AOS-W Instant 6.3.1.2-4.0.0.2

Release Notes

AOS-W Instant 6.3.1.2-4.0.0.2 is a software patch release that introduces enhancements and fixes to the issues detected in the previous releases of AOS-W Instant.

For more information on features described in the following sections, see the *AOS-W Instant 6.3.1.1-4.0 User Guide*.

Contents

Contacting Support

Table 1: *Contact Information*

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

This chapter provides information on the enhancements and issues fixed in this release of AOS-W Instant.

Enhancements

The following enhancements are introduced in the current patch release.

Automatic Negotiation Support for Authentication between OAW-IAP and OmniVista Management Platform

To establish a connection with the OmniVista management server, the OAW-IAP authenticates to the OmniVista server by using a certificate-based authentication model or the PSK login model. OmniVista management platform supports PSK only, Certificate only, or both PSK and certificate-based authentication models. In the 6.3.1.2-4.0.0.2 release, an automatic negotiation mechanism is introduced for authentication between OAW-IAP and OmniVista management server, irrespective of the authentication model used.

PPPoE Configuration

You can now configure up to 80 characters for a user name, service name, password, and the secret key for CHAP authentication.

To configure PPPoE details:

- In the AOS-W Instant UI, navigate to **System**>**Uplink**. Under PPPoE, specify the required values for **User**, **Service name**, **Password**, and **CHAP secret** fields.
- In the AOS-W Instant CLI, use the **pppoe-username**, **pppoe-chapsecret**, **pppoe-passwd**, and **pppoe-svcname** commands in the PPPoE configuration mode.

Support for VPN Tunnel States and Statistics Reporting from an OAW-IAP

In the earlier releases, in an IAP-VPN network, the switch behind the OAW-IAP was sending information on the VPN tunnel status to the OmniVista management server. In thethe 6.3.1.2-4.0.0.2 release, an enhancement has been introduced to allow the OAW-IAP to send a report on the VPN tunnel states and statistics directly to the OmniVista server.

Resolved Issues in this Release

The following issues are fixed in this patch release.

ARM

Table 2: *ARM Fixed Issue*

Bug ID	Description
90503	**Symptom**: The radios on an OAW-IAP were continuously getting reset. A potential fix has been in implemented in the ARM algorithm to measure the channel quality and switching to better channel in environments when interfering devices are randomly turned on and off. **Scenario**: The issue occurred when interfering devices such as Drive-Thru Headset Systems HME-37R03939 were present in the same channel as that of AP. The AP was not able to detect and change the channel based on the randomly used RF-interfering devices. This issue was found in OAW-IAPs running AOS-W Instant 6.2.1.0-3.4 or later versions.

Firewall

Table 3: *Firewall Fixed Issue*

Bug ID	Description
94162	**Symptom**: When **Drop bad ARP** was enabled, clients could not reconnect to the network. This issue is resolved by allowing the ARP packets to pass. **Scenario**: This issue occurred when the **Drop bad ARP** option in the **Security**>**Firewall Setting** window was enabled. This issue was found in OAW-IAPs running AOS-W Instant 6.3.1.1-4.0.0.0 and 6.3.1.1-4.0.0.1.

IDS

Table 4: *IDS Fixed Issue*

Bug ID	Description
93778	**Symptom**: A syslog message was not generated when a rogue AP was detected in the network. The OAW-IAPs now generates syslog message (with 106000 as the message ID) when a rogue AP is detected. **Scenario**: This issue was found in OAW-IAPs running AOS-W Instant 6.3.1.1-4.0.0.1 or earlier versions.

OmniVista

Table 5: *OmniVista Fixed Issue*

Bug ID	Description
93909	**Symptom**: The AOS-W Instant UI allowed double byte characters for the organization string configured for the OmniVista management console login. The UI now allows only the ASCII characters in the organization string. **Scenario**: This issue was found in OAW-IAPs running AOS-W Instant 6.3.1.1-4.0.0.0 or later versions.

