AOS-W Instant 6.4.2.3-4.1.1.2

Release Notes

Contents

AOS-W Instant 6.4.2.3-4.1.1.2 is a patch release that introduces feature enhancements and fixes to the issues found in the previous releases.

For more information on upgrading OAW-IAPs to the new release version, see the *Upgrading an OAW-IAP* topic in *AOS-W Instant 6.4.2.0-4.1.1 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 provides information on the enhancements and the issues resolved in this release of AOS-W Instant.

Features and Enhancements

The following enhancements are introduced in the 6.4.2.3-4.1.1.2 release.

Support for Proxy-based Servers for AirGroup Clients

Starting from the 6.4.2.3-4.1.1.2 release, OAW-IAPs support proxy based servers such as Printopia or PaperCut. With this enhancement, AirGroup can discover services that are advertised by the proxy servers.

Enhancements to AppRF Data for OAW-IAPs Managed by OmniVista

The OmniVista managed OAW-IAPs can now send the destination details in the AppRF data to the AMP. Ensure that you use OmniVista 8.0.6.1 with the OAW-IAPs running 6.4.2.3-4.1.1.2 to view the historical statistics of an OmniVista managed OAW-IAP. However, the OmniVista 8.0.6.1 version does not display the web category and web-reputation data sent from an OAW-IAP.

Security Update

In the 6.4.2.3-4.1.1.2 release, a potential crash in a management process is fixed.

Enhancements to EAP Request Retry Time

In the 6.4.2.3-4.1.1.2 release, the EAP retry time is reduced from 30 seconds to 5 seconds. With this enhancement, if the OAW-IAP does not receive an EAP-response from the client within 5 seconds, it resends the EAP-request, to ensure that the 802.11X client authentication is not delayed.

Resolved Issues in This Release

The following issues are fixed in the 6.4.2.3-4.1.1.2 release.

AP Platform

Table 2: *Access Point Fixed Issues*

Bug ID	Description
108725	**Symptom**: A higher CPU utilization was observed in some OAW-IAP models when the captive portal clients continuously sent more than 12 HTTPS requests per second. This issue is resolved by making a change in the code to throttle HTTPS requests. **Scenario**: This issue occurred when the guest clients sent more number of HTTPS requests. This issue was observed in OAW-IAP93, OAW-IAP105, and OAW-IAP175P/175AC devices running 6.3.1.1-4.0 or later versions.
104947	**Symptom**: A OAW-RAP109 was unable to send or receive data packets through the Ethernet0 port. The fix ensures that the OAW-IAP reboots when it stops sending or receiving packets through Ethernet0 port for about six minutes. **Scenario**: This issue was not limited to a specific OAW-IAP model or software release version.
110994	**Symptom**: An OAW-IAP225 device crashed and rebooted. A change in the internal OAW-IAP code has resolved this issue. **Scenario**: This issue was found in an OAW-IAP cluster with OAW-IAP225 and OAW-IAP275 devices running 6.4.2.0-4.1.1 release.
111019	**Symptom**: The client Idle time in the **show ap debug client-table ap-name** command output was not reset when APs received null data packets. This issue is resolved by updating an internal module. **Scenario**: This issue occurred when Station Control Block (SCB) was not updated with the time stamp on receiving any packet from the client. This issue was found in OAW-IAP224/225 devices running 6.4.2.0-4.1.1.1 or later.
111418	**Symptom**: The OAW-IAP104/105 devices were unable to send packets when the link speed was 10 Mbps or half of it. This issue is resolved by making a change in the OAW-IAP code. **Scenario**: This issue was observed in OAW-IAP104/105 running 6.4.2.0-4.1.1.1 and earlier release versions.

OmniVista

Table 3: *OmniVista Fixed Issue*

Bug ID	Description
109732	**Symptom**: A OAW-RAP3WN managed by OmniVista went back to partial factory default setting. To resolve this issue, log out of the OmniVista session and then log in again. **Scenario**: This issue occurred when OmniVista propagated the configuration template while provisioning an OAW-IAP. This issue was observed in all OAW-IAPs running 6.4.2.0-4.1.1.1 or earlier versions.

AirGroup

Table 4: *AirGroup Fixed Issues*

Bug ID	Description
108666	**Symptom**: AirGroup servers with uppercase letters in the service ID were not displayed in the output for the **show airgroup servers** command. This issue is resolved by making the entry for the service ID as case-sensitive. **Scenario**: This issue occurred when the service ID for the AirGroup server contained both lowercase and uppercase letters. This issue was not limited to a specific OAW-IAP model or Instant release version.
107215	**Symptom**: OAW-IAPs were unable to handle the records of service IDs that were case-sensitive and hence failed to respond to the client queries. This issue is resolved by making a change in the OAW-IAP code. **Scenario**: This issue occurred when the OAW-IAPs misinterpreted the information stored in the cache by the server advertising the service ID with case-sensitive values. This issue was not limited to a specific OAW-IAP model and was found in OAW-IAPs running 6.3.1.1-4.0.0.0 release or later versions.

ARM

Table 5: *ARM Fixed Issues*

Bug ID	Description
109601	**Symptom**: The OAW-IAP UI and CLI displayed incorrect values for transmission power when the OAW-IAPs were operating in certain DFS channels such as 116. The fix ensures that the OAW-IAP UI and CLI display the correct values for transmission power when operating in DFS channels. **Scenario**: This issue occurred when the OAW-IAPs were operating in DFS channel such as 116 in the US regulatory domain and was observed in the OAW-IAP135 and OAW-IAP105 devices running 6.4.2.0-4.1.1 release.
110143	**Symptom**: An OAW-IAP crashed during a client match operation for the clients connected to an 802.11v (BSS transition management) enabled WLAN SSID. A change in the internal OAW-IAP code has resolved this issue. **Scenario**: This issue was found in the OAW-IAP103 devices running 6.4.0.2-4.1 or later release versions when the client match operation was performed on the 802.11v clients.
110407	**Symptom**: Some wireless clients could not connect to an SSID on which 802.11r (fast roaming) was enabled. This issue is resolved by using a SSID specific variable to check SSID 802.11r configuration on a driver. **Scenario**: The issue occurred when two SSIDs were configured on the IAP, one with 802.11r enabled and the other with 802.11r disabled. This issue was found in OAW-IAPs running 6.4.2.0-4.1.1.1 release version.

Authentication

Table 6: *Authentication Fixed Issues*

Bug ID	Description
108831	**Symptom**: When the client was connected to a dynamic WEP SSID and roamed to a new AP in the cluster, the username in the accounting start packet was its MAC address instead of the client's real username. This issue is resolved by ensuring that the cached username is used or the accounting is delayed until the 802.1X authentication is completed by client. **Scenario**: This issue occurred when the dynamic WEP authentication was configured on the SSID with accounting enabled. This issue was not limited to a specific OAW-IAP model or software version.
110935	**Symptom**: The virtual controller sent the accounting packet with an old class ID for the reconnecting clients. The OAW-IAPs now send the accounting packets with appropriate class IDs, after a successful client authentication. **Scenario**: This issue was not limited to any specific OAW-IAP platform or release version.

CLI

Table 7: *CLI Fixed Issues*

Bug ID	Description
109165	**Symptom**: The OAW-IAP CLI was running in a degraded state and was stuck in a wait state, although the sub-processes were completed. A change in the CLI module has resolved this issue. **Scenario**: This issue occurred when the CLI process was left idle for a long time and was found in OAW-IAPs running 6.4.2.0-4.1.1 or later versions.

