AOS-W Instant 6.4.4.8-4.2.4.18

Release Notes

Revision History

The following table lists the revisions of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

AOS-W Instant 6.4.4.8-4.2.4.18 is a patch release that introduces feature enhancements, fixes to the issues found in the previous releases as well as known and outstanding issues in this 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 6.4.4.6-4.2.4.0 User Guide.*

Chapter Overview

What's New in this Release on page 8 lists the regulatory information, feature enhancements, fixed issues, and the outstanding issues in AOS-W Instant 6.4.4.8-4.2.4.18 release.

Features in Previous Releases on page 12 describes the features and enhancements in previous AOS-W Instant 6.4.4.x-4.2.4.x releases.

Known Issues on page 11 lists the known issues identified in the 6.4.4.x-4.2.4.x releases.

Issues Resolved in Previous Releases on page 14 lists the issues fixed in the previous AOS-W Instant 6.4.4.x-4.2.4.x releases.

For list of terms, see Glossary.

Supported Browsers

The following browsers are officially supported for use with Instant Web User Interface (WebUI):

- Microsoft Internet Explorer 10.x and 11 on Windows 7 and Windows 8
- Mozilla Firefox 23 or later on Windows Vista, Windows 7, Windows 8, and macOS
- Apple Safari 5.1.7 or later on macOS

Contacting Support

Table 2: *Contact Information*

Contact Center Online	
Main Site	https://www.al-enterprise.com
Support Site	https://businessportal2.alcatel-lucent.com
Email	ebg_global_supportcenter@al-enterprise.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, features and enhancements, fixed issues, and outstanding issues in the AOS-W Instant 6.4.4.8-4.2.4.18 release.

Regulatory Domain Updates

The following table lists the DRT file versions supported by Instant 6.4.4.x-4.2.4.x releases:

Table 3: *DRT Versions*

Instant Release Version	Applicable DRT Version
Instant 6.4.4.8-4.2.4.18	1.0_78620
Instant 6.4.4.8-4.2.4.17	1.0_75772
Instant 6.4.4.8-4.2.4.16	1.0_73578
Instant 6.4.4.8-4.2.4.15	1.0_72670
Instant 6.4.4.8-4.2.4.14	1.0_70267
Instant 6.4.4.8-4.2.4.13	1.0_69377
Instant 6.4.4.8-4.2.4.12	1.0_68143
Instant 6.4.4.8-4.2.4.11	1.0_64134
Instant 6.4.4.8-4.2.4.10	1.0_62496
Instant 6.4.4.8-4.2.4.9	1.0_61527
Instant 6.4.4.8-4.2.4.8	1.0_60114
Instant 6.4.4.8-4.2.4.7	1.0_59783
Instant 6.4.4.8-4.2.4.6	1.0_58258
Instant 6.4.4.8-4.2.4.5	1.0_57815
Instant 6.4.4.8-4.2.4.4	1.0_57223
Instant 6.4.4.8-4.2.4.3	1.0_56643
Instant 6.4.4.8-4.2.4.2	1.0_56050
Instant 6.4.4.8-4.2.4.1	1.0_55489
Instant 6.4.4.6-4.2.4.0	1.0_54870

For a complete list of countries certified with different AP models, see the respective DRT release notes at https://businessportal2.alcatel-lucent.com.

New Features and Enhancements

There are no new features introduced in this release.

Resolved Issues in this Release

The following issue is fixed in this release:

Platform

Table 4: *Platform Fixed Issue*

Bug ID	Description
AOS-212241	**Symptom:** An Instant AP failed to communicate with the NTP server and synchronize system time. The fix ensures that the Instant AP connects to the NTP server and synchronizes system time as expected. **Scenario:** This issue was observed in APs running AOS-W Instant 6.4.4.8-4.2.4.16 or later versions.

Known Issues

There are no known issues identified in this release.

This chapter describes the features and enhancements introduced in previous AOS-W Instant 6.4.4.x-4.2.4.x releases.

Features and Enhancements

The following features and enhancements were introduced in Instant 6.4.4.x-4.2.4.x releases.

Disabling TLS RSA Cipher Suites

Starting from Alcatel-Lucent Instant 6.4.4.8-4.2.4.11, the following TLS RSA cipher suites are disabled to ensure complete forward confidentiality and to prevent the Return of Bleichenbacher's Oracle Threat (ROBOT) attacks in OAW-IAPs:

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

This enhancement impacts functionalities such as OpenFlow, RadSec, SSH, WebUI, Authentication, Captive Portal, and OmniVista.

Support for Huawei E3372H-153 Modem on OAW-IAP205H

Starting from Instant 6.4.4.8-4.2.4.5, the Huawei E3372H-153 modem is supported on OAW-IAP205H access points.

WebUI Enhancement

The WPA Enterprise AES setting was not available in the Instant UI. A new field is added in the Instant UI for the WPA Enterprise AES setting.

Wildcard Server Certificate Support for Captive Portal

Instant 6.4.4.8-4.2.4.4 now supports the wildcard server certificate for captive portal authentication.

New Command for Using VC IP Address as Source IP Address

The following command is introduced in Instant 6.4.4.8-4.2.4.4 to use the VC IP address as the source IP address for a TFTP session.

(Instant AP)# download-source vcip

In the above command, the user enters vcip as a string which gets substituted by the real VC IP address when executed.

Support for Telus Aircard 340U Modem

Starting from Instant 6.4.4.8-4.2.4.1, the Telus Aircard 340U modem is supported.

Support for Hotspot 2.0 on OAW-IAP325 Access Points

Starting from Instant 6.4.4.6-4.2.4.0, the Hotspot 2.0 (Passpoint Release 1) feature is supported on OAW-IAP325 access points. For more information, see:

- *Hotspot Profiles* in *AOS-W Instant 6.4.4.6-4.2.4.0 User Guide*.

Enhancement to Routing Profile Capability

A new field called **metric** has been added as part of the routing profile configuration. When two or more routes with the same destination are available for data transfer, the route with the lowest metric value takes precedence. For more information, see:

- *Configuring Routing Profiles* in *AOS-W Instant 6.4.4.6-4.2.4.0 User Guide.*
- **routing-profile** command in *AOS-W Instant 6.4.4.6-4.2.4.0 CLI Reference Guide.*

Enhancement for Disabling Default Auto Topology Rules

Starting from Instant 6.4.4.6-4.2.4.0, the auto topology rules can be disabled using the Instant UI and CLI. For more information, see:

- *Configuring Firewall Settings to Disable Auto Topology Rules* in *AOS-W Instant 6.4.4.6-4.2.4.0 User Guide.*
- **Firewall** command in *AOS-W Instant 6.4.4.6-4.2.4.0 CLI Reference Guide.*
- **show Firewall** command in *AOS-W Instant 6.4.4.6-4.2.4.0 CLI Reference Guide.*

Enhancement to ALE Monitoring Capabilities

Starting from Instant 6.4.4.6-4.2.4.0, ALE monitoring capabilities have been enhanced to receive notifications on the Wireless Backup Unit (WBU) stats and status of LTE 3G/4G modems. ALE is now notified with the following monitoring statistics:

- A LTE 3G/4G modem is plugged in or unplugged from the OAW-IAP USB port.
- The modem is incorrectly plugged in to the USB port of the slave OAW-IAP instead of the master OAW-IAP.
- The current status of the SIM card used in the modem.
- The current status of the uplink in use when the modem is connected to the master OAW-IAP.
- The WBU Rx or Tx bytes from the modem traffic when there is an uplink connectivity between the modem and the master OAW-IAP.

Additionally, the Master OAW-IAP will now notify ALE through hearbeat messages indicating the status (UP or DOWN) of the slave OAW-IAPs.