SNMP

Table 6: *SNMP Fixed Issue*

Bug ID	Description
94307	**Symptom**: The ColdStart or WarmStart traps were not generated after an OAW-IAP boot or reload. To resolve this issue, upgrade to AOS-W Instant 6.3.1.2-4.0.0.2. **Scenario**: This issue was found in OAW-IAPs running AOS-W Instant 6.3.1.1-4.0.0.0 and 6.3.1.1-4.0.0.1.

Uplink Management

Table 7: *Uplink Management Fixed Issue*

Bug ID	Description
94467	**Symptom**: Users could not configure uplink VLAN through the AOS-W Instant CLI. To resolve this issue, the procedure for setting or resetting the environment variable was changed. **Scenario**: This issue occurred when a user configured uplink VLAN using the AOS-W Instant CLI and executed the **commit apply** command, which in turn cleared the individual OAW-IAP settings. This issue occurred in OAW-IAPs running AOS-W Instant 6.3.1.1-4.0.0.1 or earlier versions.

VPN Configuration

Table 8: *VPN Configuration Fixed Issue*

Bug ID	Description
93353	**Symptom**: DHCP renew packets were dropped in a network of single OAW-IAP, resulting in the VPN tunnel going down. A change in the firewall rules has fixed this issue. **Scenario**: This issue occurred when VPN switched over in a network with a single OAW-IAP. This issue was found in OAW-IAPs running AOS-W Instant 6.2.1.0-3.4.0.4.

WLAN Configuration

Table 9: *WLAN Configuration Fixed Issue*

Bug ID	Description
93921	**Symptom**: An OAW-IAP93 broadcast the SSID configured in the incorrect band. This issue is resolved by introducing a change to the OAW-IAP's internal software. **Scenario**: As OAW-IAP93 supports a single dual band radio, it can only work on 2.4GHz or 5GHz at a time, which is a global configuration. This issue occurred when the SSID configured in the other band was broadcast by OAW-IAP93 in the 2.4 GHz band. This issue was found in OAW-IAP93 devices running AOS-W Instant 6.3.1.1.-4.0.0.1 or earlier versions.

The following issues were fixed in the previous release of AOS-W Instant.

Resolved Issues in 6.3.1.1-4.0.0.1

AOS-W Instant UI

Table 10: *AOS-W Instant UI Fixed Issue*

Bug ID	Description
93647	**Symptom**: The wired profile could not be created through the AOS-W Instant UI. A change in the ACL process has fixed this issue. **Scenario:** This issue occurred when the user tried to create a wired profile using the Wired Network wizard in the AOS-W Instant UI. This issue was found in OAW-IAPs running AOS-W Instant 6.3.1.1-4.0.0.0.

This chapter provides information on the new features and enhancements introduced in the previous release of AOS-W Instant.

New Features and Enhancements

The following features and enhancements were introduced in the 6.3.1.1-4.0.0.0 and 6.3.1.1-4.0.0.1 releases.

Support of HTTP Proxy Configuration

If your OAW-IAP is deployed in a wired network, which requires an HTTP proxy server to access the internet, you need to configure HTTP proxy on the OAW-IAP. After you set up the HTTP proxy settings, the OAW-IAP can connect to the Activate server, OmniVista3600 or OpenDNS server through a secure HTTP connection. You can also configure a list of hosts which do not need proxy by providing their host names or IP address.

You can configure the HTTP Proxy in the AOS-W Instant UI and CLI. For more information, see:

- *Configuring HTTP Proxy on an OAW-IAP* in *AOS-W Instant 6.3.1.1-4.0 User Guide*
- The **proxy** command in the *AOS-W Instant 6.3.1.1-4.0 CLI Reference Guide*

OAW-IAP Provisioning Enhancements

In the AOS-W Instant 6.3.1.1-4.0 release, for option DHCP 43, besides the old format **<organization>,<ams-ip>,<ams-key>**, a new format **<organization>,<ams-domain>** is supported. If you use the format **<organization>**,**<ams-ip>**,**<ams-key>**, the Pre-Shared Key (PSK) based authentication is used for accessing the OmniVista. If you use the format **<organization>**,**<ams-domain>**, the OAW-IAP resolves the domain name into two IP address as AirWave primary, AirWave backup, and then starts a certificate-based authentication with the OmniVista, instead of the PSK based login.

