AOS-W Instant
6.4.3.1-4.2.0.0

Alcatel·Lucent

Release Notes

Copyright

© 2015 Alcatel-Lucent. All rights reserved.

Specifications in this manual are subject to change without notice.

Originated in the USA.

AOS-W, Alcatel 4302, Alcatel 4304, Alcatel 4306, Alcatel 4308, Alcatel 4324, Alcatel 4504, Alcatel 4604, Alcatel 4704, Alcatel 6000, OAW-AP41, OAW-AP68, OAW-AP60/61/65, OAW-AP70, OAW-AP80, OAW-AP92/93, OAW-AP105, OAW-AP120/121, OAW-AP124/125, OAW-AP175, OAW-IAP92/93/105, OAW-RAP2, OAW-RAP5, and Omnivista 3600 Air Manager are trademarks of Alcatel-Lucent in the United States and certain other countries.

Any other trademarks appearing in this manual are the property of their respective companies. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al.

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.

Contents

AOS-W Instant 6.4.3.1-4.2.0.0 is a major software release that introduces new features and enhancements for OAW-IAPs.

For information on upgrading OAW-IAPs to the new release version, refer to the *Upgrading an OAW-IAP* topic in the *AOS-W Instant 6.4.3.1-4.2 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 Downloadable Regulatory Table (DRT) file versions supported by AOS-W Instant 6.4.3.x-4.2.x.x releases.

Supported DRT Versions

The following table lists the DRT file versions supported by Instant 6.4.3.x-4.2.x.x releases:

Table 2: *DRT Versions*

Instant Release Version	Applicable DRT Version
6.4.3.1-4.2.0.0	1.0_50970

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

This chapter describes the features and enhancements introduced in AOS-W Instant 6.4.3.1-4.2.x.x releases.

Features and Enhancements

This section describes the features introduced in Instant 6.4.3.1-4.2.0.0 release.

Support for New OAW-IAP Devices

Instant 6.4.3.1-4.2.0.0 release introduces support for the following new OAW-IAP devices. These new devices do not interoperate with Instant versions lower than 6.4.3.1-4.2.0.0. If these OAW-IAPs are placed into a cluster running older Instant versions such as 6.4.x.x-4.1.x.x, the devices will reboot with the **Image Sync Fail** reason. To resolve this issue, upgrade the existing cluster to minimum Instant 6.4.3.1-4.2.0.0, and then add the new OAW-IAP devices.

Table 3: *New OAW-IAP Devices*

AP Platform	Description
OAW-IAP205H	The OAW-IAP205H is a high-performance, dual-radio wireless and wired access point for small business, hospitality, and branch deployments. This device combines high-performance wireless mobility with Gigabit wired local access to deliver secure network access to dormitories, hotel rooms, classrooms, medical clinics, and multi-tenant environments. The OAW-IAP205H can be attached to a wall box using the bracket provided, or converted into a desk-mounted remote access point for branch office deployments using the AP-205H-MNTR desk mount kit. The OAW-IAP205H is equipped with a total of four active Ethernet ports (E0-E3) and USB port . MIMO (Multiple-Input, Multiple-Output) technology enables the OAW-IAP205H to provide wireless 2.4 GHz 802.11n and 5 GHz 802.11n/ac functionality, while simultaneously supporting existing 802.11a/b/g wireless services.
OAW-IAP228	The OAW-IAP228 is a fully temperature-hardened, water-resistant, indoor-rated, dual-radio IEEE 802.11ac wireless access point. This access point use MIMO technology, and other high-throughput mode techniques to deliver high-performance, 802.11ac 2.4 GHz and 5 GHz functionality, while simultaneously supporting existing 802.11a/b/g/n wireless services.
OAW-IAP277	The OAW-IAP277 is an environmentally-hardened, outdoor rated, dual-radio IEEE 802.11ac wireless access point. This access point use MIMO technology and other high throughput mode techniques to deliver high-performance, 802.11ac 2.4 GHz and 5 GHz functionality, while simultaneously supporting existing 802.11a/b/g/n wireless services.

For more information about the AP platforms, visit https://service.esd.alcatel-lucent.com.

No Support for OAW-IAP92/93

Starting with 6.4.3.1-4.2.0.0 release, Instant does not support OAW-IAP92/93 devices.

Do not upgrade an OAW-IAP cluster containing OAW-IAP92/93 devices to Instant 6.4.3.1-4.2.0.0 or later version. In case of an accidental upgrade, the OAW-IAPs will be automatically downgraded most of the time.

You can also manually downgrade OAW-IAPs to an Instant 4.0 or 4.1 release, without losing the existing configuration.

