AOS-W Instant 6.2.0.0-3.2.0.4

Release Notes

www.alcatel-lucent.com

26801 West Agoura Road
Calabasas, CA 91301

Contents

Chapter 1

Release Overview

AOS-W Instant 6.2.0.0-3.2.0.4 is a patch software release that introduces fixes to issues detected in previous releases.

For more information on features described in the following sections, see the AOS-W Instant 6.2.0.0-3.2 User Guide.

Chapter Overview

- "What's New in this Release" on page 7 lists the new features introduced in this release.
- "Features Added in the Previous Releases" on page 11 describes the new features that were added in the previous release of AOS-W Instant.
- "Known Issues in Previous Releases" on page 25 lists the known issues reported in previous releases of AOS-W Instant.

Contacting Support

Table 1 *Alcatel-Lucent Contacts*

Contact Center Online	
• **Main Site**	http://www.alcatel-lucent.com/enterprise
• **Support Site**	https://service.esd.alcatel-lucent.com
• **Email**	esd.support@alcatel-lucent.com
Service & Support Contact Center Telephone	
• **North America**	1-800-995-2696
• **Latin America**	1-877-919-9526
• **Europe**	+33 (0) 38 855 6929
• **Asia Pacific**	+65 6240 8484
• **Worldwide**	1-818-878-4507

This chapter provides a list of fixed bugs and known issues in this release of AOS-W Instant.

Fixed Issues in this Release

Access Point Platform

Table 1 *Access Point Platform Fixed Issue*

Bug ID	Description
79966	**Symptom:** OAW-AP104, OAW-AP105, and OAW-IAP9x in a cluster rebooted randomly with the **master transitioned to local** reboot reason. Changes to the OAW-IAP's internal process have resolved this issue. **Scenario:** This issue was observed when the OAW-IAPs rebooted randomly, although there were less number of clients connected to the OAW-IAP. Due to this issue, the slave OAW-IAPs could not connect to the master OAW-IAP. This issue was found in OAW-AP104, OAW-AP105, and OAW-IAP9x running AOS-W Instant 6.2.0.0-3.2.

Access Point Wireless

Table 2 *Access Point Wireless Fixed Issues*

Bug ID	Description
80334	**Symptom**: After connecting to the 2.4 GHz band on an OAW-IAP, the clients were disconnected from the OAW-IAP intermittently. Changes to the AP scan flag clearing mechanism have resolved this issue in AOS-W 6.2.1.1. **Scenario:** Sometimes, when an AP deferred scanning, some scan flags on AOS-W were turned on. Due to this, the APs could not transmit data frames.
80094	**Symptom:** Some clients could not connect to the open SSID. Changes to the information in association response packets sent to the clients have resolved this issue. **Scenario:** This issue occurred when the association response packets were sent with **Privacy enabled** information for the clients connected to an open SSID.

Adaptive Radio Management (ARM)

Table 3 *Adaptive Radio Management Fixed Issues*

Bug ID	Description
81332	**Symptom:** A client could not access the Internet when connected to a slave OAW-IAP. Changes to the SSID configuration have resolved this issue. **Scenario:** This issue occurred when a client was assigned an IP address by the Virtual Controller in the guest VLAN, with the Extended SSIDs feature enabled on the OAW-IAP. This issue was found in the OAW-IAPs running AOS-W Instant 6.2.0.0-3.2.
75756	**Symptom:** A OAW-RAP109 was unable to detect the correct channels for the JP3 (Japan) regulatory domain. Changes to the signal detection mechanism have resolved this issue. **Scenario:** This issue occurred when the OAW-RAP109 configured to operate on channel 52+ could not detect RADAR and constantly switched channels. This issue was found in OAW-RAP109 and was not limited to any specific AOS-W Instant software version.

AirGroup

Table 4 *AirGroup Fixed Issue*

Bug ID	Description
83144	**Symptom:** Clients could not connect to the AirGroup services such as AirPrint and AirPlay. Changes to checksum of the AirPrint or AirPlay discovery packets proxied by the OAW-IAP have resolved this issue. **Scenario**: This issue occurred when the AirPrint and AirPlay discovery packets proxied by the OAW-IAP were discarded by some third-party routers. This issue occurred due to checksum errors in the packets proxied by the OAW-IAP and was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2.

AirWave

Table 5 *AirWave Fixed Issue*

Bug ID	Description
82419	**Symptom:** Incorrect user role information was displayed in AirWave. Changes to the OAW-IAP's role retrieval mechanism for the AirWave Management Platform (AMP) have resolved this issue. **Scenario:** This issue occurred when an OAW-IAP sent incorrect user role information to the AirWave server. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2 with AMP 7.7.0402 version.

Captive Portal

Table 6 *Captive Portal Fixed Issue*

Bug ID	Description
81518	**Symptom:** A guest user could not access the Captive portal page when connected to the Wi-Fi network. Changes to the HTTP request handling procedure have resolved this issue. **Scenario:** The issue occurred when the Tinyproxy server did not work for wired connections. Due to this unusual behavior, the captive portal page did not show up for clients in the wireless network. The issue was not specific to any software version.