You can configure the domain name in the AOS-W Instant UI and CLI. For more information, see:

- *Configuring OmniVista Information and Standard DHCP option 60 and 43 on Windows Server 2008* in *AOS-W Instant 6.3.1.1-4.0 User Guide*
- The **ams-ip** and **ams-backup-ip** commands in *AOS-W Instant 6.3.1.1-4.0 CLI Reference Guide*

Support for Centralized,L3 DHCP Scope

This release of AOS-W Instant supports Centralized L3 DHCP scope to serve L3 clients. When this feature is enabled, the OAW-IAP relays all DHCP request packets to the DHCP server and acts as gateway for the centralized DHCP scope serving L3 clients. The **DHCP server** window in the AOS-W Instant UI allows the configuration of a centralized DHCP scope.

When a centralized DHCP scope is configured:

- The Virtual Controller does not assign an IP address to the client and the DHCP traffic is directly forwarded to the DHCP Server.
- For L2 clients, the Virtual Controller bridges the DHCP traffic to the switch over the VPN/GRE tunnel. The IP address is obtained from the DHCP server behind the switch serving the VLAN/GRE of the client. This DHCP assignment mode also allows you to add the DHCP option 82 to the DHCP traffic forwarded to the switch.
- For L3 clients, the Virtual Controller acts as a DHCP relay agent that forwards the DHCP traffic to the DHCP server located behind the switch in the corporate network and reachable through the IPSec tunnel. The centralized L3 VLAN IP is used as the source IP. The IP address is obtained from the DHCP server.

For more information, see:

- *Configuring a Centralized DHCP Scope* in *AOS-W Instant 6.3.1.1-4.0 User Guide*
- The **ip dhcp** command in the *AOS-W Instant 6.3.1.1-4.0 CLI Reference Guide*

Support for Automatic Configuration of the GRE Tunnel

In the 6.3.1.1-4.0 release, AOS-W Instant allows you to enable automatic configuration of the GRE tunnel from an OAW-IAP to Alcatel-Lucent OmniAccess WLAN Switch. By using an IPsec connection, the OAW-IAPs can now set up a GRE tunnel with the switch. This feature eliminates the need for the manual configuration of tunnel interface on the switch.

For more information, see:

- *Enabling Automatic Configuration of GRE Tunnel* in *AOS-W Instant 6.3.1.1-4.0 User Guide*
- The **vpn gre-outside** command in the *AOS-W Instant 6.3.1.1-4.0 CLI Reference Guide*

Bandwidth Contract Enhancements

AOS-W Instant supports assigning bandwidth contracts to the user roles. The administrator can assign a bandwidth contract configured in Kbps to upstream (client to the OAW-IAP) or downstream (OAW-IAP to clients) traffic for a user role. All clients with this user role assigned, will be part of that bandwidth contract. The administrators can also set per user bandwidth to provide a specific bandwidth for every user.

To support this feature:

- In the AOS-W Instant UI, the **Access** tab of WLAN wizard and Wired network windows now allow setting a rule for bandwidth contract and allocate the bandwidth for downstream and upstream traffic per user in Kbps. You can also assign bandwidth limit for each SSID user under the **WLAN Settings** tab of the WLAN wizard. For more information, see *AOS-W Instant 6.3.1.1-4.0 User Guide*.
- In the AOS-W Instant CLI, the **wlan access-rule** command is enhanced to include the **bandwidth-limit** configuration command. For more information, see *AOS-W Instant 6.3.1.1-4.0 CLI Reference Guide*.

In the earlier releases, bandwidth contract could be assigned per SSID. In the 6.3.1.1-4.0 release, the bandwidth contract can also be assigned per SSID user. If the bandwidth contract is assigned for an SSID in *AOS-W Instant* 6.2.1.0-3.4.0.x image and when the OAW-IAP is upgraded to 6.3.1.1-4.0 release version, the bandwidth configuration per SSID will be treated as per-user downstream bandwidth contract for that SSID.