Allow Zero-Touch Provisioning When NTP Server is Unreachable

Starting from Instant 6.4.4.6-4.2.4.0, zero-touch provisioning is allowed even when the NTP server is unavailable.

This chapter describes the issues fixed in previous AOS-W Instant 6.4.4.x-4.2.4.x releases.

Issues Resolved in 6.4.4.8-4.2.4.17

Activate

Table 5: *Activate Fixed Issue*

New Bug ID	Old Bug ID	Description
AOS-170960 AOS-177472 AOS-201318	140548 175139	**Symptom:** An Instant AP failed to convert to Remote AP when the convert rule was pushed from Activate. The fix ensures that the Instant AP converts to Remote AP as expected. **Scenario:** This issue was observed in APs running AOS-W Instant 6.4.4.4-4.2.3.0 or later versions.

Issues Resolved in 6.4.4.8-4.2.4.16

Authentication

Table 6: *Authentication Fixed Issue*

New Bug ID	Old Bug ID	Description
AOS-198121	–	**Symptom:** The default captive portal, server, and WebUI certificates of an Instant AP were about to expire. The fix ensures that the validity of these default certificates is extended to December 2029. **Scenario:** This issue was observed in access points running AOS-W Instant 6.4.4.8-4.2.4.0 or later versions.

Issues Resolved in 6.4.4.8-4.2.4.15

Configuration

Table 7: *Configuration Fixed Issue*

New Bug ID	Old Bug ID	Description
AOS-181492	193906	**Symptom:** A set of pre-defined commands were vulnerable to manipulation by an unauthorized user, as invalid characters were introduced in the URL and process name. The fix ensures that the URL and process name does not contain special characters. **Scenario:** This issue was observed in Instant APs running AOS-W Instant 6.4.4.8-4.2.4.0 or later versions.
AOS-181509	193932	**Symptom:** An Instant AP crashed as some special characters were automatically inserted in the WebUI URL. The fix ensures that the special characters are deleted before the URL is processed. **Scenario:** This issue was observed in Instant APs running AOS-W Instant 6.4.4.8-4.2.4.0 or later versions.
AOS-181515	193975	**Symptom:** An Instant AP crashed unexpectedly. Enhancement to the parsing logic resolved this issue. **Scenario:** This issue occurred because of a memory segmentation error. This issue was observed in Instant APs running AOS-W Instant 6.4.4.8-4.2.4.0 or later versions.

Firewall

Table 8: *Firewall Fixed Issue*

New Bug ID	Old Bug ID	Description
AOS-185676	—	**Symptom:** The bandwidth limit contract was not enforced for clients connected to the WLAN SSID. The fix ensures that the bandwidth limit contract is enforced for clients. **Scenario:** This issue was observed in Instant APs running AOS-W Instant 6.4.4.8-4.2.4.0 or later versions.

WebUI

Table 9: *WebUI Fixed Issue*

New Bug ID	Old Bug ID	Description
AOS-176690	171385	**Symptom:** The old version of the Instant WebUI returned a blank page. The fix ensures that the old version of the WebUI is visible. **Scenario:** This issue was observed in Instant APs running AOS-W Instant 6.4.4.8-4.2.4.0 or later versions.

Issues Resolved in 6.4.4.8-4.2.4.14

Wi-Fi Driver

Table 10: *Wi-Fi Driver Fixed Issue*

Bug ID	Description
AOS-184150	**Symptom:** Clients were unable to detect the 2.4 GHz network broadcasted by an OAW-IAP103. This issue is resolved by a software enhancement that triggers the AP to reboot and work as expected. **Scenario:** This issue occurred due to a clock module flaw in old hardware versions of OAW-IAP103, OAW-IAP108 and OAW-IAP109. This issue was observed in OAW-IAP103 running AOS-W Instant 4.2.4.0 or later versions.

Issues Resolved in 6.4.4.8-4.2.4.13

Configuration

Table 11: *Configuration Fixed Issue*

Bug ID	Description
AOS-182084	**Symptom:** A CLI command parameter sent in the HTTP GET request triggered a crash. This issue is resolved by filtering out the invalid command parameter from the HTTP GET request. **Scenario:** This issue occurred because the command parameter entered was invalid. This issue was observed in Instant APs running Alcatel-Lucent Instant 6.4.2.6-4.1.3.0 or later versions.

Issues Resolved in 6.4.4.8-4.2.4.12

Captive Portal

Table 12: *Captive Portal Fixed Issue*

Bug ID	Description
151119	**Symptom**: Clients were getting stuck on the captive portal authentication page when they use external captive portal over HTTP. The fix ensures that the captive portal authentication is successful. **Scenario**: This issue was observed OAW-IAPs running Alcatel-Lucent Instant 6.4.4.8-4.2.4.3 or later versions.

Mesh

Table 13: *Mesh Fixed Issue*

Bug ID	Description
181972	**Symptom**: Some OAW-IAPs were unable to connect to the network on the 5 GHz radio. The fix ensures that the OAW-IAPs are able to connect to the network on the 5 GHz radio. **Scenario**: This issue was observed OAW-IAPs running Alcatel-Lucent Instant 6.4.4.8-4.2.4.3 or later versions.

VPN

Table 14: *VPN Fixed Issue*

Bug ID	Description
170406 179705	**Symptom**: An OAW-IAP sent traffic from an invalid IP address to a VPN controller. The fix ensures that the OAW-IAP does not send traffic from an invalid IP address. **Scenario**: This issue occurred when the DHCP server was not stable and the OAW-IAP obtained an invalid IP address, like an automatic private IP address. This issue was not limited to a specific OAW-IAP model or Alcatel-Lucent Instant software version.

XML-API

Table 15: *XML-API Fixed Issue*

Bug ID	Description
158869	**Symptom**: XML API did not return calls made through port 443. The fix ensures that calls are successfully made through port 443. **Scenario**: This issue was observed in OAW-IAPs running Alcatel-Lucent Instant 6.5.0.0-4.2.4.3 or later versions.

Issues Resolved in 6.4.4.8-4.2.4.11

VC Management

Table 16: *VC Management Fixed Issue*

Bug ID	Description
152473 174838	**Symptom**: Some slave OAW-IAPs were unable to synchronize configurations from a master OAW-IAP. The fix ensures that the synchronization is successful. **Scenario**: This issue was observed OAW-IAPs running Alcatel-Lucent Instant 6.4.4.6-4.2.4.0 or later versions.

Issues Resolved in 6.4.4.8-4.2.4.10

AppRF

Table 17: *AppRF Fixed Issue*

Bug ID	Description
154245	**Symptom**: The web content classification was incorrect for some sites. Updating the SDK to the latest version resolves this issue. **Scenario**: This issue was not limited to any specific OAW-IAP model or Alcatel-Lucent Instant release version.

Authentication

Table 18: *Authentication Fixed Issue*

Bug ID	Description
144105	**Symptom**: OAW-IAPs sent incorrect details to clients about the RADIUS accounting session time. This issue is resolved by setting the system uptime as the accounting start time. **Scenario**: This issue was observed in OAW-IAPs running Alcatel-Lucent Instant 6.4.4.6-4.2.4.0 or later versions.

Datapath

Table 19: *Datapath Fixed Issue*

Bug ID	Description
170598	**Symptom**: Clients connected to an OAW-IAP through a guest VLAN were unable to obtain the DHCP IP address even after the DHCP helper was configured. The fix ensures that clients are able to obtain the IP address on the OAW-IAP through the guest VLAN. **Scenario**: The issue occurred because DHCP helper was unexpectedly stuck, and was unable to relay DHCP packets to the master OAW-IAP. This issue was observed in OAW-IAPs running Alcatel-Lucent Instant 6.4.4.6-4.2.4.0 or later versions.

