNC ack when has been fixed.
26998	You can now get the status of the AP connected to the Aeroscout server and discover tags.
27474	When VRRP is enabled for a non-existent VLAN, Module Layer2/3 because busy. This issue is now fixed.
27490	The ADD value for both tracking VLAN and interface for VRRP configuration is removed.
27680	Customized Captive Portal users are redirected properly when the initial authentication fails.
27841	The issue with adding more than two Gigabit Ports added under port channel interface missing after reboot has been fixed.
27965	The issue with S3 Mark 1 crashing has been fixed.
27657	The temperature display for OAW-AP12x has been removed.
27705	Retrieving the switches CPU load via SNMP was inaccurate, this issue is resolved.
27775	The issue with A5000/A6000 Supervisor Cards (SC1 or SC2) in slot 0 and Supervisor Card S3 Mark 1 in slot 1 resolving to the same base MAC address has been fixed.

Table 18 *AOS-W 3.3.1.14*

Bug ID	Description
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.
27965, 28228	Switch reboot during network flood has been fixed.
28052	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.

Table 19 *AOS-W 3.3.1.13*

Bug ID	Description
26286	When mobility is enabled on a mux server, wired clients associated with it do not get an IP address from the DHCP server. This issue is now fixed.
26750	The issue with IDS profile “ids-high-setting” causing OAW-AP125 to crash under network load has been fixed.
26940	Support for mux-tunnel forwarding-loop prevention added.
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	The issue with the 2400 switch crashing frequently has been fixed.
27744, 19977	An upgrade to 3.3.1.11 version causing the switch to reboot has been fixed.

Table 20 *AOS-W 3.3.1.12*

Bug ID	Description
22929	The connectivity issue with a wired device connected to enet1 has been fixed.
23722	The unicast response message from a DHCP server is now correctly forwarded by the relay to the client that initiated the message.
25146	Appropriate bandwidth contract is now applied between two known users.
26461	When a running configuration is copied via FTP, the configuration file is copied to a directory if it is specified. By default, they configuration file is copied to the root directory.
27163	You can now configure any country code in a regulatory domain profile, regardless of the country of the switch.
27286	The WebUI now supports Firefox 3.
27404	More Data bit for all frames are reset when a client switches from WMM-UASPD power-save to power-active mode.
27405	An AP now accounts for the first power-save frame from client after the association.
27415	The Captive Portal proxy can now be connected to port 80 in the base operating system.
27514	All on-valid SSIDs are classified as rogue, when Rogue AP classification is disabled.
27587	The issue with TKIP clients unable to receive broadcast traffic has been fixed.
27623	The issue with 'write mem' command sometimes causing the switch to crash has been fixed.

Table 21 *AOS-W 3.3.1.11*

Bug ID	Description
26782	Inconsistent channel information issue for the 40Mhz spectrum in RF Plan has been fixed.
27118	CDR buffer causing an overload of log messages in the console has been fixed.
27211	The issue with a management user created using the WebUI not being displayed in the WebUI has been fixed.
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.

Table 22 *AOS-W 3.3.1.10*

Bug ID	Description
23328	Memory leak due to extremely large WMS database has been resolved.
24286	The issue with users in the L3 table not being removed after the idle time-out period 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.
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.
26647	The issue with user entries of the disconnected VPN users still persisting in the user table has been fixed.
26653	A new parameter has been added to fix the MAC connectivity issue due to timer 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.
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 provides information on clients based on the following HT Types: ● Active Interfering Clients ● Active Valid Clients ● Top Talker Clients
26896	The issue with delay in creating mesh link between two OAW-AP70s has been fixed.
26904	TKIP re-keying issue causing multicast packets to be dropped has been fixed.
27105	The issue with multiple auth manager crash has been fixed.

Table 23 *AOS-W 3.3.1.9*

Bug ID	Description
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.
25586	The issue with traffic not moving across the master / local tunnel has been fixed.