DHCP

Table 7 *DHCP Fixed Issue*

Bug ID	Description
81302	**Symptom:** An OAW-IAP used an old Gateway address after the DHCP lease renewal. Changes to the default router configuration in DHCP clients have resolved this issue. **Scenario:** This issue occurred when an OAW-IAP used an old gateway address instead of the new default gateway after a DHCP lease renewal. Due to this issue, the client traffic destined to the OAW-IAP was discarded. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2.

SNMP

Table 8 *SNMP Fixed Issue*

Bug ID	Description
80274	**Symptom:** The SNMP trap host could not be configured on the OAW-IAPs. Changes to the OAW-IAP configuration saving mechanism have resolved this issue. **Scenario:** This issue occurred when the OAW-IAPs could not save the SNMP trap host information configured by the users. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2.

Station Management

Table 9 *Station Management Fixed Issue*

Bug ID	Description
80274	**Symptom:** Some clients could not connect to the open SSID. Changes to the Privacy enabled information in assoication response packets have resolved this issue. **Scenario:** This issue occurred when the OAW-IAPs could not save the SNMP trap host information configured by the users. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2.

Known Issues and Limitation

The following known issue is identified in the AOS-W Instant 6.2.0.0-3.2.0.4 release.

Table 10 *Authentication Known Issue*

Bug ID	Description
75821	**Symptom:** Radius authentication fails on the OAW-IAPs with the Dynamic Proxy feature enabled. **Scenario:** This issue occurs when the RADIUS server response is lost due to network issues resulting in multiple outstanding RADIUS authentication requests. This issue is found in OAW-IAPs running AOS-W Instant 6.1.3.1-3.0 or later, in the L2 network topology.

Chapter 3

Features Added in the Previous Releases

This chapter provides a list of the new features included in the previous version of AOS-W Instant.

New Features and Enhancements in AOS-W Instant 6.2.0.0-3.2

Fast Failover with Two Tunnels

With this feature, an Instant AP (OAW-IAP) creates a backup VPN tunnel to the switch along with the primary tunnel, and maintains both the primary and backup tunnel separately. If the primary tunnel fails, the OAW-IAP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.

WISPr Authentication

AOS-W Instant now supports authentication for Wireless Internet Service Provider roaming (WISPr). WISPr authentication allows a smart client to authenticate on the network, when they roam between wireless internet service providers (ISP), even if the wireless hotspot uses an ISP with whom the client may not have an account.

If you are a hotspot operator using WISPr authentication and a client that has an account with your ISP attempts to access the Internet at your hotspot, your ISP's WISPr AAA server authenticates that client directly and allows the client access on the network. If, however, the client only has an account with a *partner* ISP, then your ISP's WISPr AAA server forwards that client's credentials to the partner ISP's WISPr AAA server for authentication. When the client is authenticated on the partner ISP, it is also authenticated on your hotspot's own ISP as per their service agreements. The OAW-IAP assigns the default WISPr user role to the client when your ISP sends an authentication message to the OAW-IAP.

AOS-W Instant supports the following smart clients:

- iPass
- Boingo

These smart clients enable client authentication and roaming between hotspots by embedding iPass Generic Interface Specification (GIS) *redirect*, *authentication*, and *logoff* messages within HTML messages that are sent to the OAW-IAP.

To configure WISPr authentication, go to **Settings > Advanced > WISPr** tab in the AOS-W Instant UI. Once configured, WISPr authentication may be enabled or disabled in the **Networks > New WLAN > Access** tab.

SSH Support on OAW-IAPs

AOS-W Instant supports terminal access for diagnostic purposes only. Telnet access to the CLI has been deprecated as of this release. When the Terminal Access option is enabled, only SSH access to the CLI will be possible.

To enable or disable the SSH access, go to **Settings > Show Advanced options > Terminal access**.

AOS-W Instant Administration Interface Port Change

The port number for the AOS-W Instant administration interface is now changed to 4343. The 80 and 443 port numbers are no longer supported. The HTTP and HTTPS connections to port 80 and 443 respectively will be redirected to port 4343.

Destination NAT Rule in ACL

AOS-W Instant supports configuration of the destination NAT rule, which can be used to redirect traffic to the specified IP address and destination port.

To configure a destination-NAT rule in AOS-W Instant UI, go to **Networks**>**New WLAN**>**Access** tab, click **New** to add a new rule and select **Destination-NAT** from the **Action** drop-down menu.

Destination-NAT configuration is supported only in the bridge mode without VPN.

OAW-RAP108/109 Support

AOS-W Instant now supports OAW-RAP108/109.

AirGroup Support

AOS-W Instant now supports AirGroup™ services. AirGroup is a unique enterprise-class capability that leverages zero configuration networking to enable Bonjour® services such as Apple® AirPrint and AirPlay from mobile devices. Bonjour, the trade name for the zeroconf implementation introduced by Apple, is the most common example. It is supported by most of the Apple product lines, including the Mac OS X operating system, iPhone, iPod Touch, iPad, Apple TV and AirPort Express.