Wi-Fi Driver

Table 20: *Wi-Fi Driver Fixed Issue*

Bug ID	Description
156787 170341	**Symptom**: The OAW-IAP management packets were dropped in kernel. The issue is resolved by adding a time gap between creation of radio and creation of virtual access points. **Scenario**: This issue occurred because the radio configuration work queue was scheduled when the virtual access points were not completely registered. This issue was observed in OAW-IAP205 access points running Alcatel-Lucent Instant 6.4.4.6-4.2.4.0 or later versions.

Issues Resolved in 6.4.4.8-4.2.4.9

This release includes fixes for vulnerability documented in:

- WPA2 Key Reinstallation Vulnerabilities - CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13084, CVE-2017-13086, CVE-2017-13087, and CVE-2017-13088.
- Multiple Vulnerabilities in 'dnsmasq' - CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494, CVE-2017-14495, and CVE-2017-14496.

Additionally, the following issues are fixed in the Instant 6.4.4.8-4.2.4.18 release.

AirGroup

Table 21: *AirGroup Fixed Issue*

Bug ID	Description
166285	**Symptom**: Clients were unable to connect to OAW-IAPs. The fix ensures that clients connect to the OAW-IAPs. **Scenario**: The issue occurred because AirGroup cached several TXT records for its servers. This resulted in a high memory utilization. This issue was observed in OAW-IAP205 access points running Instant 6.4.3.1-4.2.0.0 or later versions.

Authentication

Table 22: *Authentication Fixed Issues*

Bug ID	Description
165835	**Symptom**: Captive Portal prompted the clients to re-login although the clients re-connected within the inactivity timeout period. The fix ensures that the clients are not prompted to re-login every time. **Scenario**: This issue was observed in OAW-IAPs running Instant 6.4.4.6-4.2.4.7 or later versions.
165693 166099	**Symptom**: RADIUS authentication failed on some OAW-IAPs because the authentication ports on different OAW-IAPs became inconsistent after the RADIUS server configurations were deleted. The fix ensures that the RADIUS authentication is successful. **Scenario**: The issue occurred only under the following conditions: 1. Dynamic RADIUS Proxy was enabled. 2. RADIUS server configuration was deleted. 3. Some (but not all) OAW-IAPs were reloaded. This issue was not limited to any specific OAW-IAP model or Instant release version.

OmniVista

Table 23: *OmniVista Fixed Issue*

Bug ID	Description
159499	**Symptom**: The output of the **show log provision** command displayed an error message **Unexpected end of XML data, aborting**. The fix ensures that the CLI output does not display the error. **Scenario**: The issue occurred because the size of the provisioning log file was lengthy. This issue was not limited to any OAW-IAP model or Instant release version.

Captive Portal

Table 24: *Captive Portal Fixed Issue*

Bug ID	Description
148645	**Symptom**: The Captive Portal assistance page did not pop up automatically for Samsung devices. This issue is resolved by adding a space in the status line of the HTTP response header. **Scenario**: This issue was not limited to any specific OAW-IAP model or Instant release version.

Configuration

Table 25: *Configuration Fixed Issue*

Bug ID	Description
166938	**Symptom**: OAW-IAPs incorrectly processed XML API requests from port 80. The fix ensures that XML-API requests are processed correctly. **Scenario**: This issue was observed in OAW-IAPs running Instant 6.4.4.6-4.2.4.0 or later versions.

Mesh

Table 26: *Mesh Fixed Issue*

Bug ID	Description
165956	**Symptom**: The mesh link was unstable as de-authentication frames were continuously sent from the mesh portal. The fix ensures that the mesh point entry does not age out frequently. **Scenario**: This issue occurred because the mesh point entry aged out frequently on the mesh portal. This issue was observed in OAW-IAPs running Instant 6.4.4.8-4.2.4.7 or later versions.

Modem

Table 27: *Modem Fixed Issue*

Bug ID	Description
161631	**Symptom**: OAW-IAPs failed to come up when connected to a 4G-LTE modem. The issue is resolved by introducing a support for the secondary access point name of the ISP. **Scenario**: This issue was observed in OAW-IAP215 access points running Instant 6.4.3.1-4.2.0.0 or later versions.

VC Management

Table 28: *VC Management Fixed Issue*

Bug ID	Description
165973	**Symptom**: OAW-IAPs were unable to generate user-debug logs. The issue is resolved by re-enabling the user-debug syslog functionality. **Scenario**: This issue occurred when user-debug was accidentally disabled. This issue was observed in OAW-IAPs running Instant 6.4.4.8-4.2.4.5 release version.

Wi-Fi Driver

Table 29: *Wi-Fi Driver Fixed Issue*

Bug ID	Description
164019 164426 164893 165984 166654 166691	**Symptom**: OAW-IAPs rebooted due to a kernel panic. The log file listed the reason as **Reboot caused by kernel page fault at virtual address 001a000 when 11k enabled**. Improvements to the 802.11k beacon report management resolved this issue. **Scenario**: This issue was observed in OAW-IAP103 and OAW-IAP105 access points and was not limited to specific Instant release versions.

Issues Resolved in 6.4.4.8-4.2.4.8

Platform

Table 30: *Platform Fixed Issues*

Bug ID	Description
159348 159445 159489	**Symptom**: OAW-IAPs failed to respond and rebooted. The log file listed the reason for the event as **Internal watchdog reset**. The fix ensures that the OAW-IAPs run as expected. **Scenario**: This issue occurred because the OAW-IAPs were stuck while dumping the status registers in the L2 cache error handler. This issue was observed in OAW-IAP32x devices running Instant 6.4.4.8-4.2.4.6 or later versions.
161659	**Symptom**: OAW-IAPs became unresponsive to control and management packets due to heavy traffic, and took a long time to recover. Implementation of a more graceful handling of the heavy traffic reduces control or management packet loss as well as recovery time. **Scenario**: This issue occurred in OAW-IAP215 devices under heavy downstream VPN tunnel traffic conditions. This issue was not limited to any specific Instant release version.
162087	**Symptom**: The **SAPD** process consumed a large amount of memory because the memory capping logic in one of the MAC tablets failed to take effect correctly. The issue is resolved by ensuring that memory capping takes effect correctly. **Scenario**: The issue occurred in OAW-IAPs that were installed in large VLANs with more than 250000 MAC addresses. This issue was not limited to any specific OAW-IAP model or Instant release version.

VPN

Table 31: *VPN Fixed Issue*

Bug ID	Description
152838	**Symptom**: High CPU usage was observed in OAW-IAPs due to inefficient error handling in the IPsec cryptographic driver. The fix ensures that error handling is efficient and does not cause high CPU usage. **Scenario**: This issue was observed in OAW-IAP215 devices during heavy downstream IPSEC traffic. This issue was not limited to any specific Instant release version.

Wi-Fi Driver

Table 32: *Wi-Fi Driver Fixed Issue*

Bug ID	Description
141594 142974 144029 145174 145583 148384 149916 153615	**Symptom**: OAW-IAPs crashed and unexpectedly rebooted. The log file listed the reason for the event as **AP rebooted caused by internal watchdog reset**. The issue is resolved by refreshing the watchdog when messages are loaded to the console. **Scenario**: The issue occurred because the hardware watchdog timed out when several messages were loaded to the console. This issue was observed in OAW-IAP32x series devices and was not limited to any specific Instant release version.

Issues Resolved in 6.4.4.8-4.2.4.7

OmniVista

Table 33: *OmniVista Fixed Issue*

Bug ID	Description
153781 155617	**Symptom**: Inactive clients were reported to OmniVista only after a full timeout occurred. The fix ensures that the OAW-IAPs report inactive clients to OmniVista in a timely fashion. **Scenario**: This issue was observed in OAW-IAPs running software versions prior to Instant 6.4.4.8-4.2.4.7.