Table 23 *AOS-W 3.3.1.9*

Bug ID	Description
26462	The 'user_add' XML-API command can now be used in systems that have VLAN interfaces defined with non /24 netmask.
26689	The issue with 'httpd' not starting after an image is loaded to the switch 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.
26760	The issue with the WebUI (Monitoring > Network > All Access Points) displaying incorrect number (0-zero) of clients associated with an AP has been fixed.
26772	After upgrading from 2.5 to 3.3.1.x, users with certain chipsets (Inter 3945ABC) could not connect to a bridged SSID. This has been fixed.
26985	Setup Wizard help files are updated.

Table 24 *AOS-W 3.3.1.8*

Bug ID	Description
22900	The issue with the 'show user-table station' command failing has been fixed. The 'show user-table station' command now works with large number of stations.
23327	You can now blacklist known and unknown clients to the switch permanently.
24061	You can now view the status of RADIUS and LDAP servers.
24976	The issue with high retry rates causing poor voice quality in Vocera badges has been fixed.
25533	An issue with the CPU running at 100% utilization has been fixed.
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 Base OS, the user is given AAA profile initial role instead of "denyall" role. An L3 authentication can still be performed. ● The max-authentication-failure option in MAC auth profile is removed from the WIP license.
25821	The issue with OAW-AP70 not working after upgrading from 2.5.6.2 to 3.1.1.12 with the country code JP3 has been fixed.
25902	Backward compatible legacy traps 'wlsxSignatureMatchAP' or 'wlsxSignatureMatchSta' are now generated whenever the new factory default signature matches traps like 'wlsxSignAPDeauthBcast' and 'wlsxSignStaDeauthBcast'.
25987	The issue with db sync between the master switches when the RF plan is included has been fixed.
26041	The outdoor channels (20MHz) for Turkey (TR) in 2.4 GHz band has been enabled.
26097	The issue with low performance with legacy clients on OAW-AP125 has been fixed.
26132	The issue with mesh point not working with JPX country code has been fixed.
26348	The issue with active probe-req and Auth messages during a call has been fixed.
26957	The issue with STM crashing on the master switch has been fixed.

Table 25 *AOS-W 3.3.1.7*

Bug ID	Description
26268	The issue with the Captive Portal login page not displaying after upgrading to 3.3.1.5 has been fixed.

Table 26 *AOS-W 3.3.1.6*

Bug ID	Description
26074	Stateful firewall for IPv6 is disabled by default. To enable the stateful firewall for IPv6 use the “ipv6 firewall enable” command.
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.
25094	The issue with not being able to save an RF plan after updates has been fixed.
25991	The issue with mgmt-user radius authentication based on calling-station-id and nas-port-id has been fixed. When using a RADIUS server 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.
26249	The time difference issue on the 4504, 4604, and 4704 platforms has been fixed.
26426	The watchdog timer issue on OAW-AP85 has been fixed.

Table 27 *AOS-W 3.3.1.5*

Bug ID	Description
24704	You can now drop broadcast and multicast packets in air using the “drop-mcast” option in the “wlan ssid-profile” command. When the “drop-mcast” option is enabled, all downstream broadcast and multicast traffic is dropped. **NOTE:** You must enable the “voip-proxy-arp” option before using the “drop-mcast” option.
25656	The issue with datapath timeout error and the subsequent rebooting of the switch has been fixed.
25743	The issue with the 'admin' user role in CLI changing to a snmp user role after a switch reboot has been fixed.
25911	The issue with LEAP 802.1x authentication not working in IBM Access client with Atheros driver has been fixed.
26035	The issue with the crash of STM module caused by SIP-TCP messages of large size has been fixed.
26067	The issue with RAPs not working after downgrading from 3.3 to 2.5.xhas been fixed.

Table 28 *AOS-W 3.3.1.4*

Bug ID	Description
22654	The issue with incorrect output in the “show user-table” command has been fixed. The “show user-table” 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.
24973	The issue with messages being sent due to fan failures have been fixed.

