AOS-W Instant 6.2.1.0-3.4.0.1

Alcatel·Lucent

Release Notes

Copyright

Legal Notice

The use of Alcatel-Lucent switching platforms and software, by all individuals or corporations, to terminate Cisco or Nortel VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Alcatel-Lucent from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of Cisco Systems or Nortel Networks.

Alcatel·Lucent

www.alcatel-lucent.com

26801 West Agoura Road
Calabasas, CA 91301

Contents

Release Overview

AOS-W Instant 6.2.1.0-3.4.0.1 is a software patch release that introduces fixes to the issues detected in the previous releases.

For more information on features described in the following sections, see the *AOS-W Instant 6.2.1.0-3.4 User Guide*.

Contents

- "What's New in this Release" on page 7 lists the issues fixed in this release of AOS-W Instant.
- "Features Added in the Previous Releases" on page 11 describes the new features introduced in the previous release of AOS-W Instant.
- "Issues Resolved in Previous Releases" on page 17 describes the issues fixed in the previous releases of AOS-W Instant.
- "Known Issues from Previous Releases" on page 19 describes the known issues and limitations that were detected in the previous releases of AOS-W Instant.

Contacting Support

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

Chapter 2

What’s New in this Release

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

Provisioning Support for Huawei HWD12 Modem

This release of AOS-W Instant supports automatic provisioning of the Huawei HWD12 modem.

Enhancements to the Personal Network Encryption Settings

In the current release, AOS-W Instant allows wpa-psk-aes and wpa-psk-tkip encryption types for WPA personal security configuration.

You can configure wpa-psk-aes and wpa-psk-tkip encryption types for personal networks through the AOS-W Instant UI or CLI.

Using the AOS-W Instant UI

1. Go to **New WLAN or Edit WLAN**>**Security>Personal**.
2. Select the **WPA Personal** option from the **Key management** drop-down.
3. Click **Next**.

Using the AOS-W Instant CLI

Execute the following commands at the command prompt:

```
(Instant Access Point)(config)# wlan ssid-profile <Name>
(Instant Access Point)(SSID Profile <name>)# opmode wpa-psk-tkip,wpa-psk-aes
```

Resolved Issues in 6.2.1.0-3.4.0.1

Access Point

Table 1 *Access Point Fixed Issue*

Bug ID	Description
78122 87187	**Symptom:** Some APs rebooted randomly due to memory issues. To resolve this issue, upgrade to AOS-W Instant 6.2.1.0-3.4.0.1. **Scenario:** This issue was found in APs running AOS-W 6.2.1.0 and OAW-IAPs running AOS-W Instant 6.2.1.0-3.3.

AirGroup

Table 2 *AirGroup Fixed Issue*

Bug ID	Description
87139	**Symptom:** The AirGroup clients were not able to discover the AirPrint servers as the server records were not synchronized in all OAW-IAPs in a cluster. An increase in the buffer from 2K to 4K for storing the server records has resolved this issue. **Scenario:** When the server records exceeded 2K buffer, the synchronization of server records across the OAW-IAPs failed. This issue was found in OAW-IAPs running AOS-W Instant 6.2.1.0-3.3 or later.

Authentication

Table 3 *Authentication Fixed Issue*

Bug ID	Description
86932	**Symptom:** The clients could not authenticate when the IP address for the Bridge interface was lost. To resolve this issue, upgrade to AOS-W Instant 6.2.1.0-3.4.0.1. **Scenario:** This issue occurred when the IP address for the Bridge interface was not available in the datapath user entry, after the Bridge interface IP was changed. This issue was found in OAW-IAPs running AOS-W Instant 6.2.1.0-3.2.0.x releases with Dynamic RADIUS proxy enabled.

Datapath

Table 4 *Datapath Fixed Issue*

Bug ID	Description
86865	**Symptom:** Clients could not connect to the OAW-IAP when the master OAW-IAP sent packets to the default gateway MAC address instead of the Virtual Controller gateway MAC address. The packets from the Virtual Controller IP address are now channelled through a routing module to ensure correct routing. **Scenario:** The issue occurred on a master OAW-IAP with dynamic RADIUS proxy feature enabled. When the Virtual Controller VLAN and gateway were configured on an OAW-IAP and the Virtual Controller gateway IP and the default gateway had different MAC addresses, the master OAW-IAP sent packets to the default gateway. This issue was found in OAW-IAPs running AOS-W Instant 6.2.1.0-3.3 and later versions.