Authentication

Table 34: *Authentication Fixed Issues*

Bug ID	Description
148031	**Symptom**: When 802.11r was enabled, the client got a wrong role while roaming between OAW-IAPs. This issue is resolved by allowing the 802.11r cache save the role name of the client. **Scenario**: This issue occurred when the client roamed from one OAW-IAP to another with 802.11r enabled. This issue was observed in all OAW-IAPs running software versions prior to Instant 6.4.4.8-4.2.4.7.
155873	**Symptom**: OAW-IAP205 access points were dropping RADIUS frames when the framed MTU was ignored by the RADIUS server. **Scenario**: The frames were getting dropped if the MTU is greater than 1500. This issue was observed in all Instant APs running Instant versions prior to Instant 6.4.4.8-4.2.4.7.
159823	**Symptom**: The Acct-Multi-Session-ID attribute was not unique when the user connects backs quickly after a disconnect. The fix ensures that a unique accounting session ID is generated when the user connects back quickly after a disconnect. **Scenario**: This issue was observed in Instant APs running Instant versions prior to Instant 6.4.4.8-4.2.4.7.
160295	**Symptom**: Zebra Printer QL-220 Plus client was unable to complete EAP-TLS authentication. This issue is fixed by modifying the EAP request period. **Scenario**: This issue occurred due to server timeout. This issue was observed in OAW-IAP215 access points running Instant versions prior to Instant 6.4.4.8-4.2.4.7.

Captive Portal

Table 35: *Captive Portal Fixed Issue*

Bug ID	Description
156360	**Symptom**: Apple users were sometimes not redirected to the ClearPass Guest welcome page after a captive portal authentication was successful. The fix ensures that the clients are redirected to the URL after a captive portal authentication is successful. **Scenario**: This issue occurred because clients used the HTTPS post on Clear Pass Policy Manager. This issue was observed in Instant APs running Instant versions prior to Instant 6.4.4.8-4.2.4.7.

CLI

Table 36: *CLI Fixed Issue*

Bug ID	Description
156295	**Symptom**: The NAS ID was sent with extra double quotes to the RADIUS server. The fix ensures that the NAS ID is not sent with the extra double quotes **Scenario**: This issue occurred when there was a space in the NAS ID string. This issue was observed in Instant APs running Instant versions prior to Instant 6.4.4.8-4.2.4.7.

Datapath/Firewall

Table 37: *Datapath/ Firewall Fixed Issue*

Bug ID	Description
154464	**Symptom**: Continuous packet drops were observed when traffic was sent through the Eth1 port at 100 Mbps. The issue is resolved by enabling flow control inside the ethernet switch clip. **Scenario**: This issue occurred due to the difference in speeds between the uplink and downlink ports. This issue was observed in OAW-IAP205H access points running a software version prior to Instant 6.4.4.8-4.2.4.7.

L3 Mobility

Table 38: *L3 Mobility Fixed Issue*

Bug ID	Description
152688	**Symptom**: Windows clients lost connectivity when they roamed to a different L3 cluster. The fix ensures the client is not disconnected when roaming from one cluster to another. **Scenario**: This issue was observed in OAW-IAPs running software versions prior to Instant 6.4.4.8-4.2.4.7.

Platform

Table 39: *Platform Fixed Issues*

Bug ID	Description
152062	**Symptom**: Some OAW-IAPs randomly rebooted due to a kernel panic. The issue is resolved by adding a crash protection mechanism to the power state code of the OAW-IAP. **Scenario**: This issue occurred within the first few minutes of boot, and was observed in OAW-IAP275 access points running any software version prior to Instant 6.4.4.8-4.2.4.7.
158297	**Symptom**: The ESSID name in DHCP option 82 was missing for some access points. This issue is resolved by making a change in the driver function to display the ESSID. **Scenario**: This issue was observed in Instant access points running Instant versions prior to Instant 6.4.4.8-4.2.4.7.

WebUI

Table 40: *WebUI Fixed Issue*

Bug ID	Description
154558	**Symptom**: Instant WebUI was not loading on the Internet Explorer or Mozilla Firefox browsers if the OAW-IAP name contained special characters. The fix ensures that the Instant WebUI is able to load on the Internet Explorer and Mozilla Firefox browsers. **Scenario**: This issue was observed in OAW-IAPs running software versions prior to Instant 6.4.4.8-4.2.4.7.

Wi-Fi Driver

Table 41: *Wi-Fi Driver Fixed Issue*

Bug ID	Description
159343	**Symptom**: A slave OAW-IAP crashed and rebooted without displaying any reason for the error. The fix ensures that slave OAW-IAPs do not crash without an error. **Scenario**: This issue was observed in OAW-IAP103 access points running software versions prior to Instant 6.4.4.8-4.2.4.7.

Issues Resolved in 6.4.4.8-4.2.4.6

ARM

Table 42: *ARM Fixed Issue*

Bug ID	Description
154557	**Symptom**: AnOAW-IAP103 access point crashed and rebooted unexpectedly. This issue is resolved by fixing the locking issue. **Scenario**: This issue was observed in OAW-IAP103, OAW-IAP215, and OAW-IAP325 devices running a software version prior to Instant 6.4.4.8-4.2.4.6

CLI

Table 43: *CLI Fixed Issue*

Bug ID	Description
154713	**Symptom**: The response for the XML API query did not provide the correct XML API statistics. The fix ensures that the XMI API statics are periodically updated and the response to the XML API query provides the correct information. **Scenario**: This issue was observed in OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.6.

Datapath/Firewall

Table 44: *Datapath/ Firewall Fixed Issues*

Bug ID	Description
146666	**Symptom**: Slave OAW-IAPs connecting to a guest networks were unable to pass traffic. This issue is resolved by programming an ACL for the guest vlan to allow slave OAW-IAPs to successfully connect to the guest network. **Scenario**: This issue was observed in OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.6.
154522	**Symptom**: Clients connected to the master OAW-IAP were unable to resolve the DNS SRV record queries. This issue is resolved by disabling the DNS proxy when Local, L2 is configured as the DHCP scope. **Scenario**: This issue was observed in OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.6.

L2 Mobility

Table 45: *L2 Mobility Fixed Issue*

Bug ID	Description
154328	**Symptom**: The user ID sent for radius accounting was incorrect. The fix ensures that the correct user ID is sent for radius accounting. **Scenario**: This issue occurred when the client roamed from one OAW-IAP to another in the cluster and was observed in OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.6.

Other

Table 46: *Other Fixed Issue*

Bug ID	Description
152060	**Symptom**: A vulnerability scan performed on the OAW-IAP cluster indicated the Dropbear SSH Server had multiple vulnerabilities. This issue is resolved by upgrading to a higher Dropbear firmware. **Scenario**: This issue was observed in OAW-IAP105 access points running a software version prior to Instant 6.4.4.8-4.2.4.6.

Platform

Table 47: *Platform Fixed Issue*

Bug ID	Description
156718	**Symptom**: An OAW-IAP access point crashed after deny-inter-user-bridging was configured. This issue is resolved by running a check for valid destination. **Scenario**: This issue occurred when the p->gress is assigned to an incorrect VLAN. This issue was observed in OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.6.

SNMP

Table 48: *SNMP Fixed Issue*

Bug ID	Description
155081	**Symptom**: The **SNMP** process displayed an error - **OID not increasing**, when clients had a MAC address ending with **FF**. The fix ensures that the packets of clients having MAC address ending with FF are forwarded to the next node. **Scenario**: This issue occurred when the **SNMP** process used MAC address plus 1 and vlan to search for the node. When the client had a MAC address ending with FF, the **SNMP** process used the MAC address ending with FF and vlan to search for the next node, which resulted in an infinite loop. This issue was observed in OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.6.