Mesh Support on 802.11ac Access Points

Starting with Instant 6.4.3.1-4.2.0.0 release, the 802.11ac OAW-IAPs, including OAW-IAP220 series, OAW-IAP27x, OAW-IAP21x, and OAW-IAP20x support Mesh configuration. For more information on Mesh OAW-IAP configuration, refer to the *AOS-W Instant 6.4.3.1-4.2 User Guide*.

Configurable ESSID in a WLAN profile

Starting with 6.4.3.1-4.2.0.0, Instant UI supports changing the ESSID of a WLAN network without deleting or recreating the entire profile. You can also search for clients by the ESSID instead of the profile name. For more information on configuring an ESSID in a WLAN profile, see *Configuring WLAN Settings for an SSID Profile* in the *AOS-W Instant 6.4.3.1-4.2 User Guide*.

Captive Portal Server Offload

Instant 6.4.3.1-4.2.0.0 release introduces the server offload feature to reduce the load on an external captive portal server, by ensuring that the non-browser client applications are not unnecessarily redirected to the external captive portal server. For more information on enabling server offload for captive portal, see *Creating a Captive Portal Profile* in the *AOS-W Instant 6.4.3.1-4.2 User Guide*.

Configurable Transmission Power Limits for Radio Profiles

In Instant 6.4.3.1-4.2.0.0, the **Customize ARM power range** option is added to the radio profile configuration window to allow administrators to set transmit power limits for a specific radio band. For more information, see *Configuring Radio Settings* in the *AOS-W Instant 6.4.3.1-4.2 User Guide*.

Custom Error Page for Web Access Blocked by AppRF Policies

In Instant 6.4.3.1-4.2.0.0, instead of showing the **Access Denied** page, you can define an ACL rule to redirect users to a specific error page when they access a blocked website. You can create a custom list of URLs that you want to use as redirect URLs and add these URLs to the ACL definition. The ACL rules with redirect URLs can be assigned to the user roles of a WLAN network profile.

For more information, see:

- *Creating Custom Error Page for Web Access Blocked by AppRF Policies* in the *AOS-W Instant 6.4.3.1-4.2 User Guide*
- **wlan access-rule** in the *AOS-W Instant 6.4.3.1-4.2 CLI Reference Guide*

Support for Multiple XML API Server Configuration

Starting with Instant 6.4.3.1-4.2.0.0, users can now configure up to four XML API servers on an OAW-IAP. The server entries can be edited or deleted if required. For more information, see *Integrating an OAW-IAP with an XML API interface* in the *AOS-W Instant 6.4.3.1-4.2 User Guide*. The users can also configure multiple XML AP server profiles in OAW-IAP CLI. For more information, see *xml-server-api* in the *AOS-W Instant 6.4.3.1-4.2 CLI Reference Guide*.

Instant 6.4.3.1-4.2.0.0 release does not support SSL2.0/3.0. If the XML server sends XML commands to the OAW-IAP using SSL2.0 as the default secure protocol, the OAW-IAP does not send any response. Alcatel-Lucent recommends that TLSv1 or higher security protocol be used when executing XML commands on an OAW-IAP.

Frame Overlay Prevention Support for External Captive Portal Users

Starting with Instant 6.4.3.1-4.2.0.0, when configuring external captive portal profiles, you can enable the frame overlay prevention feature to ensure that a frame displays a web page only if it is in the same domain as the main page. For more information, see:

- *Configuring External Captive Portal for a Guest Network* in the *AOS-W Instant 6.4.3.1-4.2 User Guide*.
- **wlan external-captive-portal** in the *AOS-W Instant 6.4.3.1-4.2 CLI Reference Guide*

RADIUS and TACACS Server for Controlling Management User Access Level

Starting with Instant 6.4.3.1-4.2.0.0, you can use the attributes returned from a RADIUS or TACACS authentication transaction to determine the access level of the user. For more information on configuring RADIUS and TACACS servers, see:

- *Configuring an External Server for Authentication* in the *AOS-W Instant 6.4.3.1-4.2 User Guide*
- The **wlan auth-server** and **wlan tacacs-server** commands in the *AOS-W Instant 6.4.3.1-4.2 CLI Reference Guide*

DNS IP Configuration for Virtual Controller

Starting with Instant 6.4.3.1-4.2.0.0, you can explicitly configure the DNS IP address for Virtual Controllers. OAW-IAPs can obtain their DNS IP addresses from per AP configuration (**ip-address** command), from the DHCP server, or from the Virtual Controller DNS IP address configuration. The Virtual Controller DNS IP address is only used for APs and does not apply to the clients connected to the APs.