L2TPV3 Configuration

Table 5 *L2TPV3 Fixed Issue*

Bug ID	Description
86639	**Symptom:** When the local UDP port was set to a user-defined value, the L2TPv3 process failed to start correctly. To resolve this issue, upgrade to AOS-W Instant 6.2.1.0-3.4.0.1. **Scenario:** This issue occurred when the OAW-IAPs rebooted with a user-defined local UDP port configured for the L2TP tunnel. This issue was found in OAW-IAPs running AOS-W Instant 6.2.1.0-3.4.

Station Management

Table 6 *Station Management Fixed Issue*

Bug ID	Description
86996	**Symptom:** OAW-IAPs rebooted randomly due to a high CPU utilization. Changes in the log clearing process for the offline clients have resolved this issue. **Scenario:** When many wireless clients disassociated from an OAW-IAP, the respective L3 user entries for the offline clients were not deleted from the OAW-IAP database. Due to this, the OAW-IAPs showed a 100% CPU utilization and rebooted randomly. This issue was found in OAW-IAPs running AOS-W Instant 6.2.1.0-3.3.

Terminal Access

Table 7 *Terminal Access Fixed Issue*

Bug ID	Description
88020	**Symptom:** The SSH access to the OAW-IAP Command-Line Interface (CLI) was enabled, although it was set to disabled before the OAW-IAP reboot. A change in the OAW-IAP code has resolved this issue. **Scenario:** This issue occurred because the terminal access status was reset to enabled after each OAW-IAP reboot. This issue was found in OAW-IAPs running AOS-W Instant 6.2.1.0-3.3.0.3 or later.

Chapter 3

Features Added in the Previous Releases

This chapter provides a brief summary of the new features and enhancements introduced in the previous release of AOS-W Instant.

For more information on the features listed in this section and the related configuration procedures, see *AOS-W Instant 6.2.1.0-3.4 User Guide.*

New Features

Lawful Intercept and CALEA Integration

In the current release, AOS-W Instant supports CALEA server integration to enable service providers (SPs) to perform electronic surveillance authorized by the Law Enforcement Agencies (LEA).

Depending on the country of operation, the SPs are required to support Lawful Intercept (LI) in their respective networks. In the United States, SPs are required to ensure LI compliance based on Communications Assistance for Law Enforcement Act (CALEA) specifications.

To support CALEA integration and ensure LI compliance, you can configure the OAW-IAPs to replicate a specific client traffic and send it to a remote CALEA server. The replicated traffic can be sent either directly to the CALEA server or through the VPN.

- If the OAW-IAP is configured to send the client data directly to the CALEA server, an individual GRE tunnel is configured to the CALEA server and the client traffic is replicated within the GRE tunnel. Each OAW-IAP performs GRE encapsulation only for the clients associated to it.
- If the CALEA server is deployed with the Aruba Controller and an additional IPSec tunnel is configured for the corporate access, the client traffic is replicated by the slave OAW-IAP. The client data is encapsulated by GRE on slave and then routed to the master OAW-IAP. The master OAW-IAP sends the IPsec client traffic to the Controller. The Controller handles the IPSec client traffic, while GRE data is routed to the CALEA server.

The client traffic is replicated in the following ways:

- Through RADIUS VSA— In this method, the client traffic is replicated by using RADIUS VSA to assign clients to a CALEA related user role. To enable role assignment to clients, you need to create a user role and CALEA access rule, and then assign the CALEA rule to the user role. Whenever a client that is configured to use a CALEA rule connects, a replication role is assigned.
- Through Change of Authorization (CoA)—In this method, a user session can start without replication. When the network administrator triggers a CoA from the RADIUS server, the user session is replicated. The replication is stopped when the user disconnects or by sending a CoA to change the replication role.