UI

Table 49: *UI Fixed Issues*

Bug ID	Description
126705	**Symptom**: The password fields within the virtual controller were not encrypted. The fix ensures that the password fields are encrypted and does not display the actual password text. **Scenario**: This issue was observed in OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.6.
151749	**Symptom**: The WPA Enterprise AES setting was not available in the Instant UI. This issue is resolved by adding a new field in the UI for the AES setting. **Scenario**: This issue was observed in OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.6.

VC Platform

Table 50: *VC Platform Fixed Issue*

Bug ID	Description
151541	**Symptom**: In a hierarchical cluster with PPPoE uplink, the slave OAW-RAP was dropping DHCP requests. The fix ensures that the DHCP requests are handled as expected. **Scenario**: This issue was observed in RAP-3 running a software version prior to Instant 6.4.4.8-4.2.4.6.

Wi-Fi Driver

Table 51: *Wi-Fi Driver Fixed Issues*

Bug ID	Description
118039 156391	**Symptom**: An OAW-IAP275 access point rebooted due to an out of memory issue. The fix ensures that the MAC returns to normal functionality when it goes into the suspended state. **Scenario**: The issue occurred when the radio channel was changed and the MAC was pushed to a suspended state for a short duration. This issue was observed in OAW-IAP275 access points running a software version prior to Instant 6.4.4.8-4.2.4.6.
154237	**Symptom**: An OAW-IAP crashed and rebooted unexpectedly. The fix ensures that the OAW-IAP does not crash due to kernel panic. **Scenario**: This issue occurred as the OAW-IAP experienced a kernel panic due to softlockup hung tasks. This issue was observed in OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.6.
154370	**Symptom**: Motorola handheld scanners connected to OAW-IAP325 access points were getting disconnected every 10 seconds. This issue is resolved by making a change to the default CCA threshold value. **Scenario**: This issue was observed in OAW-IAP325 access points running a software version prior to Instant 6.4.4.8-4.2.4.6.

Issues Resolved in 6.4.4.8-4.2.4.5

AppRF

Table 52: *AppRF Fixed Issue*

Bug ID	Description
147010	**Symptom**: Skype for Business sessions marked with SESSION_FLAG_ALG flag which are not skipped or deleted for stale session entries. The fix ensures that the session entries are skipped if the entries are stale and ALG is set. **Scenario**: This issue was observed in access points running a software version prior to Instant 6.4.4.8-4.2.4.5.

Datapath/Firewall

Table 53: *Platform Fixed Issue*

Bug ID	Description
152782	**Symptom**: OAW-IAP275 was booting up with restriction mode on the Cisco 2960 switch if the native VLAN on the switch port is not 1.This issue is resolved by updating the socket binding protocol for LLDP packets. **Scenario**: This issue was observed in OAW-IAP275 access points running a software version prior to Instant 6.4.4.8-4.2.4.5.

Mesh

Table 54: *Mesh Fixed Issue*

Bug ID	Description
145637	**Symptom**: OAW-IAP225 was running into a network loop when the uplink was restored and mesh was enabled. The fix ensures that the network looping issue is resolved. **Scenario**: This issue was observed in OAW-IAP225 access points running a software version prior to Instant 6.4.4.8-4.2.4.5.

Platform

Table 55: *Platform Fixed Issues*

Bug ID	Description
154509 127848	**Symptom**: An OAW-IAP crashed unexpectedly when using Huawei E353 modem. The log file of the event listed the reason as **Reboot caused by kernel panic: Fatal exception**. The fix ensures that the OAW-IAP does not crash unexpectedly **Scenario**: This issue was observed in OAW-IAP205H access points running a software version prior to Instant 6.4.4.8-4.2.4.5.
145634	**Symptom**: An OAW-IAP crashed unexpectedly when using 10Mbps half-duplex uplink and upstream traffic exceed 10Mbps. The log file of the event listed the reason as kernel panic. The fix ensures that the OAW-IAP works without kernel panic with same uplink. **Scenario**: This issue was observed in OAW-IAP215 and OAW-IAP225 access points running a software version prior to Instant 6.4.4.8-4.2.4.5.
144570	**Symptom**: An OAW-IAP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt**. This issue is resolved by directly accessing the saved context data when crypto context is cleared. **Scenario**: This issue occurred when IPsec tunnels were closed and the queued crypto context was cleared. This issue was observed in 200, 210, and 220 series OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.5.
152840	**Symptom**: An OAW-IAP crashed and rebooted unexpectedly due to kernel panic. The fix ensures that the OAW-IAP does not crash unexpectedly. **Scenario**: This issue occurred when large size packets were sent from Centralized, L2 IPsec clients during an IPsec rekey operation. This issue was observed in OAW-IAP215 access points running a software version prior to Instant 6.4.4.8-4.2.4.5.

VPN

Table 56: *VPN Fixed Issue*

Bug ID	Description
149319	**Symptom**: Traffic sent to the corporate network was getting blocked when the volume of the traffic was heavy during IPsec SA rekey. The fix ensures that the IPsec tunnel device remains active when IPsec SA rekey is done. **Scenario**: This issue occurred during IPsec SA rekey and heavy traffic was sent to the corporate network through the IPsec tunnel. This issue was observed in OAW-IAP215 access points running a software version prior to Instant 6.4.4.8-4.2.4.5.

Wi-Fi Driver

Table 57: *Wi-Fi Driver Fixed Issue*

Bug ID	Description
151995	**Symptom**: An OAW-IAP crashed and rebooted with the reason: Reboot caused by kernel panic: Fatal exception. The fix ensures that the OAW-IAP does not crash during compiler optimization. **Scenario**: This issue occurred when the compiler optimization was in progress and was observed in OAW-IAP215 access points running a software version prior to Instant 6.4.4.8-4.2.4.5.

Issues Resolved in 6.4.4.8-4.2.4.4

AppRF

Table 58: *AppRF Fixed Issues*

Bug ID	Description
139336 138868	**Symptom**: Whatsapp traffic was not blocked by the OAW-IAP although the deny ACL was applied. The fix ensures that the blocked whatsapp traffic is not allowed by the OAW-IAP. **Scenario**: The WhatsApp traffic block was not functional as the latest version of WhatsApp was not classified as WhatsApp in the OAW-IAP. This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.4.
141891 142278 141898	**Symptom**: Some OAW-IAPs in the cluster were unable to pass traffic. This issue is resolved by introducing a mechanism to monitor and limiting the AppRF process memory. **Scenario**: The memory utilization on the affected OAW-IAPs was very high. This issue was observed on all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.4.

CLI

Table 59: *CLI Fixed Issue*

Bug ID	Description
151137	**Symptom**: The CLI for anOAW-IAP205 access point crashed and began generating multiple core files. This issue is resolved by making a change to the function used in the OAW-IAP code. **Scenario**: This issue was observed in OAW-IAP205 access points running a software version prior to Instant 6.4.4.8-4.2.4.4.

Configuration

Table 60: *Configuration Fixed Issue*

Bug ID	Description
145050 149491 149515	**Symptom**: The syslog messages from the OAW-IAP indicated a configuration mismatch between the VC and the slave OAW-IAPs in a cluster. This issue is resolved by initiating the enet-vlan configuration when the OAW-IAP restarts. **Scenario**: This issue occurred when mesh point was configured on the OAW-IAP and enet-vlan configuration was removed from the master OAW-IAP. This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.4.

Datapath/Firewall

Table 61: *Platform Fixed Issues*

Bug ID	Description
135764	**Symptom**: OAW-IAPs operating on Instant 6.4.3.4-4.2.1.2 crashed and rebooted with the reboot reason: **Reboot caused by kernel panic: assert.** The fix resolves the kernel panic issue. **Scenario**: This issue was observed in OAW-IAP205 access points running Instant 6.4.3.4-4.2.1.2 and later versions.
151748	**Symptom**: An OAW-IAP crashed and rebooted unexpectedly. The log file for the event listed the reason as **Reboot caused by kernel panic: softlockup: hung tasks**. This fix ensures that the deadlock issue causing the crash is resolved. **Scenario**: This issue occurred due a deadlock caused by a recursive lock on the anul lock function running on the CPU. This issue was observed in OAW-IAP325 access points running a software version prior to Instant 6.4.4.8-4.2.4.4.