Support for 802.11r Roaming and Fast BSS Transition

In the 6.3.1.1-4.0 release, AOS-W Instant supports 802.11r roaming standard. As part of the 802.11r implementation, AOS-W Instant supports the Fast BSS Transition protocol. The Fast BSS Transition mechanism reduces client roaming delay when a client transitions from one BSS to another within the same cluster. This minimizes the time required to resume data connectivity when a BSS transition happens.

Fast BSS Transition is operational only if the wireless client supports 802.11r standard. If the client does not support 802.11r standard, it falls back to the normal WPA2 authentication method.

You can enable 802.11r roaming on WLAN SSID by using the AOS-W Instant UI (**WLAN Wizard>Security** tab) or CLI (**dot11r** command in the **wlan ssid-profile** command configuration mode). For more information, see *AOS-W Instant 6.3.1.1-4.0 User Guide* and *AOS-W Instant 6.3.1.1-4.0 CLI Reference Guide*.

Support for Client Roaming Based on Opportunistic Key Caching

AOS-W Instant also supports opportunistic key caching (OKC) based roaming. In the OKC based roaming, the AP stores a cached pairwise master key (PMK) for each client, which is derived from last 802.1X authentication completed by the client in the network. By default, the 802.1X authentication profile enables a cached PMK, which is used when a client roams to a new AP. The cached PMK is used when a client roams to a new AP. This allows faster roaming of clients between the OAW-IAPs in a cluster, without requiring a complete 802.1X authentication.

OKC roaming (when configured in the 802.1X Authentication profile) is supported on WPA2 clients. If the wireless client (the 802.1X supplicant) does not support this feature, a complete 802.1X authentication is required whenever a client roams to a new AP.

You can enable OKC roaming on a WLAN SSID by using the AOS-W Instant UI (**WLAN Wizard>Security** tab) or CLI (**no okc-disable** command in the **wlan ssid-profile** command configuration mode). For more information, see *AOS-W Instant 6.3.1.1-4.0 User Guide* and *AOS-W Instant 6.3.1.1-4.0 CLI Reference Guide*.

Link Aggregation Support on OAW-IAP22x Series

OAW-IAP22x Series supports the IEEE 802.11ac standard for high-performance WLAN. To support maximum traffic, port aggregation is required to increase throughput and enhance reliability. OAW-IAP22x Series supports link aggregation using either standard port-channel (configuration based) or LACP (protocol signaling based). LACP provides a standardized means for exchanging information with partner systems to form a dynamic link aggregation group. The LACP feature is automatically enabled during OAW-IAP boots and it dynamically detects the AP with the LACP capability, by checking if there is any LACP Protocol Data Unit (PDU) received on either eth0 or eth1 port.

For LACP support, the port-channel must be enabled on the switch and there is no configuration required on the OAW-IAP. However, you can view the LACP status on the OAW-IAP224 and OAW-IAP225 by using the **show lacp status** command. For more information, see *AOS-W Instant 6.3.1.1-4.0 User Guide* and *AOS-W Instant 6.3.1.1-4.0 CLI Reference Guide*.

The LACP feature is supported only on OAW-IAP22x Series.

Guest Management Interface

In the 6.3.1.1-4.0 release, AOS-W Instant supports the following types of users:

- Administrator–An admin user who creates SSIDs, wired profiles, DHCP server configuration parameters and manages local user database. The admin users can access the Virtual Controller Management User Interface.
- Guest administrator–A guest interface admin who manages guest users.
- Administrator with read-only access–The read-only admin user does not have access to the AOS-W Instant CLI. The AOS-W Instant UI is displayed in the read-only mode for these users.
- Employee users – Employees who use the enterprise network for official tasks.
- Guest users–Visiting users who temporarily use the enterprise network to access the Internet.