For more information on configuring OAW-IAPs for CALEA integration, see *Lawful Intercept and CALEA Integration* section in *AOS-W Instant 6.2.1.0-3.4 User Guide* and *calea* command in *AOS-W Instant 6.2.1.0-3.4 CLI Reference Guide.*

You can configure DHCP options using AOS-W Instant UI or CLI. For more information, see *Configuring DHCP Scopes* section in *AOS-W Instant 6.2.1.0-3.4 User Guide* and *ip dhcp* command in the *AOS-W Instant 6.2.1.0-3.4 CLI Reference Guide.*

L2TPv3 Configuration

The Layer 2 Tunneling Protocol version 3 (L2TPv3) feature allows the OAW-IAP to act as an L2TP Access Concentrator (LAC) and tunnels all wireless clients L2 traffic from AP to L2TP Network Server (LNS). In a centralized L2 model, the VLAN on the corporate side is extended to remote branch sites. The wireless clients associated to the OAW-IAP get the IP address from the DHCP server running on the LNS.

In this release:

- AOS-W Instant supports tunnel and session configuration, and uses Control Message Authentication (RFC 3931) for tunnel and session establishment. Each L2TPv3 tunnel supports one data connection and this connection is termed as an L2TPv3 session.
- Each OAW-IAP supports tunneling over UDP only.
- If primary LNS is down, it fails over to the backup LNS. The primary and backup IP address can be configured under L2TPV3 tunnel profile. If the primary tunnel creation fails or if the primary tunnel gets deleted, the backup becomes available. The OAW-IAPs support the following failover modes:
  - Preemptive: In this mode, if the primary server becomes available when the backup is active, the backup tunnel is deleted and the primary tunnel is set as the only active tunnel. If you configure the tunnel to be preemptive and when the primary tunnel goes down, a persistence timer which tries to bring up the primary tunnel starts.
  - Non-Preemptive: In this mode, when the connection to backup tunnel is established after primary tunnel goes down, the primary tunnel will not be set as the active tunnel when it becomes available.

You can configure the tunnel and session for L2TPv3 by using AOS-W Instant UI or CLI. For more information, see *Configuring an L2TPv3 Tunnel* in *AOS-W Instant 6.2.1.0-3.4 User Guide*, and *l2tpv3 session* and l*2tpv3 tunnel* commands in *AOS-W Instant 6.2.1.0-3.4 CLI Reference Guide*.

Support of Regular Expressions in VLAN and Role Derivation Rules

For complex policies of role and VLAN derivation using device DHCP fingerprints, you can use a regular expression to match against the combined string of the MAC address and the DHCP options. The combined string is formed by concatenating the hexadecimal presentation of the MAC address and all of the DHCP options sent by a particular device. The regular expression is a pattern description language that can be used for advanced pattern matching of a given string.

The **matches-regular-expression** operator allows you to use regular expression when creating a VLAN or role derivation rule. The rule is applied only if the attribute value matches the given regular expression pattern. The **matches-regular-expression** operator can be used only for defining a role derivation rule based on the **mac-address-and-dhcp-options** attribute.

For more information on regular expressions, and creating VLAN and role derivation rules, see the following topics in *AOS-W Instant 6.2.1.0-3.4 User Guide:*

- *Using Regular Expressions in Role and VLAN Derivation Rules*
- *Creating a Role Derivation Rule*
- *Configuring VLAN Derivation Rules*

Dynamic CPU Management

In the current release, AOS-W Instant dynamically manages resources across different functions performed by an AP. However, under special circumstances if resource management needs to be enforced or disabled altogether, the dynamic CPU management configuration settings can be modified.

For dynamic resource management:

- The **Dynamic CPU management** drop-down with the following options is added in the **System** window of the AOS-W Instant UI:

- **Automatic**— When selected, the CPU management is automatically enabled or disabled as required during run-time. This is the default and recommended option.
- **Always enabled in all APs**— Enables dynamic management of resources across different functions performed by an OAW-IAP.
- **Always disabled in all APs**— Disables the CPU management feature on all APs, typically for small networks.

- The **dynamic-cpu-mgmt** command with the **auto**, **enable,** and **disable** parameters is added in the AOS-W Instant CLI.