Table 28 *AOS-W 3.3.1.4*

Bug ID	Description
25196	The “show user-table unique” command now outputs the correct number unique users.
25336	The issue with the switch crashing during upgrade from 3.3.1.0 to 3.3.1.1 has been fixed.
25750	The issue with the depleting storage space in flash has been fixed.

Table 29 *AOS-W 3.3.1.3*

Bug ID	Description
25345	The issue with clients not able to authenticate in a LEAP setup using Cisco ACU version 4.x has been fixed.

Table 30 *AOS-W 3.3.1.2*

Bug ID	Description
24704	When a wireless phone roams to another AP, it sends ARP and DHCP requests. In a large VoWLAN deployment, this generates heavy broadcast traffic in the air resulting in a drop of broadcast and multicast traffic in the air. You can now enable the ***voip-proxy-arp*** option to convert all broadcast ARP requests to unicast and prevent traffic loss.
24605	RFE 852 is implemented to provide the mapping of WMM categories to the corresponding DSCP fields in the upstream traffic and mapping of DSCP value to WMM categories in the downstream traffic.
24598	The issue with the **show ap monitor debug status** command displaying incorrect AP scanning status has been fixed.
24417	When the controlled is reloaded, the **show wms general** command now displays correct value for ***classification-server-ip*** option.
24415	The issue with the **snmp-server host** command being removed from the running config after the **snmpd** is restarted has been fixed.
24394	The Hello packets will not send fixed and provisioning information as strings in request. This fixes the issue of APs with longer **ap-name** or **ap-group-name** not starting
24365	An AP is sometimes classified as a suspect-rogue even though it should be a rogue AP. This happened due to the presence of the gateway MAC address in the APs’ wired MAC table. This is now fixed and further checks are implemented to classify the AP as a rogue AP.
24358	The ARM power upgrade issue has been fixed.
24350	If the mac or eth ACL is deleted from a role, the deletion is now propagated to a remote AP.
24343	If a wired user plugs a machine into the port before the AP has downloaded its config from the switch, the wired user would not be assigned to the correct AP group and thus the rules that were AP group specific would not apply. This is now fixed to update the AP group on existing wired users.
24211	The duplicate ID problem in the **show login sessions** command output has been fixed.
24209	The **show audit-trail** [***value***] command has been fixed to accept only a numeric value.
24153	The issue with the switch rebooting at large bursts of un-encrypted traffic has been fixed.
24119	RAP upload speeds have been increased, eliminating an occasional cause of watchdog timeouts at high upload rates.