GRE

Table 62: *GRE Fixed Issue*

Bug ID	Description
151725 152539 152619	**Symptom**: An OAW-IAP was using unfixed MTU than the specified MTU for GRE fragmentation. This resulted in packets fragmented with a different size which may cause possible loss during the transmission. The fix ensures that the OAW-IAP uses the specified MTU value for GRE fragmentation. **Scenario**: This issue was observed in OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.4.

Platform

Table 63: *Platform Fixed Issue*

Bug ID	Description
146564 149935	**Symptom**: The LLDP process in an OAW-IAP was unable to negotiate high power, shut down the wrong Ethernet port, and did not enable the radios. The fix ensures that the LLDP process in an OAW-IAP works correctly when both Ethernet ports are used. **Scenario**: This issue occurred when both Ethernet ports of an OAW-IAP were in use and connected to PoE+ power sources (which are reliant on LLDP protocol to provide high power). This issue was observed in OAW-IAP325 access points running a software version prior to Instant 6.4.4.8-4.2.4.4.

Wi-Fi Driver

Table 64: *Wi-Fi Driver Fixed Issues*

Bug ID	Description
147682 147681	**Symptom**: A slave OAW-IAP incorrectly classified another OAW-IAP belonging to the same cluster as a rogue OAW-IAP. The fix ensures that the OAW-IAPs can correct the wrong entry in very short time. **Scenario**: This issue occurred as the slave OAW-IAP lost the messages of the updated MAC address list from the VC. This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.4.
141429	**Symptom**: Access points crashed and rebooted. The log file for the event listed the reason as **Reboot caused by out of memory**. The fix ensures that the issue with the memory is resolved. **Scenario**: This issue was observed in all OAW-IAP2xx series access points running a software version prior to Instant 6.4.4.8-4.2.4.4.
145852 152810	**Symptom**: An OAW-IAP crashed and rebooted unexpectedly. The log file for the event listed the reason as **Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT**. This issue is resolved by checking incoming packets and dropping packets correctly. **Scenario**: This issue was observed in OAW-IAP325 access points running a software version prior to Instant 6.4.4.8-4.2.4.4.
150704	**Symptom**: OAW-IAP did not send all the interference SSID details to OmniVista. This issue is resolved by extending the maximum number of entries in the IDS table to 2048. **Scenario**: This issue occurred as the IDS table was full and was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.4.
151866	**Symptom**: Laptops running a Windows 7 64-bit OS were experiencing crashes when using Intel wireless chipset Dual Band Wireless-AC 7265 or Dual Band Wireless-AC 8260. This issue is resolved by setting the right value for the beacon interval. **Scenario**: This issue occurred as the default value of the beacon interval was altered and was observed in OAW-IAP325 access points running a software version prior to Instant 6.4.4.8-4.2.4.4.

Issues Resolved in 6.4.4.8-4.2.4.3

OmniVista

Table 65: *OmniVista Fixed Issue*

Bug ID	Description
150262	**Symptom**: Configuration changes made on the OAW-IAP through the CLI, UI, or AMP were not recorded in the syslog by default. The fix ensures that the syslog message is generated when the configuration is changed. **Scenario**: This issue occurred as the syslog level for a configuration was lower than the OAW-IAPs default syslog level. This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.3.

Authentication

Table 66: *Authentication Fixed Issues*

Bug ID	Description
147169	**Symptom**: The RADIUS server rejected successive authentication requests from the OAW-IAP. The fix ensures that the RADIUS authentication requests are handled successfully. **Scenario**: This issue occurred due to duplicate RADIUS session IDs and was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.3.
148693	**Symptom**: The browser kept displaying a warning or an error claiming the securelogin.arubanetworks.com certificate had been revoked, causing disruption to the captive portal work flow of the OAW-IAP. As a fix to this issue, the securelogin.arubanetworks.com certificate has been replaced by a different certificate for which the browser may only have warnings and not errors. However, the best practice is for customers to upload their own publically signed certificate instead of relying on the default securelogin.arubanetworks.com certificate. **Scenario**: This issue impacted all scenarios where captive portal is used and was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.3.

Platform

Table 67: *Platform Fixed Issue*

Bug ID	Description
147826	**Symptom**: OAW-IAP325 access points crashed and rebooted with a reason: **Reboot caused by kernel panic: Fatal exception.** The fix ensures that the duplicate entries are not added to the subnet table. **Scenario**: This issue occurred due to duplicate entries in the subnet table and was observed in OAW-IAP325 access points running a software version prior to Instant 6.4.4.8-4.2.4.3.

VC Management

Table 68: *VC Management Fixed Issue*

Bug ID	Description
146606	**Symptom**: Some OAW-IAPs were intermittently getting disconnected from the cluster. The fix resolves the out of memory issue that caused the OAW-IAPs to disconnect from the cluster. **Scenario**: This issue occurred when a large amount of ARP frames were sent through the wired network and resulted in the datapath running out of memory space. This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.3.

VPN

Table 69: *VPN Fixed Issue*

Bug ID	Description
144326 148161	**Symptom**: When one OAW-IAP used another OAW-IAP as an uplink, the OAW-IAP was unable to re-establish a VPN connection if its VPN session was SRC-NAT'ted at the uplink OAW-IAP. The fix ensures that the OAW-IAPs can successfully reconnect to the VPN. **Scenario**: This issue occurred as the old VPN session was still active on the uplink OAW-IAP and was observed in OAW-IAP324/325, OAW-IAP205/205H access points running a software version prior to Instant 6.4.4.8-4.2.4.3.

Wi-Fi Driver

Table 70: *Wi-Fi Driver Fixed Issues*

Bug ID	Description
147682	**Symptom**: A slave OAW-IAP incorrectly classified another OAW-IAP belonging to the same cluster as a rogue OAW-IAP. The fix ensures that the OAW-IAPs can correct the wrong entry in very short time. **Scenario**: This issue occurred as the slave OAW-IAP lost the messages of the updated MAC address list from the VC. This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.3.
140337 141943 145917 146032	**Symptom**: AnOAW-IAP325 access point rebooted due to FW assert while running multicast traffic for a long period of time. This issue is resolved by improving the checking mechanism for the Tx buffer getting stuck. **Scenario**: This issue was observed in OAW-IAP325 access points running a software version prior to Instant 6.4.4.8-4.2.4.3.
141239 148412	**Symptom**: Motorola MC75A0 handheld scanners were unable to associate to OAW-IAP325 access points. This fix ensures that the Motorola MC75A0 handheld scanner is able to connect to the OAW-IAP325 access point. **Scenario**: This issue occurred when the client always sent a deauthentication message before sending the authentication message to the OAW-IAP. Also, the OAW-IAP sent a deauthentication message to the client after receiving an association request. This issue was observed in OAW-IAP325 access points running a software version prior to Instant 6.4.4.8-4.2.4.3.
138637	**Symptom**: Frames with VLAN 0 were dropped and not retransmitted over the air. The fix ensures that frames with VLAN ID 0 are not dropped. **Scenario**: This issue was observed in OAW-IAP275 access points running a software version prior to Instant 6.4.4.8-4.2.4.3.

Issues Resolved in 6.4.4.8-4.2.4.2

ALE

Table 71: *ALE Fixed Issue*

Bug ID	Description
145729	**Symptom**: The **Age** field in the RSSI client message was not accurate. The issue is resolved by changing the calculation logic of the field. **Scenario**: This issue affected deployments in which OAW-IAPs were being used in combination with the ALE server for location-based services, resulting in inaccurate location calculations of the ALE server. This issue was observed in all the OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.2.