Datapath

Table 8: *Datapath Fixed Issues*

Bug ID	Description
108579	**Symptom**: Although the bandwidth contract values were modified for an SSID, the clients connecting to the SSID were not assigned the modified values. The updated contract values can now be applied to the traffic generated by the client. **Scenario**: This issue occurred when the client associated to an SSID that was modified to use new bandwidth contract values and was not limited to a specific OAW-IAP platform or software version.
109428	**Symptom**: The clients connected to a slave OAW-IAP could not access the Internet when the **Deny inter user bridging** feature was enabled. To resolve this issue, a change in the code was introduced to handle ARP response packets from the slave OAW-IAP to other IP addresses in VLAN subnet. **Scenario**: This issue occurred when the guest VLAN was configured on the SSID and **Deny inter user bridging** was set to enabled. This issue was found in OAW-IAPs running 6.4.2.0-4.1.1 release version.
110454	**Symptom**: When a 0.0.0.0 route was configured in a routing profile, the OAW-IAP performed source NAT for the Multicast DNS (MDNS) or Digital Living Network Alliance (DLNA) queries to the VPN clients and they did not work. To resolve this issue, an explicit permit rule was added in the ACL rules to allow these queries without source NAT. **Scenario**: This issue occurred when a 0.0.0.0 route was configured in a routing profile for the centralized L2 client and the **Split-tunnel** option was enabled for the centralized L2 DHCP profile. This issue was found this OAW-IAPs running 6.4.2.0-4.1.1 release version.

Bug ID	Description
110949	**Symptom**: The slave OAW-IAPs could not be reached from the network. A change in the uplink VLAN settings has resolved this issue. **Scenario**: This issue was found in OAW-IAPs running 6.4.2.0-4.1.1 release version when the **enet-vlan** configuration setting was not applied for the uplink VLAN on the slave OAW-IAP.

IAP-VPN

Table 9: *IAP-VPN Fixed Issue*

Bug ID	Description
108770	**Symptom**: In a Master-Local topology, although the automatic GRE tunnel configuration was enabled on the OAW-IAP, the GRE tunnel to the switch was deleted after a master OAW-IAP failover. A change in the OAW-IAP management module of switch has resolved this issue. **Scenario**: This issue occurred when a master OAW-IAP tried to connect to the switch with the same Virtual Controller key and a different inner IP address after a failover. Due to this, when the OAW-IAP tried to establish a VPN tunnel with the local switch, the GRE tunnel to the switch was deleted. This issue was observed in OAW-IAPs running 6.4.2.0-4.1.1 and switchs running 6.4.2.2 releases.

SNMP

Table 10: *SNMP Fixed Issues*

Bug ID	Description
107701	**Symptom**: The OAW-IAP sent incomplete information in the SNMP trap when a RADIUS client failed to authenticate. A change in the code has resolved this issue. **Scenario**: This issue occurred when the OAW-IAP sent only two parameters in the SNMP trap for the RADIUS client authentication failure and was found in OAW-IAPs running 6.4.0.2-4.1.0.0 or later versions.
110622	**Symptom**: OAW-IAPs did not send any traps when a rogue AP was removed from the network. The fix in this release ensures that the **wlsxUnsecureAPResolved** trap is sent when a rogue AP is removed from the network by the AM module. **Scenario**: This issue was observed in OAW-IAPs running 6.4.2.0-4.1.1.1 or earlier versions.

STM

Table 11: *STM Fixed Issues*

Bug ID	Description
104639	**Symptom**: Wireless clients unexpectedly failed to connnect to the 802.11r enabled WLAN SSID. Changes in the station management module ensure that the clients roam seamlessly in an 802.11r enabled WLAN. **Scenario**: This issue was observed when an 802.11r-capable wireless client roamed from one AP to another. This issue was not limited to any specific OAW-IAP platform.
109429	**Symptom**: The Change of Authorization (CoA) requests were acknowledged by the master OAW-IAP, although the RADIUS server sent the Change of Authorization (CoA) requests to the slave OAW-IAP. A change in the OAW-IAP code has resolved this issue. **Scenario**: This issue occurred when a client was connected to the slave OAW-IAP and the CoA requests were sent to the slave OAW-IAP by the RADIUS server. As the requests were acknowledged by the master OAW-IAP, the RADIUS server could not process these messages and kept sending CoA requests to the slave OAW-IAP. This issue was found in OAW-IAPs running 6.3.1.1-4.0 release or later versions.

Uplink Configuration

Table 12: *Uplink Configuration Fixed Issues*

Bug ID	Description
108830	**Symptom**: When the PPPoE uplink connection was enabled, web pages were partially displayed. Changes in the IAP data path were made to ensure that the packets sent by the server do not exceed the value configured for MTU. **Scenario**: This issue occurred when the Maximum Transmission Unit (MTU) set by the server was more than the MTU allowed for the PPPoE uplink. This issue was found in OAW-IAPs running 6.4.2.0-4.1.1 release or earlier versions.
108538	**Symptom**: When an OmniVista managed OAW-IAP was quickly unplugged from the cluster, after the OmniVista server applied the PPPOE configuration and the OAW-IAP configuration was restored to initial configuration, the PPPoE uplink connection could not be established on the OAW-IAP. To resolve this issue, OAW-IAPs now send the **Configuration is successfully synchronized from management server** message to the management server after a configuration check. Due to this change, the administrators must verify the configuration synchronization event on OmniVista, before unplugging or powering off the OAW-IAP. **Scenario**: This issue occurred when the OAW-IAP was unplugged, before the PPPoE configuration details were completely synchronized with the AMP management server. As a result, if the OAW-IAP failed to establish connection with the OmniVista server after a reboot, the OAW-IAP configuration including the PPPoE configuration applied from the OmniVista server was lost. This issue was observed in OAW-IAPs running 6.3.1.1-4.0 or earlier versions.

User Interface

Table 13: *User Interface Fixed Issues*

Bug ID	Description
109171	**Symptom**: The OAW-IAP UI page appeared blank when accessed through the web browsers. This issue is resolved by introducing a mechanism to resolve the non-ASCII characters in the client names. **Scenario**: This issue was observed in 6.4.2.0-4.1.1.1 or earlier release versions when the names of the OAW-IAP clients contained special characters.
109669	**Symptom**: OAW-IAPs presented the Alcatel-Lucent logo in the browser URL bar during captive portal authentication. To resolve this issue, a check in the OAW-IAP code is added. **Scenario**: Although a customized captive portal certificate was uploaded on the OAW-IAP, the OAW-IAP ignored the certificate and displayed the Alcatel-Lucent logo in the browser URL bar during authentication. This issue was not limited to a specific OAW-IAP platform or release version.
110593	**Symptom**: Although the **Client IP assignment** was set to **Network assigned** and the **Client VLAN assignment** was set to the **Dynamic** option with a VLAN ID in the SSID configuration, the OAW-IAP UI displayed the **Client IP assignment** mode as **Virtual Controller managed** and **Client VLAN assignment** as **Custom** on the **VLAN** tab of the WLAN SSID wizard. **Scenario**: This issue was observed in OAW-IAPs running occurred 6.4.2.0-4.1.1 release when a VLAN ID was configured under a DHCP scope and set as a dynamic VLAN for per-user VLAN assignment in the WLAN SSID wizard.

Wi-Fi Driver

Table 14: *Wi-Fi Driver Fixed Issues*

Bug ID	Description
111138	**Symptom**: A mismatch was found between the supported transmission rate in beacon and the minimum transmission rate configured for the 802.11g clients. A change in the internal OAW-IAP code has resolved this issue. **Scenario**: This issue was found in OAW-IAPs running 6.4.2.0-4.1.1 release version.
110481	**Symptom**: Sometimes, the OAW-IAP225 devices buffered packets for too long. A driver update in the OAW-IAP has resolved this issue. **Scenario**: This issue occurred when the AP buffered packets for an 802.11b client. The issue was found in OAW-IAPs running 6.4.2.0-4.1.1.1.
110524	**Symptom**: Some unknown SSIDs were displayed on Apple® devices. To resolve this issue, upgrade to 6.4.2.3-4.1.1.2 release version. **Scenario**: This issue was observed in OAW-IAPs running 6.4.2.0-4.1.1 release when hidden SSIDs were configured.
110650	**Symptom**: An OAW-IAP225 device could not set Traffic Indication Map (TIM) bits, before sending broadcast or multicast traffic. To resolve this issue, upgrade to 6.4.2.3-4.1.1.2 release. **Scenario**: This issue occurred when hidden SSIDs were configured on the OAW-IAPs and was found in OAW-IAPs running 6.4.2.0-4.1.1.

Known Issues in This Release

The known issues identified in the current patch release are described in the following tables.