The user access privileges are determined by OAW-IAP management settings in the OmniVista Management client, and the type of the user.

To manage guest users, a guest management interface is introduced in the AOS-W Instant UI in the 6.3.1.1-4.0 release. The guest administrators can log in with their credentials and configure guest users. To add a guest admin or read-only user, use the **mgmt-user** command in the AOS-W Instant CLI.

OAW-IAP Integration with Analytics and Location Engine (ALE)

AOS-W Instant supports integration with Analytics and Location Engine (ALE). The ALE server acts as a primary interface to all third-party applications, and the OAW-IAP sends client information and other status information to the ALE server. To enable integration integrate with ALE, the ALE server address must be configured on the OAW-IAP.

The **RTLS** tab in the **Services** window of the AOS-W Instant UI allows the configuration of ALE server on an OAW-IAP. The **ale-server** and **ale-report-interval** commands are introduced in the 6.3.1.1-4.0 release to enable OAW-IAP integration with the ALE server. For more information, see *Configuring an OAW-IAP for Analytics and Location Engine Support in AOS-W Instant 6.3.1.1-4.0 User Guide* and *AOS-W Instant 6.3.1.1-4.0 CLI Reference Guide*.

OAW-IAP92 and OAW-IAP93 do not support ALE integration.

OAW-IAP Integration with Palo Alto Networks Firewall

AOS-W Instant supports integration with the Palo Alto Networks (PAN) firewall. To integrate an OAW-IAP with PAN user ID, a global profile is required. This profile can be configured on an OAW-IAP with PAN firewall information such as IP address, port, user name, password, firewall enabled or disabled status. When PAN firewall information is configured on an OAW-IAP, the OAW-IAP sends messages to PAN based on the type of authentication and client status.

OAW-IAP maintains the network (such as mapping IP address) and user information for its clients in the network and can provide the required information for the user ID feature on PAN firewall.

OAW-IAP and PAN firewall integration is supported with the XML-API that is available with PAN-OS 5.0 or later.

To support OAW-IAP integration with PAN Firewall, the **Network Integration** tab in the **Services** window of the AOS-W Instant UI and **firewall-external-enforcement** command in the CLI are introduced. For more information, see *AOS-W Instant* and *AOS-W Instant 6.3.1.1-4.0 CLI Reference Guide*.

Support for Domain-based ACL

AOS-W Instant supports configuration of domain-based Access Control List (ACL) rule. Access to a specific domain is allowed or denied based on the ACL rule definition. To enable support for creating a domain-based ACL, the **Access Rule** window in WLAN wizard and Wired Network is modified to include **to domain name** option in **Destination** drop-down.

For more information, see *AOS-W Instant 6.3.1.1-4.0 User Guide*.

Internal Captive Portal Splash Page Enhancements

AOS-W Instant now supports customization of logo, policy text, and usage terms for the internal Captive portal splash page. The customized logo can be uploaded to the internal Captive portal server through the **Security** tab of WLAN wizard Wired network window in the AOS-W Instant UI, or by using the following command sequence in the AOS-W Instant CLI:

```
(Instant Access Point)# copy config tftp <ip-address> <filename> portal logo
```

Support for Multiple Captive Portal Profiles

You can now configure external Captive portal profiles and associate these profiles to a user role or SSID. You can create a set of Captive portal profiles in the **Security>External Captive Portal** window and associate these profiles with an SSID or a wired profile. You can also create a new Captive portal profile under the **Security** tab of the WLAN wizard or a **Wired Network** window. In the 6.3.1.1-4.0 release, you can configure up to eight external Captive portal profiles.

When the Captive portal profile is associated to an SSID, it is used before user authentication. If the profile is associated to a role, it is used only after the user authentication. When a Captive portal profile is applied to an SSID or wired profile, the users connecting to the SSID or wired network are assigned a role with the Captive portal rule. The guest user role allows only DNS and DHCP traffic between the client and network, and directs all HTTP or HTTPS requests to the Captive portal unless explicitly permitted.

