AOS-W Instant 6.4.4.4-4.2.3.2

Release Notes

AOS-W Instant 6.4.4.4-4.2.3.2 is a patch release that introduces enhancements and fixes to the issues found in the previous release.

For information on upgrading OAW-IAPs to the new release version, refer to the *Upgrading an OAW-IAP* topic in the *AOS-W Instant 6.4.4.4-4.2.3.0 User Guide.*

Contents

Contacting Support

Table 1: *Contact Information*

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

This chapter lists the regulatory information applicable to the AOS-W Instant 6.4.4.4-4.2.3.2 release.

Regulatory Domain Updates

The following table lists the DRT file versions supported by Instant 6.4.4.x-4.2.3.x releases:

Table 2: *DRT Versions*

Instant Release Version	Applicable DRT Version
6.4.4.4-4.2.3.2	1.0_54870
6.4.4.4-4.2.3.1	1.0_54367
6.4.4.4-4.2.3.0	1.0_54079

For a complete list of countries certified with different AP models, see the respective DRT release notes at service.esd.alcatel-lucent.com.

Resolved Issues in this Release

There are no issues fixed in the Instant 6.4.4.4-4.2.3.2 release.

This chapter includes the Known Issues and Limitations identified in the Instant 6.4.4.x-4.2.3.x releases:

Known Issue

The following known issue was identified in the Instant 6.4.4.4-4.2.3.0 release:

AppRF

Table 3: *AppRF Known Issue*

Bug ID	Description
120228	**Symptom**: The Skype application is not getting blocked when the App enforcement ACL is configured. **Scenario**: This issue occurs with OAW-IAPs that support the App enforcement feature, and is observed in all the OAW-IAPs running Instant 6.4.3.1-4.2.0.0 or later versions. **Workaround**: None.

Limitation

The following limitation is identified in the Instant 6.4.4.4-4.2.3.1 release:

No Support for Layer 2 Tunneling Protocol Version 3 (L2TPV3) on Certain Access Points

Starting from Instant 6.4.4.4-4.2.3.1, the L2TPV3 protocol is not supported on certain access points with 16 MB flash memory, such as OAW-IAP104/105, OAW-IAP175P/175AC, and OAW-IAP134/135.

This chapter describes the features and enhancements introduced in the previous AOS-W Instant 6.4.4.x-4.2.3.x releases.

Features and Enhancements

This section describes the features and enhancements introduced in Instant 6.4.4.4-4.2.3.0 release.

802.1X Supplicant Configuration Support for Wired Networks

In Instant 6.4.4.4-4.2.3.0, you can provision an OAW-IAPs as an 802.1X supplicant for networks where all wired devices are required to authenticate using PEAP or TLS protocol. If the ports, to which the OAW-IAPs are connected, are configured to use the 802.1X authentication method, ensure that you configure the OAW-IAPs to function as an 802.1X client or supplicant and configure the 802.1X authentication type on the uplink ports on the OAW-IAP.

To enable the 802.1X supplicant support, ensure that the 802.1X authentication parameters are configured on all OAW-IAPs in the cluster.

The 802.1X supplicant feature is not supported with mesh and Wi-Fi uplink.

This feature is also not supported on OAW-IAP104/105, OAW-IAP175P/175AC, OAW-RAP3WN, and OAW-IAP134/135.

For more information, see:

- *Enabling 802.1X Supplicant Support* in the *AOS-W Instant 6.4.4.4-4.2.3.0 User Guide*.
- The **ap1x**, **ap1x-peap-user**, **show ap1x**, **show ap1x**, **show ap1xcert** commands in the *AOS-W Instant 6.4.4.4-4.2.3.0 CLI Reference Guide.*

BLE Beacon Management

In Instant 6.4.4.4-4.2.3.0, OAW-IAPs support Alcatel-Lucent Bluetooth Low Energy (BLE) devices, such as BT-100 and BT-105, which are used for location tracking and proximity detection. The BLE devices connected to an OAW-IAP can be monitored or managed by a cloud based Beacon Management Console (BMC). The BLE beacon management feature allows you to configure parameters for managing the BLE beacons and establishing secure communication with the Beacon Management Console (BMC). You can also configure the BLE operation modes that determine the functions of the built-in BLE chip in the OAW-IAP.

The BLE beacon management and BLE operation mode feature is supported only on OAW-IAP324/325, OAW-IAP21x/215, and OAW-IAP224/225 devices.