Authentication

Table 15: *Authentication Known Issue*

Bug ID	Description
111417	**Symptom**: When Opportunistic Key Caching (OKC) is enabled, the 802.11r capable Apple Mac devices cannot reconnect to an OAW-IAP. **Scenario**: This issue occurs because IAP does not support OKC for Mac clients. Due to this, the non-OKC clients must re-associate to an OAW-IAP after silently disconnecting from the OAW-IAP. This issue is found in OAW-IAPs running 6.3.x.x-4.0.0.x releases. **Workaround**: Disable OKC for the devices that do not support OKC.

Wi-Fi Driver

Table 16: *Wi-Fi Driver Known Issue*

Bug ID	Description
112117	**Symptom**: When the 80 MHz support is enabled on an OAW-IAP, ARM chooses only 36E as a valid channel. **Scenario**: This issue occurrs when ARM is enabled on an OAW-IAP to allocate 80 MHz channels. This issue is observed in the OAW-IAP220 series and OAW-IAP27x devices running 6.4.2.3-4.1.1.2 release. **Woraround**: Disable 80 MHz support or temporarily remove 36E from the list of valid channels.

This chapter provides information on the features and enhancements introduced in 6.4.2.0-4.1 and 6.4.x.x-4.1.x.x releases of AOS-W Instant.

Features and Enhancements

The following features and enhancements were introduced in Instant 6.4.0.2-4.1.0.0 and later 6.4.x.x-4.1.x.x releases.

Support for New Access Points

Instant 6.4.2.0-4.1.1.0 introduces support for new OAW-IAP-200 Series and OAW-IAP-210 Series devices.

- The OAW-IAP-200 Series (OAW-IAP204 and OAW-IAP-205) access points support the IEEE 802.11ac and 802.11n standards for high-performance WLAN. It is a dual radio, 2x2:2 802.11ac access point. These access points use MIMO (Multiple-Input, Multiple-Output) technology and other high-throughput mode techniques to deliver high-performance, 802.11n 2.4 GHz and 802.11ac 5 GHz functionality while simultaneously supporting legacy 802.11a/b/g wireless services. For more information about this product, visit **https://service.esd.alcatel-lucent.com.**
- The OAW-IAP-210 Series (OAW-IAP-214 and OAW-IAP-215) access points support the IEEE 802.11ac standard for high-performance WLAN. It is a 3x3 802.11ac access point that uses MIMO (Multiple-Input, Multiple-Output) technology and other high-throughput mode techniques to deliver high-performance, 802.11ac 2.4 GHz and 802.11ac 5 GHz functionality while simultaneously supporting existing 802.11a/b/g wireless services. For more information about this product, visit **https://service.esd.alcatel-lucent.com.com.**

Enhancement for the AppRF Feed to OmniVista

In this release, each OAW-IAP (Master or Slave) would post the AppRF key data it has collected over the 15 last minutes to the configured OmniVista server. The data is posted only if DPI visibility and OmniVista are configured.

Support for Separate RADIUS and Accounting Servers on OAW-IAPs

Starting with 6.4.2.0-4.1.1.0, Instant enables its users to configure RADIUS authentication servers and accounting servers separately on the OAW-IAP in the SSID profile.

Support for MAC Address Delimiter and Uppercase Characters for All Authentication Types

Starting with 6.4.2.0-4.1.1.0, Instant allows its users to configure the MAC address delimiter or use uppercase letters in a MAC address string for all authentication types. This configuration was previously available only for MAC authentication types.

Improved Troubleshooting Capabilities for OAW-IAP Clustering Issues

Under the following scenarios, Instant versions prior to 6.4.2.0-4.1.1.0 prevented the users from logging into the CLI and User Interface, making troubleshooting difficult.

- When the OAW-IAP cannot be a Master OAW-IAP due to the unavailability of an IP Address and also does not have an uplink connection.
- When the OAW-IAP is unable to join the cluster because of the missing country code, image, or SKU.

- If the user changes the authentication type from Local to a RADIUS Server when the RADIUS server is not ready.
- In the case of OAW-IAP-9x platforms, when the slave OAW-IAP may not be able to join the master OAW-IAP due to certain restrictions.
- If the OAW-IAP is not allowed to join the **allowed-ap-lis**t when **auto-join** has been disabled.
- In a mixed class network, when the slave OAW-IAPs join the master OAW-IAP with a different Instant version causing the image sync from OmniVista to fail.
- When the user connects the E1 port of the OAW-IAP to a switch, and the OAW-IAP is running Instant 6.3.1.4-4.0.0.7 or earlier version.

Starting with 6.4.2.0-4.1.1.0 Instant will allow the user to login to the CLI and execute troubleshooting commands , however the following warning message would be displayed under the above mentioned scenarios:

Warning: CLI module is running in a degraded state. Some commands will not function.

AppRF

Starting with 6.4.0.2-4.1.0.0, Instant supports two AppRF feature sets: On-board Deep Packet Inspection (DPI) and cloud-based Web Policy Enforcement (WPE).

1. **Deep packet inspection**: OAW-IAPs with DPI capability analyze data packets to identify the applications in use, and allow you to create ACL rules to determine client access. The on-board firewall of the OAW-IAP performs the DPI function.
   - **Access control based on application and application category**: You can create firewall policies based application type and application categories. You can also define traffic shaping policies such as bandwidth controls and QoS per application. For example, you can block bandwidth-monopolizing applications on a guest role within an enterprise.
2. **Web Policy Enforcement:** When WPE is enabled, the OAW-IAP performs lookups against cloud-hosted services. This feature requires an annual per OAW-IAP subscription. Please contact the AOS-W Instant sales team.
   - **Access control based on web-category and web-reputation**: You can create a firewall policy to allow or deny access based on a predefined list of website categories and reputation scores. For example, if you block the **web-based-email** category, clients who are assigned this policy will not be able to visit email-based websites such as mail.yahoo.com.

Application visibility: When **AppRF visibility** is enabled in the **System** window in the UI or through the **dpi** command in the CLI, the **AppRF** link appears in the UI when selecting an OAW-IAP from the main window. When clicked, the **AppRF** link displays the application traffic summary for OAW-IAPs and client devices. The AppRF dashboard presents four different graphs with a traffic mix based on **application**, **application category**, **web-category**, and **web-reputation**. Clicking on each category displays client traffic data in real-time or the usage trend in the last 15 minutes.

Based on the AppRF classification of an application, the OAW-IAP can enforce multiple actions, including blocking, QoS enforcement, and throttling.

The AppRF features are not supported on the OAW-IAP92/93 platform. Access rule configuration and charts for applications and application categories are not supported on OAW-IAP104/105, OAW-IAP134/135, and OAW-RAP3WN/3WNP platforms. Only the web category charts are displayed for these OAW-IAP models.

For more information on DPI and AppRF, see:

- *Deep Packet Inspection and Application Visibility* in the *AOS-W Instant 6.4.0.2-4.1 User Guide*

- The **dpi**, **show dpi**, **show dpi-stats**, and **wlan access-rule** commands in the *AOS-W Instant 6.4.0.2-4.1 CLI Reference Guide*

AirGroup Enhancements

Starting with 6.4.0.2-4.1, Instant supports Universal Plug and Play (UPnP) and Digital Living Network Alliance (DLNA) enabled devices. DLNA is a network standard derived from UPnP, which enables devices to discover the services available in a network. DLNA also provides the ability to share data between the Windows or Android based multimedia devices. All the features and policies applicable to mDNS are extended to DLNA to ensure full interoperability between compliant devices.

With DLNA support, the following services are available for the OAW-IAP clients:

- DLNA Media—Applications such as Windows Media Player use this service to browse and play media content on a remote device.
- DLNA Print—This service is used by printers that support DLNA.

For more information on DLNA and how to enable DLNA services, see:

- *Configuring AirGroup and AirGroup Services on an OAW-IAP* in the *AOS-W Instant 6.4.0.2-4.1 User Guide*
- The **airgroup**, **airgroupservice**, and **show airgroup** commands in the *AOS-W Instant 6.4.0.2-4.1 CLI Reference Guide*

Support for New Access Points

This release adds Instant support for OAW-IAP270 series and OAW-IAP103 devices.