AirGroup solution supports both wired and wireless devices. Wired devices which support the Bonjour services are made part of the AirGroup when the VLANs of the devices are terminated on the Virtual Controller.

ClearPass Policy Manager and ClearPass Guest Features

AirGroup also supports Alcatel-Lucent ClearPass Policy Manager (CPPM).

With Alcatel-Lucent CPPM:

- Users, such as students in dorm rooms can register their personal devices and define a group of users who are allowed to share the users' registered devices.
- Administrators can register and manage an organization's shared devices like printers and conference room Apple TVs. An administrator can grant global access to each device, or restrict access according to the username, role, or user location.

To enable AirGroup in the AOS-W Instant UI, go to **Settings > Air Group**.

Wi-Fi Uplink

The Wi-Fi uplink feature is supported for all the OAW-IAP models but only the master OAW-IAP can establish the uplink. This feature allows the master OAW-IAP to establish Wi-Fi uplinks to **PSK-CCMP**, **PSK-TKIP**, and **open** SSIDs.

- For single radio OAW-IAPs, the radio can be used to serve both wireless clients and Wi-Fi uplink.
- For dual radio OAW-IAPs, one radio is used for both Wi-Fi uplink and to serve wireless clients, and the other radio only serves wireless clients.

To configure a Wi-Fi uplink, go to **Settings > Advanced > Uplink > WiFi** in the AOS-W Instant UI.

Local Probe Request Threshold

This feature allows you to control whether or not a BSSID of an OAW-IAP should respond when a client sends a broadcast probe request frame to search for all available SSIDs. The supported range of Received Signal Strength Indication (RSSI) values is 0-100 dB.

To configure this feature, go to **New > New WLAN > Show advanced options > Local probe request threshold** in the AOS-W Instant UI.

Maximum Clients Threshold

AOS-W Instant now allows you to configure clients for each BSSID on a WLAN. The supported range is 0 - 255 and the default value is 64.

To configure this feature, go to **New > New WLAN > Show advanced options > Max clients threshold** in the AOS-W Instant UI.

Access Control List (ACL) per SSID

This release of AOS-W Instant supports configuration of up to 64 access rules.

Authentication Survivability

This feature provides authentication and authorization survivability against remote link failure for AOS-W Instant when working with ClearPass Policy Manager. When enabled, this feature allows AOS-W Instant to authenticate the previously connected clients using EAP-PEAP authentication even when connectivity to ClearPass Policy Manager is temporarily lost.

To enable Authentication Survivability in the AOS-W Instant UI, go to **New > New WLAN > Security tab > Authentication survivability**.

Additional Authentication Methods per SSID

In previous releases, AOS-W Instant supported MAC, 802.1X, and captive portal authentications on different SSIDs. The network administrator could choose only one of these authentication methods for a SSID. This version of AOS-W Instant supports the following additional methods of authentication on a SSID:

- MAC + 802.1X Authentication
- MAC + Captive Portal Authentication

You can also apply these authentication methods to a wired profile.

MAC + 802.1X Authentication

This authentication method has the following features:

- MAC authentication occurs before 802.1X authentication

  The administrator is allowed to enable MAC authentication for 802.1X authentication. MAC authentication shares all the authentication server configurations with 802.1X authentication. If a wireless or wired client connects to the network, MAC authentication is done first. If MAC authentication fails, 802.1X authentication will not begin. If MAC authentication succeeds, 802.1X authentication is carried out. If 802.1X authentication succeeds, the client is assigned an 802.1X authentication role. If 802.1X authentication fails, the client is assigned a **deny-all** role or **mac-auth-only** role.

- MAC authentication only role

  Allows an administrator to create a **mac-auth-only** role (similar to **machine-auth-only** role concept) for role-based access rules when MAC authentication is enabled for 802.1X authentication. The **mac-auth-only** role is assigned to a client if MAC authentication succeeds and 802.1X authentication fails. If

802.1X authentication succeeds, the role will be overwritten by the final role. The **mac-auth-only** is supported only for wireless clients.

- L2 authentication fail-through

  Allows an administrator to enable the **l2-authentication-failthrough** mode. If this option is enabled and MAC authentication fails, 802.1X authentication is still allowed. If this option is disabled, 802.1X authentication is not allowed. The **l2-authentication-failthrough** option is disabled by default.

To configure MAC + 802.1X authentication, go to the **Network > WLAN > Access** tab of the AOS-W Instant UI.

MAC + Captive Portal Authentication

This authentication method has the following features:

- If the captive portal splash page type is **Internal-Authenticated** or **External-RADIUS Server**, MAC authentication reuses the server configurations.
- If the captive portal splash page type is **Internal-Acknowledged** or **External-Authentication Text** and MAC authentication is enabled, a server configuration page is displayed.
- If the captive portal splash page type is **none**, MAC authentication cannot be enabled.
- MAC authentication only role— You can use the WLAN wizard to configure the **mac-auth-only** role in the role-based access rule configuration section when MAC authentication is enabled with captive portal authentication.