For more information, see *Dynamic CPU Management* in *AOS-W Instant 6.2.1.0-3.4 User Guide* and *dynamic-cpu-mgmt* command in *AOS-W Instant 6.2.1.0-3.4 CLI Reference Guide.*

Connectivity Summary on AOS-W Instant Login Page

You can now view a summary of the connectivity status to the AOS-W Instant network. The AOS-W Instant **Login** page displays a summary indicating the status of the Internet availability, uplink, signal strength, VPN, and AirWave configuration details before logging in to the AOS-W Instant UI.

NOTE

The Internet status is available only if the Internet failover feature (**System>Show advanced option>uplink>Internet failover**) is enabled.

The cellular provider and cellular strength information is available only when a 3G or 4G modem is in use.

Enhancements to PPPoE Configuration

AOS-W Instant allows you to set a local interface for the PPPoE uplink connections by configuring the Local,L3 DHCP gateway IP address as the local IP address of the PPPoE interface. When configured, the local interface acts as an unnumbered PPPoE interface and allows the entire Local,L3 DHCP subnet to be allocated to clients.

NOTE

Before configuring a local interface for the PPPoE connections, ensure that the Local,L3 DHCP scope is configured on the OAW-IAP.

For more information, see *Configuring PPPoE Uplink Profile* in *AOS-W Instant 6.2.1.0-3.4 User Guide* and *pppoe-uplink-profile* command in *AOS-W Instant 6.2.1.0-3.4 CLI Reference Guide.*

Reconnecting Users During a VPN Failover

In the current release of AOS-W Instant, the OAW-IAPs can be configured to disable all SSIDs when the system switches during VPN tunnel transition from primary to the backup VPN tunnel Vice-Versa. You can also specify an interval for VPN tunnel transition, after which the users can be reconnected to the VPN tunnel.

To enable this feature through the AOS-W Instant UI:

1. Navigate to **More>VPN>Show advanced options>IPSec**.
2. Set **Reconnect user on failover** to **Enabled**.
3. To configure an interval during which wired and wireless users are disconnected due to a VPN tunnel switch, specify the number of seconds in **Reconnect time on failover.**

To enable this feature through the AOS-W Instant CLI, execute the following commands at the command prompt:

```
(Instant Access Point)(config)# vpn reconnect-user-on-failover
```

```
(Instant Access Point)(config)# vpn reconnect-time-on-failover <down_time>
```

For more information, see *Configuring PPPoE Uplink Profile* in *AOS-W Instant 6.2.1.0-3.4 User Guide* and *pppoe-uplink-profile* command in *AOS-W Instant 6.2.1.0-3.4 CLI Reference Guide*.

Enhancements

The following enhancements are introduced in AOS-W Instant *6.2.1.0-3.4* release.

Dead Time Configuration for Authentication Servers

In the current release, you can configure a dead time for authentication servers to enable an unavailable authentication server to be marked as “out of service”. When two or more authentication servers are configured on the OAW-IAP and if a server is unavailable, the dead time configuration determines the duration after which an authentication server is marked as unavailable. The dead time configuration determines how long an authentication server will be available when it is marked as an unavailable server. When the dead time duration is passed, the OAW-IAP retries to connect to the server.

For dead time configuration:

- The **Dead time** field is added in the **New Server** window. The **New Server** window can be launched through **Security>Authentication Servers>New**, or **New WLAN or Edit WLAN>Security> Authentication server 1>New**). For more information, see the *Configuring Authentication Servers* in *AOS-W Instant 6.2.1.0-3.4 User Guide*.
- The **deadtime** parameter is added to the **wlan auth-server** command. For more information, see *wlan auth-server* command in *AOS-W Instant 6.2.1.0-3.4 CLI Reference Guide*.

Deletion of Dynamically Blacklisted Clients

In the current release of AOS-W Instant, the administrators can delete the clients that were dynamically blacklisted. The dynamic blacklisting is used when the clients exceed the authentication failure threshold, or when a blacklisting rule triggers as part of the authentication process.

To delete the clients that are blacklisted dynamically, execute the following command:

```
(Instant access point)# remove-blacklist-client <MAC_adress> <AP_name>
```

For more information, see the *remove-blacklist-client* command in *AOS-W Instant 6.2.1.0-3.4 CLI Reference Guide*.