- The OAW-IAP270 series (OAW-IAP274 and OAW-IAP275) are environmentally hardened, outdoor rated, dual-radio IEEE 802.11ac wireless access points. These access points use MIMO (Multiple-Input, Multiple-Output) technology and other high-throughput mode techniques to deliver high-performance, 802.11ac 2.4 GHz and 5 GHz functionality while simultaneously supporting existing 802.11a/b/g/n wireless services.
- The OAW-IAP103 wireless access point supports the IEEE 802.11n standard for high-performance WLAN. This access point uses MIMO (Multiple-Input, Multiple-Output) technology and other high-throughput mode techniques to deliver high performance, 802.11n 2.4 GHz or 5 GHz functionality while simultaneously supporting existing 802.11a/b/g wireless services.

For more information about these products, visit https://service.esd.alcatel-lucent.com.

Configurable DSCP Mapping Values for WMM Access Categories

Starting with 6.4.0.2-4.1, Instant supports customized mapping between Wi-Fi Multimedia and DSCP tags for upstream (client to OAW-IAP) and downstream (OAW-IAP to client) traffic.

DSCP classifies packets based on network policies and rules. You can customize the mapping values between WMM ACs and DSCP tags to prioritize various traffic types and apply these changes to a WMM-enabled SSID profile. When WMM AC mappings values are configured, all packets received are matched against the entries in the mapping table and prioritized accordingly.

The following table shows the default WMM AC to DSCP decimal mappings and the recommended WMM AC to DSCP mappings.

Table 17: *Default WMM-DSCP Mapping*

DSCP Decimal Value	WMM Access Category
8	Background
16	
0	Best effort
24	
32	Video
40	
48	Voice
56	

For more information on configuring DSCP mapping values, see:

- *Wi-Fi Multimedia Traffic Management* in the *AOS-W Instant 6.4.0.2-4.1 User Guide*
- The **wlan ssid-profile** command in the *AOS-W Instant 6.4.0.2-4.1 CLI Reference Guide*

Console Access to OAW-IAP

You can use the UI or CLI to allow or restrict access to an OAW-IAP console through the serial port. By default, the console access to an OAW-IAP is enabled.

To disable console access to an OAW-IAP:

- In the UI, navigate to **System** >**General** >**Show advanced options** and select **Disabled** from the **Console** access drop-down.
- In the CLI, run the following commands:

```
(Instant AP)(config)# console
(Instant AP)(console)#
```

Instant UI Changes

Starting with Instant 6.4.0.2-4.1, the **DHCP** tab for configuring a default DHCP scope for Virtual-Controller managed networks is no longer available in the **System** window of the Instant UI. The default DHCP scope configuration options are now available in the **DHCP Server** window. To open the **DHCP Server** window, navigate to **More** >**DHCP Server**.

The **VLAN** tab of the WLAN SSID configuration wizard allows you create a customized DHCP scope to configure a Virtual Controller managed IP and VLAN assignment mode. On selecting the **Virtual Controller managed** option for **Client IP assignment**, the following client VLAN assignment options are displayed:

- **Default**: When selected, the default VLAN as determined by the Virtual Controller is assigned for clients.
- **Custom**: On selecting this, you can either select an existing DHCP scope or create a new DHCP scope by clicking **New**.

For more information, see the following in the *AOS-W Instant 6.4.0.2-4.1 User Guide*:

- *Configuring VLAN Settings for a WLAN SSID Profile*

- *DHCP Configuration*

Full Tunnel-Mode VPN Configuration

Starting with Instant 6.4.0.2-4.1, you can disable split-tunnel configuration for the centralized, L2 subnets. When split-tunnel is enabled, a VPN user can access a public network and a local LAN or WAN network at the same time through the same physical network connection. By default, the split-tunnel function is enabled for all centralized, L2 DHCP profiles.

When split-tunnel is disabled, all the traffic including the corporate and Internet traffic is tunneled irrespective of the routing profile specifications. If the GRE tunnel is down and when the corporate network is not reachable, the client traffic is dropped.

For more information on disabling split-tunnel, see:

- *Configuring Centralized DHCP Scope* in the *AOS-W Instant 6.4.0.2-4.1 User Guide*
- The **ip dhcp** command in the *AOS-W Instant 6.4.0.2-4.1 CLI Reference Guide*

Inbound Firewall

Starting with Instant 6.4.0.2-4.1, you can configure firewall rules for the inbound traffic coming through the uplink ports of an OAW-IAP. The rules defined for inbound traffic are applied if the destination is not a user connected to the OAW-IAP. If the destination already has a user role assigned, the user role overrides the actions or options specified in inbound firewall configuration. However, if a deny rule is defined for the inbound traffic, it is applied irrespective of the destination and user role. Unlike the ACL rules in a WLAN SSID or wired profile, the inbound firewall rules can be configured based on the source subnet.

For all subnets, a deny rule is created by default as the last rule. If at least one rule is configured, the deny all rule is applied to the upstream traffic by default.

Management access to the AP is allowed irrespective of the inbound firewall rule. For more information on configuring restricted management access, see *Configuring Management Subnets* in *AOS-W Instant 6.4.0.2-4.1 User Guide*.

The inbound firewall is not applied to traffic coming through GRE tunnel.

For more information, see:

- *Configuring Inbound Firewall Rules* in the *AOS-W Instant 6.4.0.2-4.1 User Guide*
- The **inbound-firewall** and **show inbound-firewall-rules** commands in the *AOS-W Instant 6.4.0.2-4.1 CLI Reference Guide*

Fast Roaming Enhancements

Starting with 6.4.0.2-4.1, Instant supports 802.11k (Radio Resource Management) and 802.11v (BSS Transition Management) standards to improve Quality of Service (QoS) and seamless connectivity.

The 802.11k protocol provides mechanisms for APs and clients to dynamically measure the available radio resources and enables stations to query and manage their radio resources. In an 802.11k enabled network, APs and clients can share radio and link measurement information, neighbor reports, and beacon reports with each other. This allows the WLAN network infrastructural elements and clients to assess resources and make optimal mobility decisions to ensure Quality of Service (QoS) and seamless continuity.

Ensure that the client match feature is enabled to allow AP and clients to exchange neighbor reports.

The 802.11v standard provides Wireless Network Management enhancements to the IEEE 802.11 MAC and PHY. It extends radio measurements to define mechanisms for wireless network management of stations including BSS transition management. OAW-IAPs support the generation of the BSS transition management request frames to the 802.11k clients when a suitable AP is identified for a client through client match.

For information on configuring a WLAN SSID for 802.11k and 802.11v support, see:

- *Configuring Fast Roaming for Wireless Clients* in the *AOS-W Instant 6.4.0.2-4.1 User Guide*
- The **wlan ssid-profile** command in the *AOS-W Instant 6.4.0.2-4.1 CLI Reference Guide*

Support for 4G Modems

Instant 6.4.0.2-4.1 adds support for the following 4G modems:

- Netgear Aircard 341u
- Pantech UML295
- Franklin Wireless u770
- Huawei 3276s-150

For information on configuring modems to enable 3G or 4G uplink, see:

- *Cellular Uplink* in the *AOS-W Instant 6.4.0.2-4.1 User Guide*
- The **cellular-uplink-profile** command in the *AOS-W Instant 6.4.0.2-4.1 CLI Reference Guide*

Client Match Enhancements

Starting with Instant 6.4.0.2-4.1, in addition to dynamic load balancing, sticky clients, and band steering, the following conditions trigger client match to allow the clients to be moved from one AP to another for better performance.

- **Channel Utilization**: Based on the percentage of channel utilization, clients are steered from a busy channel to an idle channel.
- **Client Capability Match**: Based on the client capability match, clients are steered to appropriate channel, for example HT20, HT40, or VHT80.

If client match is enabled, you can also view a graphical representation of the radio map of an AP and the client distribution on an AP radio.

- Select an access point in the **Access Points** tab and the **Client Match** link, to display a stations map view and a graph with real-time data points for the AP radio. If the AP supports dual band, you can toggle between 2.4GHz and 5 GHz links in the client match graph area to view the data. When you hover the mouse on the graph, details such as RSSI, client match status, and the client distribution on channels are displayed.
- Select a client in the **Clients** tab and the **Client Match** link, to display a graph with real-time data points for an AP radio map. When you hover the mouse on the graph, details such as RSSI, channel utilization details, and client count on each channel are displayed.

For more information on client match configuration and visualization, see the *AOS-W Instant 6.4.0.2-4.1 User Guide*.