To configure MAC + captive portal authentication, go to the **Network > WLAN > Access** tab of the AOS-W Instant UI.

OAW-IAP and Client Information Synchronization Enhancements

This release improves the process to detect and synchronize the client information between the Virtual Switch and slave OAW-IAP associated with the clients.

OAW-IAP Functions without Uplink

This feature operates in the following scenarios:

- OAW-IAP boots up without uplink.
- All the physical uplinks are down after the boot up.

The following table shows the status of the OAW-IAP before and after the implementation of this feature.

Table 1 *OAW-IAP status before and after this feature*

Scenario	OAW-IAP Status Before	OAW-IAP Status After
OAW-IAP boots up without uplink.	• OAW-IAP functions as a mesh point. • OAW-IAP tries to boot, but fails.	• OAW-IAP functions as a mesh point. • OAW-IAP boots up with default IP or static IP and then performs master election and load configuration. Thus OAW-IAP can setup a local network for its clients.
All the physical uplinks turn down after the boot up completes.	Clients cannot access internet or local network.	OAW-IAP keeps its local network available for the clients.

In both these scenarios OAW-IAP functions as mentioned below:

- OAW-IAP retries all the physical uplinks in **standalone mode**, **uplink enforced**, or **PPPoE configured** mode. If a physical uplink is up, OAW-IAP uses this physical uplink.

- If OAW-IAP reboot time (due to an uplink failure) is more than 5 minutes, the OAW-IAP boots again except when it is in standalone mode where the **uplink is enforced** and **PPPoE configured**.

Preference to an OAW-IAP with 3G/4G Card for Master Election

The Master Election Protocol prefers an OAW-IAP with 3G/4G card, when electing a Virtual Switch (VC) for the AOS-W Instant network during initial startup. The VC is selected as follows:

- If there is more than one OAW-IAP with 3G/4G cards, one of these is dynamically elected as the VC.
- When an OAW-IAP without 3G/4G card is elected as the VC, but is up for less than 5 minutes, another OAW-IAP with 3G/4G card in the network will be elected as the VC to replace the previous VC. The VC that is down reboots.
- When an OAW-IAP without 3G/4G card is already elected as the VC and is up for more than 5 minutes, the VC will not be replaced until it goes down.

Preference to an OAW-IAP with Non-Default IP for Master Election

The Master Election Protocol prefers the OAW-IAP with a non-default IP, when electing a Virtual Switch (VC) for the AOS-W Instant network during initial startup. If there is more than one OAW-IAP with non-default IP in the network, all OAW-IAPs with default IP automatically reboot and the DHCP process is used to assign new IP addresses.

RTLS Enhancement

Real-time Asset Location Server (RTLS) feature is enhanced to send mobile unit reports to the Aeroscout RTLS server for the client stations that are not associated to any OAW-IAP (unassociated stations). The Aeroscout RTLS server is now able to locate unassociated stations.

To configure RTLS, go to **Settings > RTLS** in the AOS-W Instant UI.

IAP-VPN over HTTP

You can use an HTTP connection instead of an HTTPS when the communication between the RAP next generation (RNG) and OAW-IAP is through a VPN. This avoids the overhead of using the HTTPS connection and improves the overall performance.

SNMP Support for Uplink Management Events

This release includes SNMP traps for reporting the 3G/4G uplink changes. The SNMP trap includes five objects as follows:

- **wlsxTrapAPMACAddress**— This object is used to indicate the wired MAC address of an OAW-IAP, for which the trap is being raised.
- **wlsxTrapAPPreviousUplinkType**— This object is used to indicate the type of uplink used before the trap is being raised, including:
  - Ethernet
  - 3G/4G
  - PPPoE
  - Wi-Fi Uplink
- **wlsxTrapAPPreviousUplinkActiveTime**— This object is used to indicate the duration for which the previous uplink was used.
- **wlsxTrapAPActiveUplinkType**— This object is used to indicate the type of the current used uplink which is currently used, including:
  - Ethernet

- 3G/4G
- PPPoE
- Wi-Fi Uplink

- **wlsxTrapAPUplinkChangeReason**— This object is used to indicate the reason for the change in the uplink configuration. This may be due to the following reasons:
  - Physical link down
  - VPN link down
  - Preemption

Daylight Savings Time Configuration

AOS-W Instant allows you to enable daylight saving time on OAW-IAPs if the time zone you selected supports the daylight saving time. This feature ensures that the OAW-IAPs reflect the seasonal time changes in their respective regions.

Basic Wired 802.1X Authentication

In previous releases, OAW-IAP supported the Captive portal and MAC-authentication wired authentication methods. This version of AOS-W Instant introduces a new authentication method, OAW-IAP Wired 802.1X for wired clients.