For more information on creating an Captive portal profile, see:

- *Configuring External Captive Portal for a Guest Network* in *AOS-W Instant 6.3.1.1-4.0 User Guide*
- **wlan external-captive-portal** command in *AOS-W Instant 6.3.1.1-4.0 CLI Reference Guide*

Client Match

AOS-W Instant supports the ARM client match feature to continually monitor a client's RF neighborhood and to provide the ongoing client bandsteering service, load balancing, and enhanced OAW-IAP reassignment for roaming mobile clients.

The Client Match feature supersedes the legacy bandsteering and spectrum load balancing features, which unlike client match, do not trigger OAW-IAP changes for clients already associated to an OAW-IAP. When the client match feature is enabled on an OAW-IAP, the OAW-IAP measures the RF health of its associated clients. When the client match criteria is met, the clients are moved from one AP to another for better performance and user experience.

In the AOS-W Instant 6.3.1.1-4.0 release, the client match feature is supported only within an OAW-IAP cluster.

You can enable client match in the **ARM** tab of the **RF** window in the AOS-W Instant UI or by using the **client-match** commands in the ARM configuration mode in AOS-W Instant CLI.

For more information, see *AOS-W Instant 6.3.1.1-4.0 User Guide* and *AOS-W Instant 6.3.1.1-4.0 CLI Reference Guide*.

Support for Spanning Tree Protocol

AOS-W Instant allows enabling of Spanning Tree Protocol (STP) on a wired profile. STP ensures that there are no loops in any bridged Ethernet network and operates on all downlink ports, regardless of the forwarding mode. By default Spanning tree protocol is disabled on wired profiles.

To enable STP on a wired profile, navigate to the **More>Wired>Wired Network>Wired Settings** window and select **Enabled** from the **Spanning tree** drop-down. You can also enable STP by using the **spanning-tree** command in the wired port profile configuration mode in the AOS-W Instant CLI.

STP will not operate on the uplink port and is supported only on the OAW-IAPs with three or more ports.

Customization of Internal Captive Portal Server Certificates

In the 6.3.1.1-4.0 release, AOS-W Instant supports uploading customized internal Captive Portal server certificates in the PEM or PKCS#12 format to the OAW-IAP database. The Captive portal server certificate verifies internal Captive portal server's identity to the client.

To upload a Captive portal server certificate, navigate to **Maintenance>Certificates>Upload New Certificate** and select **Captive portal server** from **Certificate type** drop-down. You can also upload the Captive portal certificate by using the following command in the AOS-W Instant CLI:

```
(Instant Access Point)# copy tftp {<ip-address> <filename> cpserver cert <password> format {p1
2|pem}}
```

For more information, see *AOS-W Instant 6.3.1.1-4.0 User Guide* and *AOS-W Instant 6.3.1.1-4.0 CLI Reference Guide*.

Provisioning an OAW-IAP as a master OAW-IAP

In most cases, the master election process automatically determines the OAW-IAP that can perform the role of Virtual Controller, which will apply its image and configuration to all other OAW-IAPs in the same AP management VLAN. When the Virtual Controller goes down, a new Virtual Controller is elected. If manual specification of the Virtual Controller is required, AOS-W Instant allows you to manually assign one OAW-IAP as the master OAW-IAP based on network-specific parameters such as the physical location of the Virtual Controller.

To provision an OAW-IAP as a master OAW-IAP:

- In the AOS-W Instant UI, go to **Access Points tab> edit>Edit Access Point** <*AP-name*> window and select **Enabled** from the **Preferred Master** drop-down. For more information, see *AOS-W Instant 6.3.1.1-4.0 User Guide*.
- In the AOS-W Instant CLI, execute the **iap-master** command. For more information, see *AOS-W Instant 6.3.1.1-4.0 CLI Reference Guide*.