Sourcing Virtual Controller Traps from the Virtual Controller IP

Starting with Instant 6.4.0.2-4.1, if the Virtual Controller IP is configured, traps are generated from the Virtual Controller IP. However, the source IP address for the interface up and interface down traps is the AP IP address.

The **sysObject** OID object is enhanced to return information on Virtual Controller. Generally, the **sysObjectID** returns OIDs for a specific model number of the device within the OAW-IAP product family. When an SNMP query is performed for this object on an AP IP address (either master OAW-IAP or slave OAW-IAP IP address), information on AP type is retrieved. However, if the query is performed on a Virtual Controller IP address, information on the OAW-IAP acting as the Virtual Controller is displayed.

For example, if an OAW-IAP135 is the master OAW-IAP, a query on this OAW-IAP returns the iso.org.dod.internet.private.enterprise.aruba.products.apProducts.ap135 (1.3.6.1.4.1.14823.1.2.48) result. Similarly, a query on the Virtual Controller IP returns the OID details with **iapvc**.

For more information on SNMP traps and MIB objects, see *AOS-W Instant 6.4.0.2-4.1 MIB Reference Guide*.

Support for TACACS+ Servers

In Instant 6.4.0.2-4.1, a new external server is added to support authentication and accounting privileges for management users. The users can create several TACACS+ server profiles, out of which one or two of the servers can be specified to authenticate management users.

If two TACACS+ servers are configured as authentication servers, the users can use them as primary and backup servers or in the load balancing mode.

TACACS+ servers can also be used along with RADIUS servers. For example, you can use a TACACS server as the primary server and a RADIUS server as the backup server. OAW-IAPs also support the TACACS+ accounting feature that reports management commands to TACACS+ servers through console port, Telnet, SSH, web, and Cloud,

The TACACS+ accounting option is available only if one of the specified servers is a TACACS+ server.

For more information on TACACS+ Server and TACACS+ accounting, see:

- *Supported Authentication Servers*, *Configuring an External Server for Authentication* in the *AOS-W Instant 6.4.0.2-4.1 User Guide*.
- The **wlan tacacs-server**, **show tacacs server**, and **mgmt-accounting** commands in the *AOS-W Instant 6.4.0.2-4.1 CLI Reference Guide*.

Integration with an XML API Interface

Starting with Instant 6.4.0.2-4.1, OAW-IAPs can be integrated with an XML API Interface by sending specific XML commands to the OAW-IAP from an external server. These commands can be used to add, delete, authenticate, query, or blacklist a user or a client.

For more information on XML API, see:

- *Integrating an OAW-IAP with an XML API interface* in the *AOS-W Instant 6.4.0.2-4.1 User Guide*.
- The **xml-api-server**, **show xml-api-server** commands in the *AOS-W Instant 6.4.0.2-4.1 CLI Reference Guide*.

Backup RADIUS Server Configuration with Termination Enabled

By default, for 802.1X authorization, the client conducts an EAP exchange with the RADIUS server, and the AP acts as a relay for this exchange. When **Termination** is enabled, the OAW-IAP by itself acts as an authentication server and terminates the outer layers of the EAP protocol, only relaying the innermost layer to the external RADIUS server. You can now configure two RADIUS servers for a WLAN SSID when EAP termination is enabled and use these servers in the primary and backup mode.

For more information, see *Configuring 802.1X Authentication for a Wireless Network Profile* in the *AOS-W Instant 6.4.0.2-4.1 User Guide*.

AP Zone Configuration

Starting with 6.4.0.2-4.1, you can configure zone settings for an OAW-IAP. The same zone information can be configured on a WLAN SSID, so that the SSID can be broadcast on the OAW-IAP.

The following constraints apply to the AP zone configuration:

- An OAW-IAP can belong to only one zone and only one zone can be configured on an SSID.
- If an SSID belongs to a zone, all OAW-IAPs in this zone can broadcast this SSID. If no OAW-IAP belongs to the zone configured on the SSID, the SSID is not broadcast.
- If an SSID does not belong to any zone, all OAW-IAPs can broadcast this SSID.

For information on configuring an AP zone, see:

- *Configuring Zone Settings on an OAW-IAP* and *Configuring WLAN Settings for an SSID Profile* in the *AOS-W Instant 6.4.0.2-4.1 User Guide*
- The **zonename** and **wlan ssid-profile** commands in the *AOS-W Instant 6.4.0.2-4.1 CLI Reference Guide*

Authentication Survivability with EAP-TLS

In Instant 6.4.0.2-4.1, the authentication survivability feature is enhanced to support EAP-TLS authentication protocol. The authentication survivability feature supports a survivable authentication framework against the remote link failure when working with the external authentication servers. When enabled, this feature allows the OAW-IAPs to authenticate the previously connected clients against the cached credentials if the connection to the authentication server is temporarily lost.

For EAP-PEAP authentication, ensure that CPPM 6.0.2 or later is used for authentication. For EAP-TLS authentication, any external or third-party server can be used.

For EAP-TLS authentication, ensure that the server and CA certificates from the authentication servers are uploaded on OAW-IAP. For more information, see *Uploading Certificates* in *AOS-W Instant 6.4.0.2-4.1 User Guide*.

The **show auth-survivability** command is also enhanced to display debug logs for troubleshooting issues. For more information, see:

- *Support for Authentication Survivability* in the *AOS-W Instant 6.4.0.2-4.1 User Guide*.
- The **show auth-survivability** command in the *AOS-W Instant 6.4.0.2-4.1 CLI Reference Guide*

Support for 128 ACL Rules

Starting with Instant 6.4.0.2-4.1 release, you can now configure up to 128 ACL rules for a wired or wireless profile through the WLAN wizard or wired user role through the UI and CLI.

- To configure ACL rules for an SSID or wired port profile role in the CLI, use the **wlan access-rule** command.
- To configure ACL rules in the UI, navigate to **Security** > **Roles**. Select the role and click **New** under **Access Rules**.

Configurable Port for Communication between OmniVista Management Server and OAW-IAP

Starting with Instant 6.4.0.2-4.1, you can now customize the port number of the OmniVista management server through the server_host:server_port format.

For more information on managing an OAW-IAP through OmniVista, see *Managing OAW-IAP from OmniVista* in *AOS-W Instant 6.4.0.2-4.1 User Guide*.

Disabling of Bridging and Routing Traffic between Clients Connected to an SSID

Starting with Instant 6.4.0.2-4.1, you can now disable bridging and routing traffic between two clients connected to an SSID. When inter-user bridging and local routing is denied, the clients can connect to the Internet but cannot communicate with each other, and the bridging and routing traffic between the clients is sent to the upstream device to make the forwarding decision.

To deny inter-user bridging and local routing for the WLAN SSID clients, run the following commands at the CLI:

```
(Instant AP)(config)# wlan ssid-profile <ssid-profile>
(Instant AP) (SSID Profile <ssid-profile>)# deny-inter-user-bridging
(Instant AP) (SSID Profile <ssid-profile>)# deny-local-routing
(Instant AP) (SSID Profile <ssid-profile>)# end
(Instant AP)# commit apply
```

NTP Server Configuration Options

The Network Time Protocol (NTP) helps obtain the precise time from a server and regulate the local time in each network element. Connectivity to a valid NTP server is required to synchronize the OAW-IAP clock to set the correct time. If NTP server is not configured in the OAW-IAP network, an OAW-IAP reboot may lead to variation in time data.

By default, the OAW-IAP tries to connect to **pool.ntp.org** to synchronize time. A different NTP server can be configured from the UI. It can also be provisioned through the DHCP option 42. If the NTP server is configured, it takes precedence over the DHCP option 42 provisioned value. The NTP server provisioned through the DHCP option 42 is used if no server is configured. The default server pool.ntp.org is used if no NTP server is configured or provisioned through DHCP option 42.

Change in Extended SSID Factory Default Settings

Starting with Instant 6.4.0.2-4.1, extended SSID is enabled by default in the factory default settings of Instant APs. This disables mesh in the factory default settings.

Support for Read-Only Users to Access CLI

Starting with Instant 6.4.0.2-4.1, read-only users can access the OAW-IAP CLI through telnet, SSH, or console.