MAC OUI Role Derivation for Open and PSK SSIDs

In a MAC address, the first three octets are known as Organizationally Unique Identifier (OUI), is purchased from the Institute of Electrical and Electronics Engineers, Incorporated (IEEE) Registration Authority. This identifier uniquely identifies a vendor, manufacturer, or other organization (referred to by the IEEE as the "assignee") globally and effectively reserves a block of each possible type of derivative identifier (such as MAC addresses) for the exclusive use of the assignee.

OAW-IAP uses the OUI part of the MAC address to identify device manufacturers and assigns a desired role for users who have completed 802.1X authentication and MAC authentication.

VLAN Pooling

This release of AOS-W Instant supports VLAN pooling for wireless clients. VLAN pooling allows a single SSID to be mapped to multiple VLANs wherein each client is randomly assigned a VLAN from a pool of VLANs on the same SSID, thereby automatically partitioning a single broadcast domain of clients into multiple VLANs.

To configure VLAN pooling, go to **New WLAN > WLAN Settings > Static**.

Select **Static** to specify a single VLAN, a comma separated list of VLANs, or a range of VLANs for all clients on the new WLAN network.

The following issues have been fixed in the previous releases:

Issues Fixed in 6.2.0.0-3.2.0.3

3G/4G

Table 1 *3G/4G Fixed Issue*

Bug ID	Description
80945	**Symptom:** The `show cellular config` command log displayed the **/aruba/bin/check_usb: 37: Syntax error: end of file unexpected (expecting "fi")**"error message, thereby preventing the detection and provisioning of a cellular USB modem. Changes to cellular configuration process have resolved this issue. **Scenario:** As the cellular configuration triggered a script parser error, the USB modem could not be detected or provisioned automatically. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2.0.2 and was not limited to a specific hardware platform.

Adaptive Radio Management (ARM)

Table 2 *Adaptive Radio Management Fixed Issues*

Bug ID	Description
75126 74968	**Symptom:** The hybrid spectrum monitor functionality on 5 GHz band failed on an OAW-IAP. **Scenario:** This issue occurred when rf dot11a-radio-profile and spectrum-monitor were configured on an OAW-IAP. Due to this issue, the scan result in CLI and AOS-W Instant UI was empty and histogram in the AOS-W Instant UI displayed incorrect data. This issue was found in OAW-AP105 models running AOS-W Instant 6.2.0.0-3.2 or later.
77579	**Symptom:** Although the clients moved out of the RF coverage area of an OAW-IAP, the client details were retained in the OAW-IAP user-table. **Scenario:** This issue occurred when an OAW-IAP took more time than the configured inactivity timeout value to clear the connected clients. The issue occurred because the timestamp of the client was not updated in some cases.This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2 or later.
79995	**Symptom:** Radio channels could not be configured successfully for a mesh point through the AOS-W Instant UI. **Scenario:** After upgrading to AOS-W Instant 6.2.0.0-3.2.0.2, the users could not configure a radio profile for a mesh point through **Edit Access Point** > **Radio** > **Administrator assigned** > **Channel** in the AOS-W Instant UI. This issue occurred because the channel configuration values were overwritten by transmission power values. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2.0.2.

AirWave

Table 3 *AirWave Fixed Issue*

Bug ID	Description
79775	**Symptom:** Incorrect BSSID information was displayed for the OAW-IAP clients in AirWave. Changes to the BSSID generation process have resolved this issue. **Scenario:** This issue occurred because the Extended SSID was enabled on OAW-IAP. As a result, the BSSID generation algorithm changed and incorrect VLAN and SSID were sent to the Airwave server. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2 or later.

Authentication

Table 4 *Authentication Fixed Issues*

Bug ID	Description
78700	**Symptom:** A system running Windows Vista OS could not obtain an IP address while connecting to a slave OAW-IAP. **Scenario:** This issue was found when the systems running Windows Vista OS tried to connect to slave OAW-IAP on which wpa2-PSK and DHCP was configured. This issue was not specific to any OAW-IAP model or AOS-W Instant release version.
79603	**Symptom:** OAW-IAPs sent empty class attribute in RADIUS accounting packets for some devices. **Scenario:** This issue was observed when an OAW-IAP was turned on, or reconnected after a session timeout. This issue occurred because the OAW-IAPs could not save the user authentication information in PMK cache. This issue was found in both master and slave OAW-IAPs running AOS-W Instant 6.2.0.0-3.2 or later.
80130	**Symptom:** Some clients could not access WLAN when an OAW-IAP used clear encryption. **Scenario:** The issue occurred when a client tried to re-associate to an already associated BSSID. When the OAW-IAP received 802.11 authentication request from a client, the MAC address of which was already present in OAW-IAP client table, the OAW-IAP used clear encryption and then reauthenticated the client. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2 or later.
80475 78437	**Symptom:** A client had to complete RADIUS authentication each time it roamed back to the APs. **Scenario:** This issue occurred when a client was trying to associate to an OAW-IAP with a valid PMKID. The OAW-IAP ignored the PMKID provided by the client, which resulted in full RADIUS authentication. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2.