AirGroup Enhancements

In the 6.3.1.1-4.0 release, AOS-W Instant supports the following AirGroup services:

- AirPlay™– Apple® AirPlay allows wireless streaming of music, video, and slideshows from your iOS device to Apple TV® and other devices that support the AirPlay feature.
- AirPrint™– Apple AirPrint allows you to print from an iPad®, iPhone®, or iPod® Touch directly to any AirPrint compatible printers.
- iTunes– iTunes service is used by iTunes Wi-Fi sync and iTunes home-sharing applications across all Apple devices.
- RemoteMgmt– Use this service for remote login, remote management, and FTP utilities on Apple devices.
- Sharing– Applications such as disk sharing and file sharing, use the service ID that are part of this service on one or more Apple devices.
- Chat– The iChat® (Instant Messenger) application on Apple devices uses this service.

The services are pre-configured and are available as part of the factory default configuration. The administrator can also enable or disable any or all services by using the AOS-W Instant UI or CLI.

For more information, see:

- The *Configuring AirGroup and AirGroup Services on an OAW-IAP* topic in *AOS-W Instant 6.3.1.1-4.0 User Guide*
- The AirGroup commands such as **airgroupservice**, **show airgroup**, **show airgroupservice-ids** in *AOS-W Instant 6.3.1.1-4.0 CLI Reference Guide*

Dynamic RADIUS Proxy IP Address Configuration

When the dynamic RADIUS proxy feature is enabled, a static Virtual Controller IP must be configured to ensure that all RADIUS packets use Virtual Controller IP as source IP and VLAN. However, if the users need to authenticate to the RADIUS servers through different VLANs, you can specify the dynamic RADIUS proxy parameters such as IP address and VLAN when configuring the authentication server information on an OAW-IAP.

When configured, the dynamic RADIUS proxy IP address and VLAN details are used as source IP address and VLAN for RADIUS packets.

For more information, see:

- *Configuring Dynamic RADIUS Proxy Parameters* in *AOS-W Instant 6.3.1.1-4.0 User Guide*

- **wlan auth-server** command in *AOS-W Instant 6.3.1.1-4.0 CLI Reference Guide*

Restricted Access Management

AOS-W Instant supports enhanced inbound firewall configuration and allows you to configure management subnets and restrict access to the corporate network. To allow flexibility in firewall configuration, AOS-W Instant supports the following configuration options:

- Management Subnets—You can configure subnets to ensure that the OAW-IAP management is carried out only from these subnets. When the management subnets are configured, Telnet, SSH, and UI access is restricted to these subnets only.
- Restricted corporate access—You can configure restricted corporate access to block unauthorized users from accessing the corporate network. When restricted corporate access is enabled, corporate access is blocked from the uplink port of master OAW-IAP, including clients connected to a slave OAW-IAP.

You can configure management subnets and restricted corporate access by using the AOS-W Instant UI or CLI. For more information, see *Managing Inbound Traffic* in *AOS-W Instant 6.3.1.1-4.0 User Guide* and **restricted-mgmt-access** and **restrict-corp-access** command pages in *AOS-W Instant 6.3.1.1-4.0 CLI Reference Guide*.

Support for OAW-IAP224 and OAW-IAP225

This release extends support to OAW-IAP224 and OAW-IAP225, which enable support for the IEEE 802.11ac standard for high performance WLAN. These OAW-IAPs use MIMO (Multiple-in, Multiple-out) 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 existing legacy wireless services. The OAW-IAP224 and OAW-IAP225 support 802.11ac on the 5GHz band using 80 MHz channels.

OAW-IAP22x Series does not support wireless mesh functionality.

Support for OAW-IAP114 and OAW-IAP115

This release extends support to OAW-IAP114 and OAW-IAP115 dual radio, dual-band wireless access points that support the IEEE 802.11n standard for high-performance WLAN. These APs use MIMO (Multiple-in, Multiple-out) technology and other high-throughput mode techniques to deliver high-performance, 802.11n 2.4 GHz and 5 GHz functionality while simultaneously supporting existing 802.11a/b/g wireless services.

Uplink VLAN Monitoring and Detection on Upstream Devices

The AOS-W Instant UI now displays an alert message when a client connects to an SSID or a wired interface with a VLAN that is not allowed on the upstream device. The alert message notifies the users about the mismatch in the VLAN configuration on the OAW-IAP or the upstream device of an OAW-IAP. To resolve this issue, ensure that there is no mismatch in the VLAN configuration.