Enhancement to the Client Match Maximum Threshold Limit

Starting with Instant 6.4.0.2-4.1, the maximum threshold limit for Client Match is set to 255. The previous maximum threshold value was 20.

Regulatory Updates

Table 18: *Regulatory Domain Updates*

Regulatory Domain	Description
Mexico	Support for all shipping OAW-IAPs.
Australia, New Zealand, and Canada	Support for OAW-IAP275 platform.
Australia, New Zealand, and India	Support for OAW-IAP103 platform.

Reintroducing OAW-IAP92/93 in AOS-W Instant 6.4.0.3-4.1.0.1 and future 6.4.x.x-4.1.x.x releases

Support for OAW-IAP92/93 is reintroduced in Instant 6.4.0.3-4.1.0.1 and will continue in future 6.4.x.x-4.1.x.x releases. However, the following features are no longer available for OAW-IAP92/93 in 6.4.x.x-4.1.x.x releases:

- AirGroup
- Internal RADIUS server for 802.1x authentication
- EAP Termination
- Authentication Survivability
- LLDP integration

The features listed above may be configured through Instant CLI/Web UI and OmniVista Management Platform, but will have no effect on OAW-IAP92/93. In a cluster running Instant 6.4.x.x-4.1.x.x, only OAW-IAP92/93 will have the above limitations.

In order to conserve memory, OAW-IAP92/93 is now restricted to a single active CLI session, either through a console, SSH, or telnet. An error message "**All CLI sessions are in use**" is displayed if the user attempts to open multiple sessions.

Security Update

As part of CVE-2014-3566 security vulnerabilities and exposures, SSLv3 transport layer security is disabled from Instant 6.4.2.0-4.1.1.1 release. Clients using SSLv3 will not be able to access captive portal or Instant UI. Instead of SSLv3, use TLS1.0 transport security or later versions.

Addition of NOTICE Syslog Message

In the 6.4.2.0-4.1.1.1 release, when a new user is added or deleted, a syslog NOTICE message with the IP and MAC address of the client is generated.

Age Field in RSSI Entry Sent to ALE Server

In the 6.4.2.0-4.1.1.1 release, the **Age** field is added to the RSSI entry in the data sent from the OAW-IAP to the ALE server, to ensure that the information pertaining to the aged clients are discarded from the ALE database.

Resolved Issues in 6.4.2.0-4.1.1.1

The following issues are fixed in the 6.4.2.0-4.1.1.1 release.

Authentication

Table 19: *Authentication Fixed Issues*

Bug ID	Description
105221	**Symptom:** When using separate accounting servers for a specified OAW-IAP, the accounting packets were not being sent to both accounting servers. This issue is resolved after making an internal code change. **Scenario**: This issue occurs when the user sets 2 accounting servers for accounting purposes. This issue was observed in all OAW-IAPs running Instant 6.4.2.0-4.1.1.0 release.
106750	**Symptom:** An 802.11b legacy handy terminal failed to authenticate using dynamic WEP/EAP-TLS. This issue is resolved by modifying the Instant software to handle the frames from the EAP terminals. **Scenario**: The OAW-IAP works fine with open system ESSID and static WEP, but fails when dynamic WEP is used. This issue was observed in OAW-IAP225 running Instant 6.3.1.1-4.0.0.0 release and later versions.

Captive Portal

Table 20: *Captive Portal Fixed Issue*

Bug ID	Description
105924	**Symptom**: Captive Portal did not work with custom certificates. This issue is resolved by adding a support unencrypted private key in the custom certificate. **Scenario**: This issue occurred when a custom certificate was being used and the private key header was "BEGIN PRIVATE KEY". This issue was observed in all OAW-IAPs running Instant 6.3.1.1-4.0.0.0 and later versions.

Datapath / Firewall

Table 21: *Datapath / Firewall Fixed Issue*

Bug ID	Description
106268	**Symptom**: DHCP routing was delayed when Captive Portal and MAC-auth were enabled. This issue is resolved after mapping the client to the ACL103. **Scenario**: This issue was observed because of the pre-auth role ACL and was observed in OAW-IAP225 running Instant 6.4.2.0-4.1.1.0 and earlier releases.

General

Table 22: *General Fixed Issues*

Bug ID	Description
106291	**Symptom:**OAW-IAPs were getting automatically rebooted in the cluster stating that the system clock was far ahead of the NTP sync result. This issue is resolved by preventing the OAW-IAPs from rebooting automatically. **Scenario**: This issue occurred when the OAW-IAP changed the system time based on the data in the UDP packets. This issue is not limited to a specific OAW-IAP model or software release version.
108209	**Symptom:**OAW-IAP-22x series was unable to perform an LACP failover when the E0 port was down. The fix ensures a successful LACP failover. **Scenario**: This issue was observed in OAW-IAP220 series and OAW-IAP270 series access points running Instant 6.4.0.2-4.1.0.x versions.

IDS

Table 23: *IDS Fixed Issue*

Bug ID	Description
104645	**Symptom:** False alarms were raised in the cluster indicating that the connected OAW-IAP was a **Rogue**OAW-IAP. The fix prevents the false alarms. **Scenario**: This issue occurred when the OAW-IAP considered a remote MAC client as a wired client This issue was observed in all OAW-IAPs running Instant 6.4.2.0-4.1.1.0 release and earlier versions.

Mesh

Table 24: *Mesh Fixed Issues*

Bug ID	Description
105155	**Symptom:** SNMPv3 traps with inform enabled were not getting processed on the OAW-IAP204/205 platforms as there were failures in the initial exchange of the INFORM messages. The fix ensures there are no failures during the exchange of INFORM messages. **Scenario**: This issue occurred when the SNMPv3 INFORM receiver was configured on the OAW-IAP204/205 platforms. This issue was observed in OAW-IAP204/205 platforms running Instant 6.4.2.0-4.1.1.0 release.
108512	**Symptom:** Large number of packet drops were reported on the OAW-IAP Mesh point. This issue is resolved by making an internal code change. **Scenario**: When reporting the failed tx packets, OAW-IAP also included the 802.11 management packets and some control packets which were not relevant for the report. This issue was observed in OAW-IAP175P/175AC running Instant6.4.0.3-4.1.0.2 release.

SNMP

Table 25: *SNMP Fixed Issues*

Bug ID	Description
105155	**Symptom:** SNMPv3 traps with inform enabled were not getting processed on the OAW-IAP204/205 platforms as there were failures in the initial exchange of the INFORM messages. The fix ensures there are no failures during the exchange of INFORM messages. **Scenario**: This issue occurred when the SNMPv3 INFORM receiver was configured on the OAW-IAP204/205 platforms. This issue was observed in OAW-IAP204/205 platforms running Instant 6.4.2.0-4.1.1.1 release.
107073	**Symptom**: Incorrect output was generated for ESSID with SNMP walk, get, or get-next functions. This issue is resolved after making an internal code change. **Scenario**: This issue occurred when an existing SSID was diabled. This issue was not limited to a specific OAW-IAP model and was found in OAW-IAPs running Instant 6.4.2.0-4.1.1 and earlier versions.

STM

Table 26: *STM Fixed Issue*

Bug ID	Description
106383	**Symptom:** Clients using MAC authentication and 802.1x authentrication went into a denyall role when roaming with PMK cache in the cluster. This issue is resolved after a making a change in the code. **Scenario**: This issue was observed when the clients roam from one OAW-IAP to another with PMK cache. This issue was not limited to a specific OAW-IAP model or Instant software release version.

VPN

Table 27: *VPN Fixed Issue*

Bug ID	Description
108068	**Symptom:** An OAW-IAP managed through OmniVista was unable to establish IPSec tunnel after a factory reset. This issue is resolved by updating the time required for setting up an IPSec tunnel. **Scenario**: This issue is not limited to a specific OAW-IAP model or software release version.

Resolved Issues in 6.4.2.0-4.1.1.0

The following issue is fixed in the 6.4.2.0-4.1.1.0 release:

User Interface

Table 28: *User Interface Fixed Issue*

Bug ID	Description
104466	**Symptom:** An OAW-IAP User Interface (UI) session remained connected even after the password was changed in another CLI/UI session. This issue is resolved by making a code level change to disconnect the UI/CLI session logged in using the old password. **Scenario**: This issue occurred when a change was made to the admin, read-only, or guest accounts for management user accounts. This issue was observed in all OAW-IAPs running Instant 6.4.0.3-4.1.0.1 release.