Cellular Modem Configuration with PAP and CHAP

In the current release of AOS-W Instant, the USB modems can be configured to use Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) authentication types. This allows the 3G Point-to-Point protocol (PPP) to use either PAP or CHAP to validate clients.

To configure the USB modem, execute the following commands:

```
(Instant access point)(config)# cellular-uplink-profile
(Instant Access Point)(cellular-uplink-profile)# usb-auth-type {pap |chap}
```

For more information on cellular uplink configuration, see *cellular-uplink-profile* command in the *AOS-W Instant 6.2.1.0-3.4 CLI Reference Guide* and *Configuring Cellular Uplink Profiles* in the *AOS-W Instant 6.2.1.0-3.4 User Guide*.

Maximum Distance Configuration for 5GHz and 2.4 GHz Radio Profiles

AOS-W Instant now allows you to configure the maximum distance between a client and an AP or between a mesh point and a mesh portal in meters. You can configure a value ranging from 600 to 1000 meters.

A value of 0 specifies the default settings for this parameter, where time-outs are only modified for outdoor mesh radios which use a distance of 16km.

For more information, see the *rf dot11a-radio-profile* and *rf dot11g-radioprofile* commands in the *AOS-W Instant 6.2.1.0-3.4 CLI Reference Guide*.

Chapter 4

Issues Resolved in Previous Releases

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

Resolved Issues in 6.2.1.0-3.4

Authentication

Table 1 *Authentication Fixed Issue*

Bug ID	Description
83848	**Symptom:** An OAW-IAP sent new accounting information for the re-associated clients, instead of sending accounting information in the previous accounting session ID. Changes to the code base have resolved this issue. **Scenario:** This issue was observed when a client re-associated to an OAW-IAP and the OAW-IAP sent RADIUS START accounting records for that client to the RADIUS server with a new session ID. This issue was found in OAW-IAPs running AOS-W Instant 6.2.1.0-3.3.

Mesh Network

Table 2 *Mesh Network Fixed Issue*

Bug ID	Description
85692	**Symptom:** The mesh OAW-IAP clients could not obtain an IP address from the DHCP server. Disabling **Deny inter-user bridging** feature through the AOS-W Instant UI or CLI resolves this issue. **Scenario:** This issue occurred because the **Deny inter-user bridging** feature was enabled on the OAW-IAP. Due to this, the OAW-IAP denied bridging traffic between its clients and wireless ports, thereby blocking the IP address assignment from the DHCP server for the mesh OAW-IAP clients. This issue was found in OAW-IAPs running AOS-W Instant 6.2.1.0-3.1 or later releases in mesh topology.

Security

Table 3 *Security Fixed Issue*

Bug ID	Description
85410	**Symptom:** The users could not view the uploaded server certificates after an OAW-IAP reboot. Changes to the CA certificate reading process have resolved this issue. **Scenario:** After a reboot, the OAW-IAPs did not display the server certificates uploaded by the user as there was no CA certificate uploaded by the users in the OAW-IAP database. This issue was found in OAW-IAPs running 6.2.1.0-3.3.0.1.

SNMP

Table 4 *SNMP Fixed Issue*

Bug ID	Description
82752	**Symptom**: The value for the SNMP **aiRadioPhyEvents** counter was displayed as **0**. The OAW-IAP now displays correct values for the SNMP aiRadioPhyEvents counter. **Scenario**: This issue was found in OAW-IAPs running AOS-W Instant 6.2.1.0-3.3.
86108	**Symptom:** The SNMP GET operations could not be performed on a Virtual Controller, although the Virtual Controller IP address was configured for SNMP operations. Upgrading to AOS-W Instant 6.2.1.0-3.4 resolves this issue. **Scenario:** This issue was found in OAW-IAPs running AOS-W Instant 6.2.1.0-3.3.