Datapath

Table 5 *Datapath Fixed Issue*

Bug ID	Description
79880	**Symptom:** When a routing profile entry with destination 0.0.0.0/0 was configured, traffic was forwarded to tunnel, but only for destinations between 128.0.0.0 to 255.255.255.255. **Scenario:** This issue occurred when the routing profile had a 0.0.0.0/0 entry with gateway configured between 128.0.0.0 to 255.255.255.255 and the Source Network Address Translation (Source-NAT) traffic to destinations between 0.0.0.0 to 127.255.255.255 was un-encrypted. This issue was not limited to a specific OAW-IAP model or AOS-W Instant release version.

AOS-W Instant UI

Table 6 *Instant UI Fixed Issues*

Bug ID	Description
80451	**Symptom:** The **Settings** window in the AOS-W Instant UI failed to open when a 3G or 4G modem was used for uplink configuration. **Scenario:** This issue occurred when the AirGroup feature was enabled on an OAW-IAP with 3G uplink configuration. This issue occurred because Process Application Programming Interface (PAPI) could not access the Multicast DNS (MDNS) process. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2.0.1 or later.

Role Derivation

Table 7 *Role Derivation Fixed Issue*

Bug ID	Description
79370	**Symptom:** When roles were assigned using role derivation, client traffic did not go through the tunnel. **Scenario:** This issue occurred when the user roles were assigned only through the 802.1X role derivation. As a result, traffic from clients did not pass through the tunnel. This issue was not limited a specific OAW-IAP model or AOS-W Instant version.

Security

Table 8 *Security Fixed Issues*

Bug ID	Description
64338	**Symptom:** A client could not obtain an IP address when two WEP-encrypted Basic Service Set (BSS) shared the same transmission key index. **Scenario:** The IP address was not assigned to client as the DHCP offer packets could not reach the client. This issue occurred when two WEP-encrypted BSSs shared the same transmission key index, but had different transmission key values configured. As the transmission values created for the latest BSS override others, when a BSS was deleted, the other BSS lost the multicast transmission key and the DHCP offer packets were dropped. This issue is found in OAW-IAPs running AOS-W Instant 6.1.2.3-2.0.0.3 or later.
79798	**Symptom:** Wireless clients could not access sites that start with the word *"instant"* in the URL, such as instantalert.honeywell.com. To resolve this issue, an OEM domain name check for the URLs starting with "*instant*" or "*securelogin*" has been added. **Scenario:** This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2 or later.

SNMP

Table 9 *SNMP Fixed Issue*

Bug ID	Description
77577	**Symptom:** A delay in OAW-IAP response was observed when configuring the engine ID for SNMP operations. **Scenario:** This issue was found in OAW-IAPs monitored by SNMPv3 on Alcatel OmniVista 2500 platform and was not limited to a specific OAW-IAP model or AOS-W Instant release version.

Issues Fixed in 6.2.0.0-3.2.0.2

3G/4G

Table 10 *3G/4G Fixed Issues*

Bug ID	Description
77928	**Symptom:** DNS query failed when UML290 uplink is configured on OAW-IAP **Scenario:** This issue occurred when UML290 uplink was configured on OAW-IAPs that were provisioned to use wired interface and DNS host name for VPN. Due to this, the DNS host names could not be resolved in OAW-IAP as well as Clients. This issue was found in OAW-RAP3WN/WNP and OAW-RAP108/109 provisioned with master switches running AOS-W 6.2.0.0.
78019 78230	**Symptom:** Novatel and Verizon Wireless MC551L 4G USB modems were not supported by OAW-IAPs. **Scenario:** This issue was found on OAW-IAPs running AOS-W Instant 6.2.0.0-3.2. Support for MC551L 4G USB modem is added in AOS-W Instant 6.2.0.0-3.2.0.2 release.

Access Point

Table 11 *Access Point Fixed Issue*

Bug ID	Description
77270 74190	**Symptom**: A high CPU consumption was observed occasionally on the OAW-IAPs. **Scenario**: This issue was found in OAW-IAPs with a higher background or client traffic, where the priority set for copying Wireless Packets for intrusion detection and protection resulted in high CPU utilization. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2. Resetting the priority for copying wireless packets when the throughput is high resolves this issue.

Adaptive Radio Management (ARM)

Table 12 *Adaptive Radio Management Fixed Issues*

Bug ID	Description
77400 78000 78531	**Symptom**: OAW-IAPs were assigned lower power than the Minimum Transmit Power configured by the administrator. **Scenario**: This issue occurred because there was no ESSID configured for the 5GHz radio band. Due to this issue, although a Minimum Transmit Power was configured for ARM, the Mesh AP radios were assigned low power. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2 when ARM is enabled.
78708	**Symptom:** Mesh Portal crashed repeatedly after a reload. **Scenario:** This issue occurred when the Mesh Portal was reloaded with **Wide-Bands All** enabled for the ARM module. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2.0.1.
78533	**Symptom:** A decrease in the antenna range was observed, although a higher antenna gain value was configured for the OAW-IAPs. **Scenario:** Due to this issue, the antenna gain was reset as 5dBi for both 2.4 GHz and 5.0 GHz radio bands, although a 10 dBi gain value was set for the 5.0 GHz band. This issue occurred in OAW-IAPs with detachable antenna, running AOS-W Instant 6.2.0.0-3.2.
78594	**Symptom:** Client association to the OAW-IAPs was delayed after the OAW-IAP boot. **Scenario:** This issue occurred when invalid channels were assigned for AP radios, instead of the channels allowed for a specific regulatory domain. This issue was found in OAW-IAPs running AOS-W Instant6.2.0.0-3.2.