Resolved Issues in 6.4.0.3-4.1.0.2

The following issues are fixed in the 6.4.0.3-4.1.0.2 release:

AirGroup

Table 29: *AirGroup Fixed Issue*

Bug ID	Description
104037	**Symptom:** AirGroup was unable to maintain the record cache of the servers connected to the OAW-IAP cluster in the network. This issue is resolved by implementing a fix to maintain the record cache. **Scenario:** This issue occurred when the AirGroup servers were roaming from one OAW-IAP to another in the cluster. This issue was not limited to a specific OAW-IAP model or Instant release version.

Authentication

Table 30: *Authentication Fixed Issue*

Bug ID	Description
103899	**Symptom:** Clients were unable to connect to the slave OAW-IAPs when the WPA-passphrase used to connect to the slave OAW-IAP contained a space. This issue is resolved by making a code level change. **Scenario:** This issue occurred when a space was included in the WPA2-PSK passphrase for the slave OAW-IAP. This issue was observed in all platforms running Instant 6.3.1.4-4.0.0.5 and later versions.

ARM

Table 31: *ARM Portal Fixed Issues*

Bug ID	Description
104127	**Symptom:** The users were experiencing voice call issues when a SIP phone was connected to OAW-IAP225. This issue is resolved by making a code level change to increase the voice aware scan rejects counter during voice calls. **Scenario:** This issue occurred when scanning was enabled on an OAW-IAP225 running Instant 6.4.0.2-4.1.0.0 and later versions.
103674	**Symptom:** Performance of 2.4G band legacy traffic was poor from the OAW-IAP towards the client. The OAW-IAP was configured to a very high max distance by default, to allow the RF signal transmitted as far as 6400 meters away, at the cost of low performance. This issue is resolved by changing the default value to 600 meters, which is the common case for ordinary client accessing. **Scenario:** This issue occurred when the legacy client was connected to the OAW-IAP at 2.4G band. This issue was observed in OAW-IAP9x and OAW-IAP1xx platforms running Instant 6.3.1.1-4.0.0.0 and later versions.

DHCP Server

Table 32: *DHCP Server Fixed Issue*

Bug ID	Description
102989	**Symptom:** The **Exclude IP address** range in DHCP profile configuration was not taking effect. This issue is resolved by making a code level change. **Scenario:** This issue occurred when the **Exclude IP address** functionality was broken after the set of configurations from the config manager were not applied correctly to the DHCP Server process. This issue was observed in all OAW-IAPs running Instant 6.4.0.2-4.1 and later versions.

General

Table 33: *General Fixed Issue*

Bug ID	Description
103575	**Symptom:** A Kernel crash was observed when Client Match was enabled on the OAW-IAP. This issue is resolved by fixing a memory corruption in the OAW-IAP. **Scenario:** This issue occurred due to a memory corruption on the OAW-IAP. This issue was observed in all OAW-IAPs running Instant 6.4.0.2-4.1 and later versions.

User Interface

Table 34: *User Interface Fixed Issue*

Bug ID	Description
104466	**Symptom:** The OAW-IAP UI session remained connected even after the password was changed in another CLI/UI session. This issue is resolved by making a code level change to disconnect the UI/CLI session logged in using the old password. **Scenario:** This issue occurred when a change was made to the admin, read-only, or guest accounts for management user accounts. This issue was observed in all OAW-IAPs running Instant 6.4.0.3-4.1.0.1 release.

VC Management

Table 35: *VC Management Fixed Issues*

Bug ID	Description
103539	**Symptom:** Some users were getting warning messages that read "CLI module is running in a degraded state. Some commands will not function", when they were trying to access the CLI mode. **Scenario:** This issue occurred when the external RADIUS server was unavailable for authentication to the management account users. This issue was observed in all OAW-IAPs running AOS-W Instant 6.4.0.3-4.1.0.1 release.
102523	**Symptom:** An OAW-IAP105 with mac-prefix D8C7C8C was unable to join the OAW-IAP cluster after an upgrade to either the 6.2.x or 6.3.x versions. This issue is resolved by making a code level change to enable the OAW-IAP to join the cluster after the upgrade. **Scenario:** This issue occurred when OAW-IAP105 with mac-prefix D8C7C8C was upgraded from a 6.1.x version to a 6.2.x or later version.

VPN

Table 36: *VPN Fixed Issue*

Bug ID	Description
105416	**Symptom:** Motorola scanners were taking longer than the expected time to connect to the network. This issue is resolved by making a code level change to prevent the OAW-IAP from sending de-authentication responses in between authentication requests. **Scenario:** This issue occurred when the OAW-IAP began sending deauthentication responses in between authentication requests. This issue was observed in OAW-IAP135 running AOS-W Instant 6.3.1.2-4.0.0.4 and later versions.

Resolved Issues in 6.4.0.3-4.1.0.1

The following issues are fixed in the 6.4.0.3-4.1.0.1 release:

OmniVista

Table 37: *OmniVista Fixed Issue*

Bug ID	Description
104037	**Symptom:** OAW-IAP was broadcasting the previous Instant SSID, even after receiving the latest configuration from OmniVista. This issue is resolved by introducing a fix to handle the packet loss issue between the Virtual Controller and the Slave OAW-IAP. **Scenario:** This issue occurred when there was packet loss in the L2 wired network to which the OAW-IAP is connected. This issue was observed in all OAW-IAP models running Instant 6.3.1.1-4.0.0.0 and earlier versions.

Authentication

Table 38: *Authentication Fixed Issues*

Bug ID	Description
101378	**Symptom:** The OAW-IAP sent an accounting stop packet when the client was re-authenticated. This issue is resolved by preventing the OAW-IAP from sending any accounting stop packets during L2 re-authentication. **Scenario:** This issue occurred when the client attempted to re-authenticate on the OAW-IAP. This issue was not limited to a specific OAW-IAP model or Instant release version.
103441	**Symptom:** Users were unable to login to the OAW-IAP cluster when the RADIUS server IP was set as 0.0.0.0. This issue is resolved by making a code level change to accept 0.0.0.0 as the RADIUS server IP address. **Scenario:** This issue occurred when the OAW-IAP was unable to send RADIUS request to the admin server and failed to fall back to the internal server. This issue was observed in all OAW-IAP models running Instant 6.3.1.2-4.0.0.4 release.
101614	**Symptom:** During 802.1X authentication, the calling-station-id was incorrectly displayed as 5A:00:00:00:00:00. This issue is resolved by using the correct calling-station-id during 802.1x authentication. **Scenario:** This issue was not limited to a specific OAW-IAP model or Instant release version.
100843	**Symptom:** OAW-IAP used MAC address as the username during MAC authentication. This issue is resolved by providing RADIUS attribute username as the client username during MAC authentication. **Scenario:** This issue was not limited to a specific OAW-IAP model or Instant release version.

Captive Portal

Table 39: *Captive Portal Fixed Issue*

Bug ID	Description
99229	**Symptom:** OAW-IAP cluster was unstable when the filename for the uploaded Captive Portal logo had a space in it. This issue is resolved after making a minor change to the code. **Scenario:** This issue was not limited to a specific OAW-IAP model or Instant release version.

Datapath

Table 40: *Datapath Fixed Issue*

Bug ID	Description
101274	**Symptom:** Prioritization of voice or video calls did not work for Lync when the classify media option was enabled. This issue is resolved after making a minor change to the code. **Scenario:** This issue was observed in all OAW-IAP models running Instant 6.4.0.2-4.1 release.
103898	**Symptom:** A crash was observed in OAW-IAP135 when multiple clients were connected. Upgrading to AOS-W Instant 6.4.0.3-4.1.0.1 resolves the issue. **Scenario:** This issue was observed when DMO was enabled on OAW-IAP135 running Instant 6.4.0.2-4.1 release.

IAP-VPN

Table 41: *IAP-VPN Fixed Issue*

Bug ID	Description
102327	**Symptom:** OAW-IAP was unable to send Syslog messages, when VPN connectivity comes online and changes the route to Syslog server, This issue is resolved by recreating the session. **Scenario:** This issue was not limited to a specific OAW-IAP model or Instant release version.