CLI

Table 72: *CLI Fixed Issue*

Bug ID	Description
144944	**Symptom**: The VPN routing profile of an OAW-IAP accepted invalid entries during CLI configuration. The issue is resolved by running a check on the CLI parameters, so that the OAW-IAP displays an error message when the users enter invalid parameters. **Scenario**: This issue was observed when the IAP-VPN profile accepted values such as ASCII and special characters without displaying an error message in the CLI. This issue was not limited to a specific OAW-IAP model or Instant software version.

Datapath/Firewall

Table 73: *Datapath/Firewall Fixed Issues*

Bug ID	Description
139022	**Symptom**: OAW-IAPs crashed and rebooted while receiving certain multicast packets from the SSID profile. The fix ensures that OAW-IAPs do not crash while receiving the multicast packets. **Scenario**: This issue was found in OAW-IAPs with the Dynamic Multicast Optimization (DMO) feature enabled. This issue was observed in OAW-IAP325 access points running Instant 6.4.4.3-4.2.2.0 and later releases.
146155	**Symptom**: When the SSID, WLAN access rule, and user-defined Src-NAT rule were in use, the bandwidth control did not have any effect on the clients associated to slave OAW-IAPs. The issue is resolved by changing the bandwidth control logic of the OAW-IAPs. **Scenario**: This issue was observed in all the OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.2.

Platform

Table 74: *Platform Fixed Issue*

Bug ID	Description
145808 136228	**Symptom**: OAW-IAPs in a cluster rebooted as they were running out of memory. The fix ensures that OAW-IAPs use the memory space appropriately. **Scenario**: This issue was observed in OAW-IAP205 and OAW-IAP275 access points running a software version prior to Instant 6.4.4.8-4.2.4.2.

PPPoE

Table 75: *PPPoE Fixed Issue*

Bug ID	Description
140549	**Symptom**: PPPoE session was not working when the uplink port of an OAW-IAP was fluctuating. The fix ensures that PPPoE works even when there are multiple fluctuations at the uplink port of the OAW-IAP. **Scenario**: This issue was observed in all the OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.2.

Wi-Fi Driver

Table 76: *Wi-Fi Driver Fixed Issue*

Bug ID	Description
132990	**Symptom**: Wireless services were unstable when the Ethernet port of the OAW-RAP109 access point was fluctuating. The fix ensures that clients receive stable wireless services from the OAW-RAP. **Scenario**: This issue was observed in OAW-RAP109 access points running a software version prior to Instant 6.4.4.8-4.2.4.2.

3G/4G Management

Table 77: *3G/4G Management Fixed Issue*

Bug ID	Description
142944	**Symptom**: A 320U 4G modem was not working when connected to an OAW-IAP. This issue is resolved by a change in condition to match the module name of the modem. **Scenario**: This issue was observed in 320U modems connected to OAW-RAP155 access points running a software version prior to Instant 6.4.4.8-4.2.4.2.

Issues Resolved in 6.4.4.8-4.2.4.1

OmniVista

Table 78: *OmniVista Fixed Issue*

Bug ID	Description
140313	**Symptom**: OmniVista managing OAW-IAPs did not display some of the interfering OAW-IAPs. The fix ensures that the interfering OAW-IAPs are displayed on OmniVista. **Scenario**: This issue occurred when a large number of interfering OAW-IAPs were present in the same physical area of the WLAN network. This issue was not limited to a specific OAW-IAP model or Instant software version.

AppRF

Table 79: *AppRF Fixed Issue*

Bug ID	Description
143257	**Symptom**: DPIMGR trace logging spiked memory usage on the OAW-IAP. This issue is resolved by moving the syslog message from error log to debug level. **Scenario**: This issue occurred when the brightcloud DNS resolve process started before trace logging of DPIMGR, which triggered default trace logging to grow and caused memory spike in OAW-IAPs running Instant 6.4.4.4-4.2.3.0 and later versions.

Datapath/Firewall

Table 80: *Datapath/Firewall Fixed Issues*

Bug ID	Description
138649	**Symptom**: OAW-IAP225 access points crashed and rebooted with the reason: **Reboot caused by kernel panic: Fatal exception in interrupt.** This issue is resolved by preventing the watchdog timer from getting triggered when the bridge entries are deleted. **Scenario**: The watchdog timer was triggered when the bridge entries were deleted. This issue was observed in OAW-IAP225 access points running a software version prior to Instant 6.4.4.8-4.2.4.1.
143390	**Symptom**: Clients connecting to OAW-RAP109 using a 3G or 4G uplink were unable to get an IP address from all Ethernet ports with enet0-bridging enabled. This issue is resolved by bringing up the br0 port when enet0-bridging is enabled. **Scenario**: The br0 port is down when enet0-bridging is enabled. This issue was observed in OAW-RAP109 access points running a software version prior to Instant 6.4.4.8-4.2.4.1.
144543	**Symptom**: Apple devices connected to the slave OAW-IAPs via the guest VLAN were intermittently losing connectivity to the network. The fix ensures that the Apple devices are able to connect to the network without intermittency issues. **Scenario**: This issue was observed in all OAW-IAPs running Instant 6.4.4.4-4.2.3.0 and later versions.

SNMP

Table 81: *SNMP Fixed Issue*

Bug ID	Description
140180	**Symptom**: The Object aiRadioStatus value was always 1 irrespective of the radio status. The fix ensures that the Object aiRadioStatus is 0 when the radio is disabled and 1 when the radio is enabled. However, when mesh is enabled on the OAW-IAP, the object aiRadioStatus will be 1 even when the radio is disabled. **Scenario**: This issue was not limited to a specific OAW-IAP model or Instant software version.

STM

Table 82: *STM Fixed Issue*

Bug ID	Description
136795	**Symptom**: STM core files were found in several OAW-IAPs as a result of the memory being cleared twice. This issue is resolved by preventing the memory from being cleared twice when the auth-server ip address is changed. **Scenario**: This issue occurred when multiple OAW-IAPs were used and DRP was enabled on the SSID profile. This issue was not limited to a specific OAW-IAP model or Instant software version.

UI

Table 83: *UI Fixed Issues*

Bug ID	Description
137227	**Symptom**: Users were getting an error message when they tried logging in to the OAW-IAP UI using Internet Explorer 11. The warning message has been removed to resolve this issue. **Scenario**: This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.1.
140803	**Symptom**: One of the ACL parameters was incorrectly displaying as **scanning activieren** instead of **scanning deaktivieren** in the German version of the OAW-IAP UI. **Scenario**: This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.1.

Wi-Fi Driver

Table 84: *Wi-Fi Driver Fixed Issue*

Bug ID	Description
129829	**Symptom**: External wi-fi devices were intermittently not displayed in the IDS table after they were re-classified as valid. The fix ensures that the external wi-fi devices are displayed in the IDS table until the device entry expires. **Scenario**: This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.1.

Issues Resolved in 6.4.4.6-4.2.4.0

AirGroup

Table 85: *AirGroup Fixed Issue*

Bug ID	Description
139943	**Symptom**: AirPrint information was not getting displayed on the AirGroup server list of the OAW-IAP. This issue is resolved by a change in code that records the response sent to the OAW-IAP query. **Scenario**: This issue was observed in OAW-IAP205 devices running a software version prior to Instant 6.4.4.6-4.2.4.0.

OmniVista

Table 86: *OmniVista Fixed Issue*

Bug ID	Description
136986	**Symptom**: OAW-IAPs were sending the tx power and channel information to OmniVista ven when the 2.4 GHz and 5 GHz radios were disabled. The fix ensures the OAW-IAP does not report the tx power, radio channel, noise floor, and channel busy values to OmniVista when the radios are disabled. **Scenario**: This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.6-4.2.4.0.