Authentication

Table 13 *Authentication Fixed Issue*

Bug ID	Description
77122	**Symptom:** OAW-IAPs displayed incorrect value for the username on the UI and sent MAC address of client as username during RADIUS authentication. **Scenario:** This issue was found during the authentication of devices running Android 4.0.0 and 2.3.5 versions. This issue occurred due to the coordination failure between authentication and accounting information synchronization processes.

IAP-VPN

Table 14 *IAP-VPN Fixed Issue*

Bug ID	Description
79130	**Symptom:** OAW-IAPs proxied DNS requests from IAP-VPN clients. **Scenario**: This issue occurred on OAW-IAPs with IAP-VPN configuration in a Layer-2 (L2) or Layer-3 (L3) network. This issue was not limited to a specific hardware model or software version. To resolve this issue, the "*" option was added to match every Fully Qualified Domain Name (FQDN), so that the DNS requests are not proxied.

AOS-W Instant UI

Table 15 *AOS-W Instant UI Fixed Issues*

Bug ID	Description
78127 78235	**Symptom:** A blank page was displayed while accessing AOS-W Instant UI. **Scenario**: This issue occurred when the users were trying to access the OAW-IAP GUI and on OAW-IAPs where the administrator login was based on Radius authentication. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2.
78515	**Symptom**: Users were not able to access AOS-W Instant UI through Internet Explorer (IE10). IOAW-IAPs now support IE10 browser. **Scenario**: The users received an **Unsupported Browser** warning message while accessing AOS-W Instant UI from the IE10 browser. This issue occurred because IE10 was not supported by the OAW-IAPs. This issue was not limited to a specific OAW-IAP model or software version.

Mesh Network

Table 16 *Mesh Network Fixed Issues*

Bug ID	Description
77809	**Symptom:** Mesh Points were not able to establish connection with the Mesh Portal. **Scenario**: This issue occurred after clearing the configuration details from the Mesh Portal Maintenance GUI. This issue occurred because there was no ESSID configured for the 5.0 GHz band. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2 or later.

Table 16 *Mesh Network Fixed Issues (Continued)*

Bug ID	Description
77815	**Symptom**: In Mesh topology, a mesh point with Ethernet Bridging enabled came up as a Mesh portal. **Scenario**: This issue occurred when Ethernet bridging was enabled on Mesh Point and after clearing configuration details in the Virtual Controller (VC) GUI. This issue occurred because the Ethernet bridging information was lost, after the configuration was cleared from the VC GUI. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2 and was not limited to a specific hardware platform.
77817	**Symptom**: Mesh Points were lost after clearing configuring details from the Mesh Portal Maintenance GUI. **Scenario**: This issue occurred because the VC key details were removed after the configuration was cleared from the Mesh Portal Maintenance GUI. Due to this, Mesh Points could not connect to the Mesh Portal after the reboot. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2 and was not limited to a specific hardware platform.
77951	**Symptom:** A mesh point was not shown in the list of APs on executing the **`show aps`** command, but was able to connect and broadcast ESSIDs. **Scenario**: This issue occurred because the Mesh Portal could not send master beacon to the Mesh Point. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2 and was not limited to a specific hardware platform.

Issues Fixed in 6.2.0.0-3.2.0.1

Access Point

Table 17 *Access Point Fixed Issues*

Bug ID	Description
76370	**Symptom:** OAW-IAPs lost configuration data and SSID. **Scenario**: This issue was found in OAW-AP134 and OAW-AP135 running AOS-W Instant version 6.1.3.4-3.1.0.0 or later. This issue occurred because OAW-IAPs could not read data from the flash memory.
76739	**Symptom:** OAW-IAPs crash and reboot intermittently. **Scenario**: This issue was found in OAW-IAPs running AOS-W Instant version 6.1.2.3-2.0.0.3. The issue was resolved when the OAW-IAPs were upgraded to AOS-W Instant version 6.1.3.4-3.1.0.1 or later.
77489	**Symptom:** Mesh Points could not establish link to the Mesh portal when the AOS-W Instant version of Mesh Portal was different from the version running on Mesh Points. **Scenario**: This issue was found in Mesh network, which consisted of a master OAW-IAP running AOS-W Instant version 6.2.0.0-3.2 and a slave Mesh Point running AOS-W Instant version 6.1.3.4-3.1.0.1.

AirGroup

Table 18 *AirGroup Fixed Issues*

Bug ID	Description
76911	**Symptom:** AirGroup server discovery failed to work consistently in Mesh topology. **Scenario:** This issue was found in OAW-IAPs running AOS-W Instant version 6.2.0.0-3.2. This issue occurred when the AirGroup feature was enabled for the OAW-IAPs configured in Mesh topology.