Table 30 *AOS-W 3.3.1.2*

Bug ID	Description
24076	Fragmented data are now re-assembled after decryption as a single PDU enabling AP to forward the re-assembled data.
24064	A bug on the switch leaks the broadcast frames after conversion to unicast to other VLAN. This has been fixed to forward unicast frames only to clients on VLAN of the broadcast packet.
24041	The captive portal redirect URL now uses the Common Name found in an uploaded SSL certificate.
24008	Under some conditions, transmitting greater than 7Mbps of upstream UDP traffic may cause Remote APs to reboot. This issue has been fixed.
23918	Path MTU value is reduced to allow RAP to function properly.
23754, 23915, 23916	Multiple issues with Remote Mesh Portal has been fixed.
23753	An AP will now accept two or more PMKIDs contained in an association request as per the 802.11i specification.
23704	The issue with a switch randomly re-booting with the “Datapath Time Out” cause message has been fixed.
23662	SNMP will now clear the memory when MMS is removed from a switch.
23606	The issue with OAW-AP65 rebooting during a packet capture has been fixed.
23472	A session initiated from the call manager is allowed to the client in addition to the one initiated by the client. This fixes the QoS issue for a call from a land line phone to a wireless handset
23370	The max EIRP value for SG (Singapore) country code is set to 23 dBm for 2.4 GHz in all APs
23367	The max EIRP value for MY (Malaysia) country code is set to 27 dBm for the 2.4 GHz band in all APs
23321	SOS adds a route cache entry only if it is an ARP response.
23302	If a RAP was not connected to any switch with the UP state, on a switch tunnel directive, it would now try to switch over to the next switch instead of rejecting that RAP.
23273	A problem has been repaired that caused the AP’s CPU to become overloaded under some conditions.
23223	The AP debug show commands now properly report GRE tunnel heartbeats sent and received.
23203	The Enet1 port on a Remote OAW-AP70 will now properly autonegotiate their link at all times.
23141	The RAP watchdog timeout issue while attaching clients has been fixed.
23090	Wired devices are now able to pass traffic properly to the Enet1 port on a Remote OAW-AP70.
23088	The filter search option for MAC/CP authenticated under Monitoring > Switch > Clients have been fixed.
23076	The WebUI Policy configuration screen is now displayed properly.
23075	After a Remote OAW-AP70 reboot, wired devices attached to the Enet1 port will now authenticate correctly.
22957	Remote APs will now correctly establish a connection with the LMS-IP and backup LMS-IP.
22930	The out of memory issue due to high throughput has been fixed.
22911	Under some conditions, bulk provisioning of Remote APs would cause a portion of those APs to fail to boot. This has been fixed.
22902	A switch reboot issue has been fixed.

Table 30 *AOS-W 3.3.1.2*

Bug ID	Description
22898	An AP crash has been fixed.
22867	WebUI error messages displayed when configuring AP groups have been fixed.
22616	Wired port session ACL information is now displayed correctly in the “show acl hits” command.
22354	The issue with high packet loss occurring on the Alcatel-Lucent S3 and Alcatel-Lucent 4504, 4604, and 4704 OnmiAccess Switches while sending AES-CCM and TKIP encrypted fragmented “ping” packets to the switch's IP address has been fixed.
22303	PPPoE was not used on APs as it might have caused frequent AP reboots.
21108	The issue with SNMP query for user phy type has been fixed.
21006	When SVP was enabled, background data traffic could degrade voice quality.
20929	When a new VLAN is created and added to two existing ports, they were not added to the two trunk ports of an allowed VLAN list. Instead, one of the ports would become an access port for the VLAN. This issue has been fixed.
19494	The issue with excess bi-directional UDP traffic causing the mesh wireless link to flap has been fixed.

Known Issues and Limitations in AOS-W 3.3.1

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

NOTE

When upgrading S3 and 4504, 4604, and 4704 WLAN switches from AOS-W 3.2.0.x to 3.3.1.0, 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 at Alcatel-Lucent WLAN switch webUI or “show license” command at Alcatel-Lucent WLAN switch CLI; if not, please re-install the licenses and reboot the system WITHOUT saving your configuration.

NOTE

AOS-W 3.3.1 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 31 *Known Issues and Limitations*

Bug ID (if any)	Description
25162	In this release, S3 and 4504, 4604, and 4704 WLAN switches do not support VRRP pre-emption. Workaround: After both VRRP pairs return to operational state, manually “shutdown” and “no shutdown” the current VRRP master instance to trigger VRRP backup instance with higher priority to take over.