For more information, see:

- *Managing BLE Beacons* in the *AOS-W Instant 6.4.4.4-4.2.3.0 User Guide*
- The ble config and show ble-config commands in the *AOS-W Instant 6.4.4.4-4.2.3.0 CLI Reference Guide.*

Out of Service Operations

In Instant 6.4.4.4-4.2.3.0, you can enable or disable an SSID when the VPN, uplink, primary uplink, or Internet connection is down. You can configure an SSID profile to enable or disable the SSID when an out-of-service state is detected on the OAW-IAP. For example, if you select the VPN down option from the drop-down list and set the status to enabled, the SSID is enabled when the VPN connection is down and is disabled when the VPN connection is restored.

If you select the Internet-down to enable or disable the SSID based on Internet availabilty, you can configure the IP address to which the master OAW-IAP can send the ICMP packets to verify if the Internet is reachable. By default, the master OAW-IAP sends ICMP packets to the 8.8.8.8 IP address.

For more information, see:

- *Configuring WLAN Settings for an SSID Profile* and *Switching Uplinks Based on VPN and Internet Availability* in *AOS-W Instant 6.4.4.4-4.2.3.0 User Guide*
- The **wlan ssid-profile** and **uplink** commands in the *AOS-W Instant 6.4.4.4-4.2.3.0 CLI Reference Guide*.

Dynamic DNS Registration Support

Starting from Instant 6.4.4.4-4.2.3.0, support for dynamically updating DNS records of the OAW-IAP and its clients on to the DNS server has been included. You can also configure dynamic dns when creating Distributed, L3 DHCP scopes and send DNS updates periodically to the DNS server.

For more information, see:

- *Dynamic DNS Registration* in *AOS-W Instant 6.4.4.4-4.2.3.0 User Guide*.
- **dynamic-dns-ap**, **dynamic-dns-interval**, **dynamic-dns**, **show ddns**, **ip dhcp** commands in the *AOS-W Instant 6.4.4.4-4.2.3.0 CLI Reference Guide*.

This feature is not supported on OAW-IAP104/105, OAW-IAP175P/175AC, OAW-RAP3WN, and OAW-IAP134/135.

Support for Client Match Feature on OAW-IAP324/325 platforms

Starting from Instant 6.4.4.4-4.2.3.0, client match is supported on the OAW-IAP324/325 platforms.

Configure-Only Mode in AMP

The latest version of OmniVista includes a new option which sets the OAW-IAP in the config-only mode. OAW-IAP will receive the firmware upgrades and configurations, but will not send any statistics for monitoring.

For more information, see:

- *OAW-IAP and Client Monitoring* in *AOS-W Instant 6.4.4.4-4.2.3.0 User Guide.*

Support for Full URL Visibility and AppRF Enhancements

- Instant now supports the extraction of full URL from the http or https sessions and periodically logs them on the ALE server.
- Instant 6.4.4.4-4.2.3.0 also supports displaying the list of blocked and allowed DPI and Web Content URLs and session count.
- The application DPI and Web Content graphs can now be viewed individually.

For more information, see:

- *Deep Packet Inspection and Application Visibility* in *AOS-W Instant 6.4.4.4-4.2.3.0 User Guide.*

- **url-visibility**, **show url-visibility**, and **show dpi-stats** in the *AOS-W Instant 6.4.4.4-4.2.3.0 CLI Reference Guide*.

Static LACP Configuration Support

Starting from Instant 6.4.4.4-4.2.3.0, new options are introduced to support the static LACP feature. You can enable, disable, and remove the static LACP configuration on the OAW-IAP.

Sometimes, the LACP functionalities vary depending on the switches being used. This feature gets the entire static LACP mode work as expected.

The static LACP mode is supported on OAW-IAP225, OAW-IAP325, and OAW-IAP275 access points.

For more information, see:

- *Wired Profiles* in the *AOS-W Instant 6.4.4.4-4.2.3.0 User Guide*.
- **lacp-mode** and **show ap-env** commands in the *AOS-W Instant 6.4.4.4-4.2.3.0 CLI Reference Guide*.

Per-AP SSID and VLAN

Starting from Instant 6.4.4.4-4.2.3.0, you can set the environment variables on a wireless profile. You can also configure the **per-ap-ssid** and **per-ap-vlan** settings for **SSID** and **VLAN** profiles respectively.

For more information, see:

- *Wireless Network Profiles* in the *AOS-W Instant 6.4.4.4-4.2.3.0 User Guide*.
- **per-ap-ssid** and **per-ap-vlan** commands on *AOS-W Instant 6.4.4.4-4.2.3.0 CLI Reference Guide*.

