

AOS-W Instant 5.0.3.0-1.1 is a major software release that introduces new features and fixes to many previously outstanding issues. For details on all of the features described in the following sections, see the *AOS-W Instant 5.0.3.0-1.1 User Guide*.

What's New in this Release

This section provides a brief summary of the new features included in this release of Alcatel-Lucent Instant.

Air Monitor Mode

The **Air Monitor Mode** configures the specific OAW IAP in the Instant network in Air Monitor Mode.

Airwave Discovery through DHCP Option

You can now configure the AirWave using the DHCP option configured on the DHCP server. On the DHCP server, the format for option 60 is "ArubaInstantAP", and the format for option 43 is "amsip, ams-key".

ARM configuration options

A new tab "ARM" is added to the "Settings" link. The following configuration options are supported:

- Valid channels
- Band steering mode
- Airtime Fairness mode
- Minimum power
- Maximum power

Basic WIP rogue prevention

The OAW IAP supports the following containment methods:

- Wireless rogue scanning and identification
- Wired rogue containment
- Wireless rogue containment via de-authorization

Bandwidth Contracts

The OAW IAP supports three types of bandwidth limits:

- Percentage of Airtime: % Air Time allocated to SSID
- Each user: Per User per SSID contract specified in kbps
- Each radio: Per radio per SSID contract specified in kbps

Client Alerts

New alerts are generated for incomplete DHCP transaction for a client.

Default IP assignment by the OAW IAP

In the absence of the DHCP server, the OAW IAP can assign a default IP within the range 169.254.x.y/16 subnet to itself.

Enable/Disable telnet

A new option, **Terminal Access** is added to the **Settings > Advanced** page to enable and disable the telnet access to the OAW IAP.

Lease time for DHCP

This feature allows the administrator to set lease time for the DHCP server.

Management Authentication Setting

The UI and the CLI authentications can now be done to external RADIUS servers with this release. This can be configured in **Settings > Admin**, under the **Local** field.

Mesh

Any provisioned OAW IAP that has an ethernet link is a mesh portal, and the OAW IAP without an ethernet link is a mesh point. A mesh network can be configured only on OAW IAP-105. By default, the 5Ghz radio is always enabled on the mesh.

RADIUS Authentication Enhancements

You can now configure Internal Captive Portal with External Radius Server Authentication when Adding a Guest Network.

Role derivation

New user roles can be created and can assign new rules for the user roles.

Search in UI

Administrators can search an OAW IAP, Client or a Network using a simple Search dialog box in the UI.

SNMP Agent

Alcatel-Lucent Instant supports versions 1, 2c, and 3 of Simple Network Management Protocol (SNMP) for reporting purposes only. In other words, SNMP cannot be used for setting values in an Aruba system in the current OAW IAP.

Support for EAP-TLS

The Extensible Authentication Protocol- Transport Layer Security method supports the termination of EAP-TLS security using the internal RADIUS server.

Timezone support for logs

A new configuration option is added to **Settings > Basic** tab to allow the system administrator to configure the timezone on the Virtual Controller.

LED Display

Administrators can turn off LED for all OAW IAPs in an Instant network by selecting **Settings > Advanced > LED Display** to enable or disable the LEDs.

VSA Support

An external RADIUS server authenticates network users and returns to the OAW IAP the vendor-specific attribute (VSA) that contains the name of the network role for the user. The authenticated user is placed into the management role specified by the VSA.

Web UI idle time out

The Instant UI logs out automatically if the window is unattended for about fifteen minutes.

WPA/WPA2 PSK Configuration

The administrator can now specify a 64 byte HEX key as WPA/WPA2 PSK.

Fixed Issues

The following issues are fixed in the AOS-W Instant 5.0.3.0-1.1 release.

Table 1 *Fixed Issues*

Bug ID	Description
52799	The build-in radius server will no longer fail with long passphrase.
51801	The 5Ghz radio works successfully after bringing up from factory default and configuring an SSID.
50743	The Make PHY restart is not a non-default setting in the interference immunity feature any more.
52503	The internal DHCP server will no longer reply DHCP discover for former clients which are bridged from other APs.
—	The Auto Join option in disable mode is no more available.

Known Issues and Limitations

The following are the known issues and limitations for AOS-W Instant 5.0.3.0-1.1 release:

Table 2 *Known Issues*

Bug ID	Description
53281	If a client is using a different domain suffix from that of the APs, the DNS requests to the client's domain will be an OpenDNS when content filtering is enabled.
54000	EAP-TLS to the external RADIUS server using dynamic radius proxy does not work with large certificates which causes RADIUS packets to become fragmented.
53936	The clients after leaving the network without sending deauth frame will take about 30 minutes to disappear from the UI. This is also same for the clients on deleted SSIDs.
54213	The Country codes ID,TN,TT,VE and JM are not yet officially supported.

Mesh Support

- Mesh is supported only on dual radio access points (OAW IAP-105).
- Mesh Points consume AP capacity from the Virtual Controller system.

- The mesh onfiguration has to be synchronized with the Master by wired link before deploying.
- Mesh Parameters Limit
 - Max mesh hop count - 2
 - Maximum number of mesh points per mesh portal - 8

Self-assigned IP addresses

- Apple clients cannot access the UI when the OAW IAP's are using self-assigned IP (169.254.x.x).
When DHCP server is not present, recommend provisioning the network using a Windows or Linux client and configure static IP for the APs before using Apple clients to manage the network.
- If self-assigned IP is used by the OAW IAP, the login time gets delayed by 2-3 minutes.

NTP Server

The OAW IAP synchronizes the system time only during the boot process. After setting up a new NTP server in the UI, a reboot is required to synchronize the time with the new NTP server.

RADIUS-based Management Authentication

When RADIUS-based management authentication fails, the event is logged into 'auth-trace buf' using the special mac address "5a:00:00:00:00:00".

Contacting Alcatel-Lucent

Table 3 *Web Sites*

Web Site	
● Main Site	http://www.alcatel-lucent.com/enterprise
● Support Site	https://service.esd.alcatel-lucent.com/

Table 4 *Contact Numbers*

Telephone Numbers	
● North America	1-800-995-2696
● Latin America	1-877-919-9526
● Europe	+33 (0) 38 855 6929
● Asia Pacific	+65 6240 8484
● Worldwide	1-818-878-4507