Table 31 *Known Issues and Limitations*

Bug ID (if any)	Description
25134	Setup Wizard: If there are any configuration errors when the user clicks the Finish button, an error message appears in a dialog box and the wizard stops sending configuration commands to the switch. Workaround: Power down the switch, then power it on again. Restart the wizard.
25132	After upgrading Alcatel-Lucent WLAN switches to 3.3.1 software release, the “Acceptable Coverage Index” value should be left as-is and the “Ideal Coverage Index” value should be set to 10, under the “rf arm-profile”. This is required to allow Alcatel-Lucent APs to utilize max-power settings, if allowed by the Adaptive Radio Management (ARM).
25114	Adhoc containment for 802.11a/b/g APs is not functional in the 5GHz band.
25109	ACL new hits and total hits may show incorrect values for “redirect src-nat” enabled session ACLs.
25107	Setup Wizard: Changes to the default speed and duplex mode for a port are not applied. Workaround: After completing the Setup Wizard and rebooting the switch, use the CLI or WebUI to change the speed or duplex mode for a port.
25057	User may temporarily get assigned to the logon role instead of the initial role in the AAA profile. Workaround: Reauthenticate the client device.
25043	Without active AP licenses on the Alcatel-Lucent S3 and 4504, 4604, and 4704 platforms, it is not possible to provision a remote AP. Workaround: Temporary AP licenses on the same WLAN switch can be used to enable remote AP provisioning. Another WLAN switch with available AP license limit can also be temporarily used to provision the correct parameters on the remote AP.
25042	SIP calls are allowed even if the voip-cac-profile configuration has the VoIP SIP Call capacity set to “0”.
25031	When users select a different server group for the authentication server group, the WLAN 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
25017	Adhoc network detection will also trigger interfering ap detection against the adhoc network devices; this alarm can be ignored.
24995	Setup Wizard: If the user moves the port on which the Setup Wizard is connected from VLAN 1 to a new VLAN, the web browser window will hang after the user clicks the Finish button. Workaround: The user just needs to close the browser window. The configuration is written properly to the switch.
24951	This release does not support wireless containment on the OAW-AP124 and OAW-AP125 802.11n access points.
24942	Setup Wizard: The month, day, and year in the Date & Time drop-down menus do not reflect changes made with the calendar icon. Workaround: Enter the month, day, and year using the drop-down menus.
24882, 24685	State of APs terminated on the local WLAN switch can sometimes be reported differently on the master WLAN switch. Workaround: Use the **`show ap active`** command in the local WLAN switch CLI to monitor AP states that are terminated on the local WLAN switch.
24778	Not able to configure the role-based reauthentication interval from the WLAN switch CLI. Workaround: Use the WLAN switch WebUI to configure the role-based reauthentication interval.
24761	Enabling port mirroring on a 1 Gbps port to a 100 Mbps port is not supported on S3 and 4504, 4604, and 4704 Alcatel-Lucent WLAN switches. Port mirrors should be disabled whenever not in use in order to prevent performance impact on these type of WLAN switches.

Table 31 *Known Issues and Limitations*

Bug ID (if any)	Description
24749	The 40MHz channel cannot be enabled against the "KR" country code for the OAW-AP124 and OAW-AP125.
24748	Not able to add channels to the regulatory domain using the WLAN switch webUI. Workaround: Use the WLAN switch CLI to add channels to the "ap regulatory-domain" configuration.
24628	The following relates to bridging devices connected to the wired Ethernet ports of a mesh portal or mesh point: Wired AP profile—If a parameter in the Wired AP profile is modified, it will not take effect until the user toggles the "wired-ap-enable" flag. To do this, you must use the "no wired-ap-profile" command followed by the "wired-ap-enable" command for the change to be applied. Native VLAN in the AP system profile—If the user connects 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 must also set the native VLAN in the AP system profile to that value.
24601, 24724	The WLAN switch WebUI may show the number and state of APs and AMs incorrectly. Workaround: Use the **`show ap active`** command in the local WLAN switch CLI to monitor AP states that are terminated on the WLAN switch.
24428	When all of the servers in a server group time out, the next authentication attempt will wait until the "dead timer" expires.
24330	Failed captive-portal authentication attempt shows the default captive portal page and not the customized background.
24234, 23496	During Alcatel-Lucent WLAN switch upgrade, FTP and SCP should be used as the preferred image transfer methods. Using TFTP as the image transfer method may cause transfer timeouts to occur.
24219	User VLAN may not show correctly in the WLAN switch WebUI. Workaround: Use the **`show user`** command in the WLAN switch CLI to verify correct client VLAN assignment.
24210, 21240	When upgrading S3 and 4504, 4604, and 4704 WLAN switches from AOS-W 3.2.0.x to 3.3.1.0, unless NTP is used, the system clock might move forward 3 hours. Workaround: 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 at Alcatel-Lucent WLAN switch webUI or "show license" command at Alcatel-Lucent WLAN switch CLI; if not, please re-install the licenses and reboot the system WITHOUT saving your configuration.
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 does not occur when an external DHCP server is used or layer-3 mobility is enabled on the switch. Workaround: When using the switch's DHCP server, force a release/renew of the DHCP lease on the client.
24148	Atheros 11n chipset installed clients may associate at the 54Mbps 802.11 rate after "stm kick-off station" command or after OAW-AP124/OAW-AP124 channel change. Workaround: Reassociate the client to the OAW-AP124/OAW-AP125.
24147	VLAN assignment might be wrong during MAC authentication. Workaround: Disable dos-prevention if this problem is observed.
24108	The WebUI and the CLI prevents configuration of an OAW-AP70 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 will fail if the DHCP server returns more than one domain name.