New Wired-Containment Knobs for NAT Rogue

Starting from Instant 6.4.4.4-4.2.3.0, the wired-containment knobs can enable the protection of the wired-containment for NAT rogue.

This feature can also identify and contain an OAW-IAP with a preset wired MAC address that is different from the BSSID of the OAW-IAP if the MAC address that the OAW-IAP provides to wireless clients as the gateway MAC is balanced by one character from its wired MAC address.

Enable this feature only when a specific containment is needed, in order to avoid a false alarm.

For more information, see:

- *Intrusion Detection* in the *AOS-W Instant 6.4.4.4-4.2.3.0 User Guide*.
- **ids** command in the *AOS-W Instant 6.4.4.4-4.2.3.0 CLI Reference Guide*.

Configuring Maximum Clients for Radio Profiles

Starting from Instant 6.4.4.4-4.2.3.0, a new per-ap setting has been included to adjust the maximum number of clients that can connect to 2.4 GHz and 5 GHz radio profiles. This option can be configured only via the Instant CLI.

For more information, see:

- **a-max-clients** and **g-max-clients** command pages in the *AOS-W Instant 6.4.4.4-4.2.3.0 CLI Reference Guide.*

Configuring a Custom Port for Speed Test Profiles

Instant 6.4.4.4-4.2.3.0 release now allows you to configure a custom server port as part of the speed test profile configuration.

For more information, see:

- Uplink Bandwidth Monitoring in *AOS-W Instant 6.4.4.4-4.2.3.0 User Guide*.
- **speed-test** command page in the *AOS-W Instant 6.4.4.4-4.2.2.3.0 CLI Reference Guide.*

This chapter describes the issues fixed in previous AOS-W Instant 6.4.4.x-4.2.3.x releases.

Issues Resolved in 6.4.4.4-4.2.3.1

The following issues are fixed in the Instant 6.4.4.4-4.2.3.1 release:

Authentication

Table 4: *Authentication Fixed Issue*

Bug ID	Description
136240	**Symptom**: Accounting packets were being sent to the Radius server even after the Radius server was down due to an authentication timeout. The issue is resolved by unifying the authentication and accounting status of servers. **Scenario**: This issue was observed in all OAW-IAPs running Instant 6.4.2.0-4.1.1.0 and later versions.

Captive Portal

Table 5: *Captive Portal Fixed Issue*

Bug ID	Description
133642	**Symptom**: Clients connected to an OAW-IAP were unable to access Captive Portal. This issue is resolved by performing a check to ensure that the data in the socket is valid. **Scenario**: This issue occurred when the clients connected to an OAW-IAP did not receive a response from the HTTP server, since Tinyproxy was blocked. This issue was not limited to a specific OAW-IAP model or software version.

Datapath/Firewall

Table 6: *Datapath/Firewall Fixed Issues*

Bug ID	Description
138430	**Symptom**: Clients on an uplink of standalone OAW-IAPs using the VPN gateway functionality were unable to connect to the resources behind the VPN tunnel. The fix ensures that clients can connect to resources behind the VPN tunnel using the OAW-IAP as the VPN gateway. **Scenario**: This issue was observed in all OAW-IAPs running Instant 6.4.4.4-4.2.3.0 version.

Wi-Fi driver

Table 7: *Wi-Fi driver Fixed Issue*

Bug ID	Description
137910	**Symptom**: The interval segment of a Beacon frame was zero on an SSID configuration of an OAW-IAP. The fix ensures that the value of the interval segment of the Beacon frame is displayed in correct sequence. **Scenario**: This issue was observed in OAW-IAP325 devices running Instant 6.4.4.4-4.2.3.0 version.

Issues Resolved in 6.4.4.4-4.2.3.0

The following issues are fixed in the Instant 6.4.4.4-4.2.3.0 release:

ARM

Table 8: *ARM Fixed Issue*

Bug ID	Description
134305	**Symptom**: An OAW-IAP205 access point crashed with a fatal exception due to kernel panic. The fix ensures that the OAW-IAP does not crash when the wide channel band is disabled. **Scenario**: This issue occurred when the 80 MHz support is enabled and wide channel band is disabled in the ARM configuration. This issue was observed in OAW-IAP205 access points running Instant 6.4.3.4-4.2.1.2 release and later versions.

Authentication

Table 9: *Authentication Fixed Issue*

Bug ID	Description
131941	**Symptom**: Client devices operating on IOS 9 software or a higher version, were unable to get an IP address from the assigned VLAN when termination was enabled on the OAW-IAP and a VLAN derivation rule was configured. The fix ensures that the client devices receive an IP address from the assigned VLAN. **Scenario**: This issue was observed in all OAW-IAPs running Instant 6.4.3.4-4.2.1.0 release and later versions.