Authentication

Table 19 *Authentication Fixed Issues*

Bug ID	Description
76700	**Symptom:** The client authentication failed when Captive portal was used on a VLAN with **Local** (NAT) DHCP server configuration. **Scenario:** This issue occurred because an incorrect pre-authenticated role was configured for the client. This issue was not specific to any OAW-IAP or AOS-W Instant version.
77122	**Symptom:** OAW-IAPs displayed incorrect value for the username on the UI and sent MAC address of client as username during RADIUS authentication. **Scenario:** This issue was found during the authentication of devices running Android 4.0.0 and 2.3.5 versions. This issue occurred due to the coordination failure between authentication and accounting information synchronization processes.
77133	**Symptom:** Reauth interval for an existing SSID could not be modified. **Scenario:** This issue was found in OAW-IAPs running AOS-W Instant version 6.2.0.0-3.2. This issue occurred because the configuration changes to an existing SSID were not saved in OAW-IAP memory.
77136	**Symptom:** The Captive portal page populated incomplete information during Captive portal authentication of guest users. **Scenario:** This issue was found in OAW-IAPs running AOS-W Instant version 6.1.3.4-3.1.0.0 or later. This issue occurred because Fully Qualified Domain Name (FQDN) was used for HTTP redirection.
77292	**Symptom:** The internal server could not be configured as authentication server when the auth survivability feature was disabled. **Scenario:** This issue was found in OAW-IAPs running AOS-W Instant version 6.2.0.0-3.2. This issue occurred because the internal server configuration changes were not saved in OAW-IAP memory.
77345	**Symptom:** A client running Mac OS could not be authenticated by using the internal server when the authentication survivability feature was enabled. **Scenario:** This issue was found OAW-IAPs running AOS-W Instant version 6.2.0.0-3.2. This issue occurred because the Generic Token Card (GTC) authentication protocol used by the Mac client was not supported by the authentication survivability feature.

Chapter 5

Known Issues in Previous Releases

This chapter provides a list of the known issues and limitations identified in the previous release of AOS-W Instant.

Authentication

Table 1 *Authentication Known Issue*

Bug ID	Description
75822	**Symptom:** The **Idle-Timeout** value returned by the RADIUS server does not take effect. **Scenario:** This issue occurs when a RADIUS server is used for authentication and the **Idle-Timeout** value is configured on this RADIUS server. **Workaround:** Configure a low **Inactivity-Timeout** value on the OAW-IAP.

Mesh Network

Table 2 *Mesh Network Known Issue*

Bug ID	Description
79171	**Symptom:** Mesh Points are not shown in the list of APs, after clearing configuration from the Mesh Portal Maintenance GUI. **Scenario:** This issue occurred in OAW-IAPs shipped as OAW-IAP-ROW (Rest of World) variant, running AOS-W Instant 6.2.0.0-3.2. **Workaround:** Reboot the Mesh Portal after selecting the country code.

Mobility

Table 3 *Mobility Known Issue*

Bug ID	Description
74309	**Symptom:** After modifying a distributed Layer-3 subnet to use a new value, the old subnet is not deleted. **Scenario:** This issue occurs when a distributed L3 subnet is modified in the OAW-IAP. This issue is found in OAW-IAPs running AOS-W Instant version 6.2.0.0-3.2 in the distributed L3 network topology. **Workaround:** As both subnet routes point to the same internal IP address, no workaround is required.

Security

Table 4 *Security Known Issue*

Bug ID	Description
64338	**Symptom:** The DHCP offer packets are dropped and do not reach the client, preventing the client from being assigned an IP address. **Scenario:** When multiple WEP-encrypted BSS share the same Tx key ID and have different Tx key values configured, the latest BSS created overrides the others. If any of these BSS are deleted, all other BSS lose the multicast TX key and this results in DHCP offer packets getting dropped. This issue is found in OAW-IAPs running AOS-W Instant 6.1.2.3-2.0.0.3. **Workaround:** Use different Tx key IDs for different BSS.

VPN Configuration

Table 5 *VPN Configuration Known Issues*

Bug ID	Description
72166	**Symptom:** The clients in the VPN NAT mode cannot ping large packets—2000, 5000, and 10000 bytes, to the corporate IP address. However, the clients in DL3 mode can ping large packets. **Scenario:** This issue is not specific to any AOS-W Instant release version. **Workaround:** None.
76564	**Symptom:** The Generic Routing Encapsulation (GRE) tunnel does not come up after swapping the master and slave OAW-IAPs. **Scenario:** This issue is found in OAW-AP105 running AOS-W Instant version 6.2.0.0-3.2. This issue occurs when the Per-AP tunnel is configured in an OAW-IAP cluster and the tunnel is disabled from slave, followed by the swapping of master and slave OAW-IAPs. **Workaround:** Reconfigure the tunnel in the new master and then reboot the master.