VLAN Configuration

Table 5 *VLAN Configuration Fixed Issue*

Bug ID	Description
85162	**Symptom:** An OAW-IAP rebooted when connected to a virtual controller that was configured to use the same VLAN as that of uplink. To resolve this issue and to avoid duplication of the route cache entries, do not configure the same VLAN for uplink and Virtual Controller. **Scenario:** This issue was observed when the same VLAN was configured for Virtual Controller and uplink on an OAW-IAP. When a client connected to this OAW-IAP and tried to reach the Virtual Controller IP, the OAW-IAP rebooted. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.3.
85902	**Symptom:** The OAW-IAP management through AirWave and the client authentication against Virtual Controller IP address failed due to incorrect VLAN tagging. The OAW-IAP now tags the uplink VLAN only if a packet is not tagged already. **Scenario:** When the Virtual Controller VLAN and uplink VLAN were configured separately on the OAW-IAP, the Virtual Controller VLAN was not enforced, and was instead tagged with the uplink VLAN. This issue was found in OAW-IAPs running AOS-W Instant 6.2.1.0-3.3.

Chapter 5

Known Issues from Previous Releases

The known issues and limitations identified in the previous releases of AOS-W Instant are described in the following tables.

Known Issues

AirWave Integration

Table 1 *AirWave Integration Known Issue*

Bug ID	Description
85335	**Symptom:** The users can configure OAW-IAP names exceeding the character limit through AirWave Management Server, although the character limit is set to 32. **Scenario:** This issue is found in OAW-IAPs running AOS-W Instant 6.2.1.0-3.4 with AirWave 7.7. **Workaround:** None

L2TPV3 Configuration

Bug ID	Description
86486	**Symptom:** If an L2TP session is created before configuring the L2TP tunnel, the session cannot be associated with the tunnel. **Scenario:** This issue occurs when a session is created before configuring the tunnel or if a session is created under an incorrectly configured tunnel. This issue is found in OAW-IAPs running AOS-W Instant 6.2.1.0-3.4. **Workaround:** Do not configure a session profile before creating the L2TP tunnel profile. If a tunnel is incorrectly configured, reconfigure the tunnel and then create a corresponding session profile.

VLAN Configuration

Table 2 *VLAN Configuration Known Issues and Limitations*

Bug ID	Description
75496	**Symptom:** A slave OAW-IAP cannot connect to the master OAW-IAP when reconnecting to the network. **Scenario:** This issue occurs when the Ethernet uplink fails and switches over to another available uplink. This issue was observed in a hierarchical network topology when the native VLAN on a wired port was set to a value other than 1. This issue is found in OAW-IAPs running AOS-W Instant version 6.2.0.0-3.2 or later. **Workaround:** None

Table 2 *VLAN Configuration Known Issues and Limitations*

Bug ID	Description
80849	**Symptom:** In a hierarchical topology, although the clients can obtain an IP address, the Virtual Controller Gateway IP address resolution fails. **Scenario:** This issue occurs when the master OAW-IAP assigns a guest VLAN IP address to the client. As the DHCP scope configuration on the slave OAW-IAP uses a different subnet, the Virtual Controller gateway IP address cannot be resolved. This issue is found in OAW-IAPs running AOS-W Instant 6.2.1.0- 3.3. **Workaround:** Manually configure the DHCP pool to ensure that the appropriate subnet is used for assigning IP addresses to the clients.

Limitations

Automatic DHCP Pool and IP Address Assignment

When the DHCP server is configured and if the Client IP assignment parameter for an SSID profile is set to **Virtual Controller Assigned**, the Virtual Controller assigns the IP addresses to the WLAN or wired clients. By default, the OAW-IAP automatically determines a suitable DHCP pool for Virtual Controller Assigned networks.

In the current release, the OAW-IAPs typically select the 172.31.98.0/23 subnet. If the IP address of the OAW-IAP is within the 172.31.98.0/23 subnet, the OAW-IAP selects the 10.254.98.0/23 subnet. However, this mechanism does not guarantee that it would avoid all possible conflicts with the wired network. If your wired network uses either 172.31.98.0/23 or 10.254.98.0/23, and you experience problems with the **Virtual Controller Assigned** networks after upgrading to AOS-W Instant 6.2.1.0-3.4, manually configure the DHCP pool. For more information, see *Configuring DHCP Server for Client IP Assignment* in *AOS-W Instant 6.2.1.0-3.4 User Guide.*