For more information on Virtual Controller DNS IP, see:

- *Configuring Virtual Controller Network Settings* in the *AOS-W Instant 6.4.3.1-4.2 User Guide*
- **virtual-controller-dnsip** in the *AOS-W Instant 6.4.3.1-4.2 CLI Reference Guide*

Accounting Server Configuration in Wired Profiles

Starting with Instant 6.4.3.1-4.2.0.0, you can configure accounting servers for a wired network profile. You can either use the same server for authentication and accounting, or configure a separate accounting server. If you enable accounting for wired profile users, configure accounting server, and set an accounting interval. For more information on wired profile configuration, see:

- *Configuring a Wired Profile* in the *AOS-W Instant 6.4.3.1-4.2 User Guide*
- **wired-port-profile** in the *AOS-W Instant 6.4.3.1-4.2 CLI Reference Guide*

Country Code Selection

When the OAW-IAP-RW variants are initialized, the country code must be selected when logging in to the OAW-IAP. On selecting a country code, the OAW-IAPs operate in the selected regulatory domain and adhere to the local EIRP regulations. However, in the earlier Instant releases, if an OAW-IAP was set to an unsupported country code, radios on that OAW-IAP were disabled to avoid regulatory conflicts. In the Instant 6.4.3.1-4.2.0.0 release, the **Country Code window** displays only the supported country codes, to ensure that an OAW-IAP is always set to a supported country code and there are no regulatory conflicts.

If the supported country code is not in the list, contact Alcatel-Lucent Support team to know if the required country code is supported and obtain the software release version that supports the required country code.

Configurable USB Port Status

Starting with Instant 6.4.3.1-4.2.0.0, you can set the USB port status to enabled or disabled based on your uplink preferences. If you do not want to use cellular uplink or 3G/4G USB modems in your current network setup, you can set the USB status to disabled. By default, the USB port status is enabled.

For more information on configuring USB port status, see:

- *Changing USB Port Status* in the *AOS-W Instant 6.4.3.1-4.2 User Guide*
- **usb-port-disable** in the *AOS-W Instant 6.4.3.1-4.2 CLI Reference Guide*

Voice Traffic Prioritization

Starting with Instant 6.4.3.1-4.2.0.0, OAW-IAPs comply with Spectralink's Voice Interoperability for Enterprise Wireless (VIEW) Certification to ensure interoperability and high performance between Spectralink 84-Series, 87-Series, and 8020/8030 Wireless Telephones and WLAN infrastructure products.

You can configure the following parameters in a WLAN SSID profile for voice traffic and Spectralink Voice Prioritization:

- **Traffic Specification (TSPEC)**—Prioritizes time-sensitive traffic such as voice traffic initiated by the client.
- **TSPEC Bandwidth**—Reserves bandwidth for voice traffic.
- **Spectralink Voice Protocol (SVP)**—Prioritizes voice traffic for SVP handsets.

New Operator for Configuring VLAN Derivation Rule

In Instant 6.4.3.1-4.2.0.0, a new operator **Is the VLAN** is introduced for configuring the VLAN derivation rules. When configured, the users are assigned the VLAN value returned by the attribute in the VLAN derivation rule. For more information, see *Configuring VLAN Derivation Rules* in the *AOS-W Instant 6.4.3.1-4.2 User Guide*.

Captive Portal Support for Web Browsers with HTTP Proxy Configuration

Starting with Instant 6.4.3.1-4.2.0.0, if your browser has a proxy configuration, you can configure a captive portal proxy server or a global proxy server in the guest SSIDs for captive portal clients to match the browser configuration.

For information on configuring ports for external captive portal profiles, see:

- *Configuring External Captive Portal for a Guest Network* in the *AOS-W Instant 6.4.3.1-4.2 User Guide*
- The **captive-portal-proxy-server** parameter in the **wlan ssid-profile** command in the *AOS-W Instant 6.4.3.1-4.2 CLI Reference Guide*

No Virtual IP Address for IAP-VPN Deployments

Starting with Instant 6.4.3.1-4.2.0.0, the Virtual Controller IP address configuration is no longer required for IAP-VPN deployments.

Support for 3G/4G Modem SIM PIN Locking

OAW-IAPs support SIM PIN lock function for 3G/4G modems that support the SIM locking feature to prevent fraudulent use. The OAW-IAP can now lock and unlock the SIM PIN using the **pin-enable** and **pin-puk** parameters in the **cellular-uplink-profile** command.