STM

Table 42: *STM Fixed Issue*

Bug ID	Description
101708	**Symptom:** OAW-IAP reported incorrect client OS type for Blackberry® Z10 device. This issue is resolved after making a minor change to the code. **Scenario:** This issue occurred when the OAW-IAP missed the user agent of the Blackberry Z10 device. This issue was not limited to a specific OAW-IAP model or Instant release version.

VPN

Table 43: *VPN Fixed Issue*

Bug ID	Description
103838	**Symptom:** OAW-IAP register message did not reach the switch due to a low buffer size. The issue is resolved by increasing the buffer size. **Scenario:** This issue was observed in OAW-IAPs running Instant 6.4.0.2-4.1 release when a VPN tunnel was established with the switch.

WiFi Driver

Table 44: *WiFi Driver Fixed Issue*

Bug ID	Description
103680	**Symptom:** OAW-IAPs send out beacon with essid **aruba-ap** during bootup. This issue is resolved after making the default essid as **OEM_vendor_name-ap**. **Scenario:** This issue occurred when the default initialization essid was **aruba-ap**. This issue was observed in all OAW-IAP models running Instant 6.4.0.2-4.1.0.0 and earlier versions.

Wireless

Table 45: *Wireless Fixed Issues*

Bug ID	Description
99833	**Symptom:** When more than 120 customers were connected in the bridge mode, broadcast packets were dropped and customers lost connectivity. This fix ensures that the broadcast packet handling is modified to resolve the issue. **Scenario:** This issue was observed when the frequency of customers trying to connect to the OAW-IAPs was high. This issue was observed in OAW-IAP225 running Instant 6.3.1.2-4.0.0.x releases.
94482	**Symptom:** An OAW-IAP crashed due to an internal Watchdog timeout. This issue is resolved by reducing the wait time, and rebooting the OAW-IAP to recover from that state. **Scenario:** This issue occurred within one of the reset functions in the Ethernet driver where there was a long wait, which exceeded the watchdog timeout, causing OAW-IAP failure. This issue was observed in OAW-IAP225 running Instant 6.4.0.0-4.0.0.x releases.

This chapter describes the known issues identified in previous 6.4.x.x-4.1.x.x releases of AOS-W Instant.

Limitations

No Support for OAW-IAP92/93

In Instant6.4.0.2-4.1.0.0, the OAW-IAP92/93 devices are not supported.

Do not upgrade an Instant network running OAW-IAP92/93 devices to Instant 6.4.0.2-4.1.0.0. In case of an accidental upgrade, you may be able to downgrade to the 6.3.1.1-4.0 release without losing the existing configuration. However, the OAW-IAP92/93 devices are supported again in subsequent patch releases (6.4.x.x-4.1.x.x) but with reduced functionality. Instant 6.4.x.x-4.1 will be the last code branch to support OAW-IAP92/93.

No Support for Mesh on OAW-IAP2xx Access Points

Mesh OAW-IAP configuration is not supported on 802.11ac AP platforms (OAW-IAP2xx access points).

Application Classification

The following table lists the popular applications and describes the expected classification behaviour associated with these applications:

Table 46: *Application Classification*

Bug ID	Description
Lync	Due to the adaptive nature of Lync, a few sessions might occasionally be wrongly classified.
Skype	If user has already logged into Skype or has the previous login session cached, classification might fail, enabling the user to login to Skype even when there is an application rule to deny Skype. Due to the adaptive nature of Skype, voice and video calls might not be wrongly classified at times, affecting bandwidth throttling and enforcement.
Speedtest.net	In certain geographical locations, speedtest.net uses an alternate port (TCP 8080) for the actual data test which can lead to classification failures.
Tor Browser	Proxying through Tor using proxy configuration or using the packaged Tor Browser does not get classified.
Carbonite	Carbonite application classification does not function as expected.
Google Drive	Google Drive application is part of the Google Docs application suite. This needs to be enabled to classify google drive.

Known Issues

3G/4G Uplink Management

Table 47: *3G/4G Uplink Management Known Issue*

Bug ID	Description
98775	**Symptom:** Sometimes, the USB modem connected to OAW-RAP108 and OAW-RAP3WN is not functional as the 3G and 4G interfaces fail to come up. **Scenario**: This issue is observed in OAW-RAP108 and OAW-RAP3WN running Instant 6.2.0.0-3.3 or later. **Workaround**: Disconnect and reconnect the USB modem.
102807	**Symptom:** Users are currently unable to provision the Netgear 340U USB modem on the OAW-IAP. **Scenario**: This issue is observed in all OAW-IAPs running Instant 6.4.2.0-4.1.1 release. **Workaround**: As a workaround, run the Netgear linux patch to enable the Netgear 340U modem to work with IAP.
105159	**Symptom:** Huawei 3276-150 verison of USB modem works with all AP types except OAW-RAP108, OAW-RAP109, and OAW-RAP3WN. **Scenario**: This issue is not limited to a specific OAW-IAP model or software version. **Workaround**: The Huawei 3276-150 modem will not be detected on OAW-RAP108 and OAW-RAP109, and so as a workaround, connect to the modem using an external hub. For OAW-RAP3WN, use Instant 6.4.0.3-4.1.0.1 as the firmware with the USB power hub to connect to the modem.
104803	**Symptom:** Changing the priorities of Ethernet uplink and Cellular uplink having default values of 0 and 7 to 7 and 4 or any other number does not work, wheras chaning the Ethernet uplink value to anything other than 7 would work. **Scenario**: This issue is observed when the priorities are changed for the Ethernet andCellular uplinks. This issue is not limited to a specific OAW-IAP model or software release. **Workaround**: None.

OmniVista

Table 48: *OmniVista Known Issue*

Bug ID	Description
101945	**Symptom:** Image sync fails when OmniVista Management Platform (AMP) uses user-defined ports with Master OAW-IAPs and Slave OAW-IAPs. **Scenario**: This issue occurs when the Master AP type is different from the Slave AP type and the Master OAW-IAP image is different from the Slave OAW-IAP image. This issue is observed in OAW-IAPs running Instant 6.4.0.2-4.1.0.0. **Workaround**: None

Authentication

Table 49: *Authentication Known Issues*

Bug ID	Description
105221	**Symptom:** When using separate accounting servers for a specified OAW-IAP, the accounting packets are not being sent to both accounting servers. **Scenario**: This issue occurs when the user sets 2 accounting servers for accounting purposes. This issue is not limited to a specific OAW-IAP model or software release version. **Workaround**: No workaround as yet.
106047	**Symptom:** Wired client is not displayed in OmniVista Management Platform (AMP) and shows an MIB_ETHERNET_TABLE error. **Scenario**: This issue occurs when the OAW-IAP has multiple Ethernet interfaces and the MAC address of the devices is set as FE or FF. This issue is observed in OAW-IAPs running Instant 6.4.0.2-4.1.0.0 release and earlier versions. **Workaround**: None.

Datapath / Firewall

Table 50: *Datapath / Firewall Known Issue*

Bug ID	Description
109301	**Symptom:** Domain ACL does not work on IAP due to a network order issue. **Scenario**: This issue occurs when domain acl is configured on the role and is observed in OAW-IAP205. **Workaround**: None

General

Table 51: *General Known Issues*

Bug ID	Description
98455	**Symptom:** The Speed or Duplex configuration change of Ethernet Port does not take effect on Instant APs. **Scenario**: This issue is observed in OAW-IAPs running Instant 6.2.0.0-3.3 or later releases. **Workaround**: Reboot the OAW-IAP.
104232	**Symptom:** Auto-negotiation information is absent in the LLDP messages for OAW-IAP204/205. **Scenario**: This issue is observed in OAW-IAP204/205 platforms running Instant 6.4.2.0-4.1.1release. **Workaround**: None.

SNMP

Table 52: *SNMP Known Issues*

Bug ID	Description
98455	**Symptom:** The Speed or Duplex configuration change of Ethernet Port does not take effect on Instant APs. **Scenario**: This issue is observed in OAW-IAPs running Instant 6.2.0.0-3.3 or later releases. **Workaround**: Reboot the OAW-IAP.