Table 31 *Known Issues and Limitations*

Bug ID (if any)	Description
24061	WebUI/CLI: Radius server status is always “Up” or “In service”. Workaround: Use “ping” or other mechanisms to verify network connectivity with the RADIUS server and verify that RADIUS service is still enabled and running on the server in case of authentication timeouts.
24042	Changing the IPSEC key on a master/local deployment with VRRP enabled causes a loss of connectivity until the master switch is rebooted. Workaround: Manually trigger a VRRP state change from master to backup, then return it to master.
24017	When using an 802.11e-capable device with TSPEC, the AP does not respond properly to an ADDTS request.
23957	The association table of the OAW-AP80M configured for static WEP may fill up with invalid entries over time, preventing further client association.
23949	PPPoE should not be used on remote APs operating in split-tunnel mode or if it has offline (backup/always) mode virtual APs. If clients connect to split-tunnel or offline (backup/always) virtual APs on a PPPoE remote AP, traffic is not passed to bridged destinations.
23929	APs do not respond to SNMP queries even though SNMP has been enabled.
23907	This release does not support Xsec opmode SSIDs for the OAW-AP124 and OAW-AP125.
23893	Bandwidth contracts do not work properly on the Alcatel-Lucent S3 and 4504, 4604, and 4704 platforms.
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 OAW-AP70 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.
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 2.4GHz and 5GHz bands. Workaround: Use dedicated air monitors or deploy dual-radio access points.
23719	After changing the IP address of a master switch, local switches may not re-build their IPSEC tunnel to the master. Workaround: Reboot the local switch.
23713	Checkbox selections may get lost after WebUI auto refresh.
23690	APs will only show up under the WebUI “unprovisioned” link 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.”
23669	SNMP total AP count will not include APs that do not have VAPs enabled. Workaround: Use the “show ap active” command on the WLAN switch to monitor the total AP count

Table 31 *Known Issues and Limitations*

Bug ID (if any)	Description
23631	LDAP authentication does not differentiate between server unreachable and user unauthorized. If local management authentication is disabled, and the LDAP server used to authenticate management users is unreachable, use password recovery to log into the switch and revert to the local database for authentication. For information about password recovery, see “Resetting the Admin or Enable Password” in the *AOS-W 3.3.1 User Guide*.
23437	In some cases voice call admission control load balancing may not function correctly. Workaround: Retry call request or association on the voice client.
23327	A blacklisted client will only remain blacklisted for a maximum of 3600 seconds, even when the block time has been set to zero.
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.
23175	This release does not support the RF Troubleshooting functionality (RFT) on the OAW-AP124 and OAW-AP125.
22960	Local bridging on enet1 does not work for OAW-AP70 access points that are not remote APs or Mesh nodes.
22925	The OAW-AP124 and OAW-AP125 might fail to boot up across a 100 MB half duplex link.
22849	Creating firewall policies with spaces in the names may cause the user's web browser to hang when displaying firewall policies.
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.
22475	This release does not support per-SSID bandwidth contracts on the OAW-AP124 and OAW-AP125.
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 WLAN switch from master to local. Workaround: Before changing the role of the WLAN switch from master to local, use the “clean wms-db” command on the WLAN switch.
22227	L3 mobility across WLAN switches that are configured with VRRP redundancy may not work as expected. Workaround: Disable VRRP pre-emption in this configuration scenario.
22203	The switch cannot authenticate users with special UTF-8 characters in their username.