Authentication

Table 87: *Authentication Fixed Issue*

140091 144445	**Symptom**: Clients were unable to pass WPA2 validation with a specific passphrase. The fix ensures client can connect to the OAW-IAP WPA2 SSID with the specified passphrase. **Scenario**: This issue occurred as the OAW-IAP failed to accept the WPA2 passphrase SSID format. This issue was observed in OAW-IAPs running Instant 6.4.3.1-4.2.0.0 or later versions.

ARM

Table 88: *ARM Fixed Issue*

Bug ID	Description
139165	**Symptom**: The 2.4 GHz channels were disabled in OAW-IAPs that support the Nigerian country code. The issue is resolved by removing the code that is used to validate DRT content of the OAW-IAP. **Scenario**: This issue was observed in OAW-IAP205 devices running a software version prior to Instant 6.4.4.6-4.2.4.0.

Datapath/Firewall

Table 89: *Datapath/Firewall Fixed Issues*

Bug ID	Description
138095	**Symptom**: After upgrading the software version from Instant 6.4.2.6-4.1.1.6 to 6.4.3.4-4.2.1.0, MAC users were experiencing delays in connecting to the network. The fix ensures that the users are able to connect to the network without delay. **Scenario**: This issue occurred as there was a delay in receiving the DHCP IP address from the server and was observed in all OAW-IAPs running Instant 6.4.3.4-4.2.1.0 and later versions.
136169	**Symptom**: Some clients were getting a higher bandwidth than the allocated limit. The fix ensures that the bandwidth does not exceed the allocated limit. **Scenario**: This issue occurred as the bandwidth contract for some of the OAW-IAPs in the cluster was not taking effect correctly. This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.6-4.2.4.0.

Hotspot 2.0

Table 90: *Hotspot 2.0 Fixed Issues*

Bug ID	Description
139116	**Symptom**: OAW-IAPs failed to send 3GPP-PLMN values in the ANQP response frame. The fix ensures that correct values for the 3GPP-PLMN element are sent by the OAW-IAP. **Scenario**: This issue was observed in OAW-IAP205H access points running Instant 6.4.4.4-4.2.3.0 and later versions.
138670	**Symptom**: Clients failed to automatically connect to OAW-IAPs even after the hotspot feature was configured in the OAW-IAPs. The fix ensures that an automatic connection between the hotspot clients and OAW-IAPs is successful. **Scenario**: This issue occurred as the OAW-IAPs were not adding hotspot information elements into the beacon. This issue was observed in OAW-IAPs running Instant 6.4.3.4-4.2.1.0 and later versions.

L2/L3 Mobility

Table 91: *L2/L3 Mobility Fixed Issue*

Bug ID	Description
137726	**Symptom**: Clients were unable to pass traffic after successfully roaming from one OAW-IAP to another in the cluster. This issue is resolved by making a change in the code to use the client information in the user path when programming the user entry for the home OAW-IAP. **Scenario**: This issue occurred as the user entry was cleared from the home OAW-IAP when the client roamed from one OAW-IAP to another in the network and was not limited to a specific OAW-IAP model or software version.

Platform

Table 92: *Platform Fixed Issues*

Bug ID	Description
140867	**Symptom**: When clients upgraded an OAW-IAP, the RTLS server displayed an error message. This issue is resolved by enabling the server compatibility settings of the RTLS server. **Scenario**: This issue was observed in OAW-IAP103 access points running a software version prior to Instant 6.4.4.6-4.2.4.0.
142400	**Symptom**: OAW-IAPs were continuously crashing every 2 to 3 minutes, causing productivity issues with the clients. This issue is resolved by introducing a mechanism to lock the bridge entry of the OAW-IAP. **Scenario**: This issue occurred due to a kernel panic in the OAW-IAP code, resulting in continuous rebooting of the OAW-IAPs. This issue was observed in OAW-IAP325 access points running Instant 6.4.4.4-4.2.3.0 and later versions.
135787	**Symptom**: When a multicast server tried to send a file to the client through an OAW-IAP, the client failed to receive the entire file. This issue is resolved by applying a condition to verify the DHCP/DNS packets. **Scenario**: This issue occurred when the OAW-IAPs dropped a section of the fragmented packets during file transfer. This issue was observed in OAW-IAPs running a software version prior to Instant 6.4.4.6-4.2.4.0.
137637	**Symptom**: OAW-IAP225 devices crashed and rebooted with a response: Reboot caused by Kernel panic: asset. This issue is resolved by removing the L3 mobility tunnel creation for the CL2 VLAN. **Scenario**: This issue occurred as the memory space was low and was observed in all OAW-IAP running a software version prior to Instant 6.4.4.6-4.2.4.0.

3G/4G Management

Table 93: *3G/4G Management Fixed Issue*

Bug ID	Description
137180	**Symptom**: Clients using Windows laptops and mobile devices were unable to access certain websites while being connected to an OAW-IAP. The issue is resolved by checking and updating the MSS value of the TCP packets that are received from the OAW-IAP. **Scenario**: This issue was observed in all OAW-IAPs running Instant 6.4.3.1-4.2.0.0 and later versions.

UI

Table 94: *UI Fixed Issues*

Bug ID	Description
140506	**Symptom**: The following error was displayed when the user tried to create a periodic time-based service profile using a certain condition: **End day must be later than start day**. This issue is resolved by changing the code for validating when a time-based service profile is created. **Scenario**: This issue was observed in all OAW-IAPs running Instant 6.4.4.4-4.2.3.1 and later versions.
141593	**Symptom**: The column under the **RF Dashboard** that displays the signal strength of the OAW-IAP clients was missing in the Instant UI. The fix ensures that the signal strength of the clients is displayed in the UI. **Scenario**: This issue was observed in all OAW-IAPs running Instant 6.4.4.4-4.2.3.0.
141757	**Symptom**: OAW-IAP clients were still active even after they were manually disconnected using the Instant UI. The fix ensures that the manual disconnect of clients using the UI is successful. **Scenario**: This issue occurred as the information and the status of the client was not erased when the disconnect operation was performed using the UI. This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.6-4.2.4.0.

VC Management

Table 95: *VC Management Fixed Issue*

Bug ID	Description
138089	**Symptom**: OAW-IAPs were experiencing a delay in establishing a connection with the SSH server when the reverse dns lookup failed. This issue is resolved by preventing the SSH server from performing a reverse dns lookup, to avoid the delay prior to establishing a connection with the OAW-IAP. **Scenario**: The issue occurred due to multiple retry attempts by the SSH server to perform a reverse dns lookup before establishing a connection with the OAW-IAP. This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.6-4.2.4.0.

VPN

Table 96: *VPN Fixed Issues*

Bug ID	Description
132490	**Symptom**: In a Distributed L3 network, windows clients were unable to open a few sites when connected to the wired network of the OAW-IAP. This issue is resolved by enabling MSS clamping in the upstream direction. **Scenario**: The issue occurred as the MSS clamping was enabled only in the downstream direction for the Distributed L3 clients. This issue was not limited to a specific OAW-IAP model or software version.
138468	**Symptom**: OAW-IAP clients were unable to connect to the corporate network. This issue is resolved by ensuring that the master OAW-IAPs receive the correct DHCP IP subnets from the VPN tunnel in the corporate network. **Scenario**: The issue was observed in all OAW-IAPs running Instant 6.4.3.4-4.2.1.0 and later versions.

Wi-Fi Driver

Table 97: *Wi-Fi Driver Fixed Issue*

Bug ID	Description
138582	**Symptom**: Clients were unable to connect to the 5 GHZ radio channel and the error logs revealed there were TX Radio and Antenna probe failures. The fix ensures the clients are now able to connect to the 5 GHz radio channel without errors. **Scenario**: This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.6-4.2.4.0.