Captive Portal

Table 10: *Captive Portal Fixed Issue*

Bug ID	Description
135837	**Symptom**: OAW-IAP205 access points were generating Tinyproxy error messages when the clients were connecting to a guest SSID using Captive Portal. This issue is resolved by changing the debugging level of the logs. **Scenario**: This issue occurred due to the high volume of error logs generated and was observed in OAW-IAP205 access points running Instant 6.4.3.4-4.2.1.0 release and later versions.

Datapath/Firewall

Table 11: *Datapath/Firewall Fixed Issues*

Bug ID	Description
122754	**Symptom**: The **disconnect-user** command failed to clear all the user details from the Virtual Controller or OAW-IAP. As a result, a new client was unable to re-use the same IP address. The fix ensures that the previous user details are cleared and the new client is able to re-use the same IP address. **Scenario**: The L3 user entry was not cleared when the **disconnect-user** command was executed. This issue was observed in all OAW-IAPs running Instant 6.4.3.1-4.2.0.0 release and later versions.
130729	**Symptom**: PXE clients connected to the wired port of an OAW-IAP were not getting an IP address. This issue is resovled by making a change in the code. **Scenario**: This issue was observed in clients with a Bcast bit set and was not limited to a specific OAW-IAP model or software version.
132867	**Symptom**: Wireless clients were unable to ping to the OAW-IAP when the uplink-vlan tag and the ssid vlan were configured with the same values. This issue is resolved by making a change in the OAW-IAP code. **Scenario**: This issue was not limited to a specific OAW-IAP model or software version.

DHCP Server

Table 12: *DHCP Server Fixed Issues*

Bug ID	Description
131394	**Symptom**: The Option 82 relay information was not excluded from the DHCP OFFER and ACK packets before they were sent to the client. The fix ensures that the Option 82 relay information is removed from the DHCP OFFER and ACK packets. **Scenario**: This issue occurred when the Option 82 relay information was enabled on the OAW-IAP L2 Centralized Local DHCP server and was observed in all OAW-IAPs running Instant 6.4.3.4-4.2.1.0 release.
131944	**Symptom**: DNS server settings were not displayed on the guest VLAN when the OAW-IAP was rebooted. This issue is resolved by making a change in the OAW-IAP code. **Scenario**: The **dnsip** setting was configured manually and different from the OAW-IAPs own DNS setting. This issue was observed in all OAW-IAPs running running Instant 6.4.3.4-4.2.1.0 release and later versions.

OAW-IAP Platform

Table 13: *OAW-IAP Platform Fixed Issue*

Bug ID	Description
128188	**Symptom**: OAW-IAP205 access points crashed and rebooted reporting that the memory space was full. This issue is resolved by making a change in the OAW-IAP code. **Scenario**: This issue was observed in OAW-IAP205 access points running Instant 6.4.3.4-4.2.1.0 release and later versions.

Mesh

Table 14: *Mesh Fixed Issue*

Bug ID	Description
125922	**Symptom**: Third party switches connected to the Mesh Portal were generating inconsistent VLAN messages, when the mesh point was rebooted. The fix ensures that the mesh point does not receive any untagged PVST+ packets that were causing this issue. **Scenario**: The mesh point was receiving untagged PVST+ packets amidst the tagged PVST+ packets resulting in the third party switch generating inconsistent VLAN messages. This issue was observed in all OAW-IAPs running Instant 6.4.4.4-4.2.3.0 release and earlier versions.

STM

Table 15: *STM Fixed Issue*

Bug ID	Description
131706	**Symptom**: OAW-IAP clients were unable to get an IP address from the assigned VLAN, when a VLAN derivation rule was configured. The fix ensures that the OAW-IAP clients receive an IP address from the assigned VLAN. **Scenario**: This issue occurred when the attributes were configured based on the AP-Name and AP-Group and was observed in all OAW-IAPs running Instant 6.4.3.1-4.2.0.0 release and later versions.

3G/4G Management

Table 16: *3G/4G Management Fixed Issue*

Bug ID	Description
126248	**Symptom**: OAW-IAP devices were taking about 50 minutes to failover to the Cellular uplink when the Ethernet uplink went down. This issue is resolved by making a change in the OAW-IAP code. **Scenario**: This issue was observed in all OAW-IAPs running Instant 6.4.3.1-4.2.0.0 release and later versions.