Table 31 *Known Issues and Limitations*

Bug ID (if any)	Description
22199	AAA FastConnect for EAP-TLS may fail if the authentication profile is configured before the CA certificate is loaded. To work around this problem, load all certificates before configuring the authentication profiles.
22190	L2 ACLs (MAC and Ethertype) do not work properly on the Alcatel-Lucent S3 and the Alcatel-Lucent 4504, 4604, and 4704 OmniAccess Switches.
21897	Microsoft Vista VPN Dialer behind a NAT device does not fail to establish a VPN session with the WLAN switch.
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.
21338	The WIP module may be logging "Disconnect Station Attacks" for mesh nodes incorrectly. If this occurs, disable detection of "Disconnect Station Attacks".
20797	Multicast streaming will not work if DTIM is not equal to 1. Workaround: To support multicast streaming applications, configure DTIM period under the SSID profile to "1".
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.
20456	L3 roaming of wireless clients with static IP addresses across WLAN switches is not supported.
20274	GRE tunnel endpoint cannot be the VRRP IP address of a VRRP redundant pair of WLAN switches.
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	Wired authentication support on ENET1 of an AP70 remote access point is not supported if "split-tunneling" is enabled.
20134	A "sapd" error message may be seen on switches 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.
19602	The AP must be rebooted after WMM is disabled for Spectralink Voice Protocol to work with an acceptable retry rate.
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.

Table 31 *Known Issues and Limitations*

Bug ID (if any)	Description
17701	The “show memory fpapps” command does not work on the S3 and the Alcatel-Lucent 4504, 4604, and 4704 switches.
17688	To deny access to a specific WLAN 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	A wired client connected to an Alcatel-Lucent OAW-4308 or Alcatel-Lucent OAW-4324 will fail 802.1x authentication. The message “Dropping EAPOL packet” appears in the logfile of the Alcatel-Lucent OAW-4308/OAW-4324. Workaround: Configure the MUX client as master and disable 802.1x.
14119	The WLAN switch does not perform NAT for traffic originated by the WLAN 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 OAW-AP124 and OAW-AP125 may not function as expected in 10 Mbs mode.
	This release does not support the secure enterprise mesh functionality on the OAW-AP124 and OAW-AP125.
	This release does not support the remote AP functionality on the OAW-AP124 and OAW-AP125.
	This release does not support FCC DFS on the OAW-AP124 and OAW-AP125.
	ETSI DFS is supported but not yet fully certified on the OAW-AP124 and OAW-AP125 at this time.
	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 OAW-AP80M uses only approved outdoor channels; however, the administrator can configure any channel using the CLI and the WebUI. If this occurs, the OAW-AP80M 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

The following new documents are available with this release:

- *Alcatel-Lucent OAW-AP120 Series Indoor Access Point Installation Guide*
- *OAW-AP120 Series AP Mounting Kit Installation Guide*

New revisions of the following documents are also part of the documentation set for this release:

- *AOS-W 3.3.1 User Guide*
- *AOS-W 3.3.1 Command Line Interface Reference Guide*

- *AOS-W 3.3.1 Quick Start Guide*
- *AOS-W 3.3.1 MIBs User Guide*
- *AOS-W 3.3.1 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:

Table 32 *Contact Information*

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

Table 33 *Contact Information*

Telephone Support	
North America	1-800-995-2696
Latin America	1-877-919-9526
Europe	+33 (0) 38 855 6929
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507