For more information on VLAN configuration, see *VLAN Configuration* in *AOS-W Instant 6.3.1.1-4.0 User Guide*.

Support for Telnet Access

In the 6.3.1.1-4.0 release, AOS-W Instant supports Telnet access to the AOS-W Instant CLI. To enable Telnet access:

- In the AOS-W Instant UI, go to **System>Show advanced options** and select **Enabled** from the **Telnet server** drop-down.
- In the CLI, execute the **telnet-server** command in the configuration mode.

Applying Configuration Changes during a CLI Session

In the 6.3.1.1-4.0 release, the **commit apply no-save** command is introduced to allow the users to apply the configuration changes to a cluster without saving the configuration during a CLI session. The users can save the configuration changes by using the **commit apply** or **write memory** command. For more information, see *AOS-W Instant 6.3.1.1-4.0 CLI Reference Guide*.

Two SKUs for OAW-IAP22x Series and OAW-IAP11x Series

In the earlier AOS-W Instant releases, the OAW-IAPs were shipped as the following variants:

- OAW-IAP-US (United States)
- OAW-IAP-JP (Japan)
- OAW-IAP-RW (Rest of World)

In the 6.3.1.1-4.0.0.1 release, the OAW-IAP11x Series and OAW-IAP22x Series are shipped as the following variants:

- OAW-IAP-US (United States)
- OAW-IAP-RW (Rest of World). This variant also includes Japan and Israel regulatory domains.

When you log in to the AOS-W Instant UI for the first time, the **Country Code** pop-up will be displayed for the OAW-IAPs shipped as OAW-IAP-RW variant. You can specify a country code by selecting an appropriate option from the **Please Specify the Country Code** drop-down list. For OAW-IAP11x Series and OAW-IAP22x Series, the JP country code is included in the drop-down list.

If the existing Virtual Controller is an older OAW-IAP with the JP country code, a new model with the RW variant can join the cluster and it will operate in the JP regulatory domain.

If the existing Virtual Controller is a new OAW-IAP-RW, an older model OAW-IAP with the JP country code can join the cluster only if the OAW-IAP-RW is configured for the JP country code.

An OAW-IAP-RW can be converted to switch-based operation with an RW variant of switch.

This chapter describes the known issues and limitations identified in the previous releases of AOS-W Instant.

No Support for PKCS#12 Certificate Format

Starting from 6.3.1.1-4.0 release, AOS-W Instant does not support uploading of certificates in the (Private-Key Information Syntax Standard) PKCS#12 (.p12) format. To view a list of server and CA certificate formats that are supported by the OAW-IAP, run the **show supported-cert-formats** command.

Known Issues

Authentication

Table 11: *Authentication Known Issue*

Bug ID	Description
93045	**Symptom:** When the same dynamic RADIUS Proxy (DRP) IP, VLAN, and gateway details are configured on both the primary and backup authentication servers and if the DRP details are deleted for either the primary or backup server, the DRP IP feature does not function. **Scenario**: This issue occurs when the same DRP IP is configured on the primary and backup authentication servers. This issue is found in OAW-IAPs running AOS-W Instant 6.3.1.1-4.0.0.0. **Workaround**: None.

Captive Portal

Table 12: *Captive Portal Known Issues*

Bug ID	Description
93173	**Symptom**: Captive portal does not support PEM certificates with passphrase protected private key. **Scenario**: This issue occurs in OAW-IAPs running AOS-W Instant 6.3.1.1-4.0.0.0 when the customized Captive portal certificates are uploaded with passphrase protected private key. **Workaround**: None
93224	**Symptom**: OAW-IAP does not support server certificate encrypted by PKCS#8. **Scenario:** This issue is found in OAW-IAPs running AOS-W Instant 6.3.1.1-4.0.0.0. **Workaround**: Use the PKCS#1 format for certificate encryption.