For more information on SIM PIN locking, see **cellular-uplink-profile** in the *AOS-W Instant 6.4.3.1-4.2 CLI Reference Guide*

RadSec Certificate Support

Starting with Instant 6.4.3.1-4.2.0.0, you can now upload RadSec and RadSec CA certificates to the OAW-IAP. These certificates are used for client authentication when RADIUS communication over TLS is enabled. For more information, see *Uploading Certificates* and *Enabling RADIUS Communication over TLS* in the *AOS-W Instant 6.4.3.1-4.2 User Guide*.

On-demand Configuration Download

The OAW-IAPs support managed mode operations such as periodic retrieval of configuration files from a specific location. Starting with Instant 6.4.3.1-4.2.0.0, if you want to apply the configuration immediately and do not want to wait until next configuration retrieval attempt, you can use **managed-mode-sync-server** to download the configuration file.

Configuring Multiple Exclusion Ranges of IP Subnets

Dell service tag for the Dell Networking W-Series OAW-IAPs, you can configure multiple exclusion ranges of IP subnets in a local, l2 DHCP profile. Based on the size of the subnet and the configured exclusion range, the IP addresses before and after the defined range are excluded. For more information on configuring local,l2 DHCP profile, see:

- *Configuring Local DHCP Scopes* in the *AOS-W Instant 6.4.3.1-4.2 User Guide*
- **ip dhcp** in the *AOS-W Instant 6.4.3.1-4.2 CLI Reference Guide*

MTU Configuration for Uplink and Bridge Interfaces

Instant 6.4.3.1-4.2.0.0 introduces the **mtu** command to support the configuration of Maximum Transmission Unit (MTU) size for bridge (br0) and cellular uplink interfaces.

DNS-based Discovery of Provisioning AMP Server

Starting with Instant 6.4.3.1-4.2.0.0, if zero-touch provisioning fails, OAW-IAPs can automatically discover the provisioning OmniVista server and transfer OmniVista configuration to the OAW-IAP. For more information on configuring automatic discovery of provisioning AMP server, see *Enabling Automatic Discovery of Provisioning AMP server* in the *AOS-W Instant 6.4.3.1-4.2 User Guide*.

Disable Radio Per AP without Rebooting

Instant 6.4.3.1-4.2.0.0 release introduces configuration changes through the OAW-IAP CLI to disable 2.4 GHz or 5.0 GHz radio profiles without rebooting OAW-IAP or deleting the SSID.

For more information on disabling the 2.4 GHz and 5.0 GHz radio profiles, see **dot11a-radio-disable** and **dot11g-radio-disable** in the *AOS-W Instant 6.4.3.1-4.2 CLI Reference Guide*

New Telnet Command in CLI

Instant 6.4.3.1-4.2.0.0 introduces the **telnet** command using which you can initiate a telnet session with the external servers.

MAC Authentication on Guest SSID with Guest-Type Users from Internal Server

Starting with 6.4.3.1-4.2.0.0, you can enable MAC authentication for guest user profiles when captive portal authentication is disabled on a guest SSID. When splash pages profiles are not configured for a guest SSID, you can enable MAC authentication to allow guest clients to authenticate against the internal server of the OAW-IAP. For more information on configuring MAC authentication for guest users, see *Disabling Captive Portal Authentication* in the *AOS-W Instant 6.4.3.1-4.2 User Guide*.

Transmission Beamforming

Starting with 6.4.3.1-4.2.0.0, the OAW-IAP2xx access points support transmission beamforming to allow effective concentration of its signal at a client location and improve signal, SNR, and throughput.

The transmission beamforming is enabled by default. To disable this feature, use the **no vht-txbf-explicit-enable** command. For more information, see the **wlan ssid-profile** command in the AOS-W Instant *6.4.3.1-4.2 CLI Reference Guide*.

Configurable SSL Protocols

Starting with 6.4.3.1-4.2.0.0, the OAW-IAP CLI includes the **web-server** command to enable or disable SSL protocols such as tlsv1, tlsv1_1, and tlsv1_2. For more information, see the **web-server** command in the *6.4.3.1-4.2 CLI Reference Guide*.

SSH Server Change

Starting with 6.4.3.1-4.2.0.0 release, the SSH server on the OAW-RAP108/109, OAW-IAP103, OAW-IAP114/115, OAW-IAP224/225, and OAW-IAP214/215 has been changed. This change may cause SSH key exchange warnings when using an SSH client that has cached the SSH key from the previous release. This warning can be safely ignored and does not represent a security risk.

Known Issues and Limitations

This section lists the known issues and limitations in Instant 6.4.3.1-4.2.0.0.

AppRF

Table 4: *AppRF Known Issues*

Bug ID	Description
120228	**Symptom::** The AppRF deny rules for Skype sessions do not block user access. **Scenario**: This issue is found in OAW-IAPs running 6.4.3.1-4.2.0.0 or earlier releases. **Workaround**: None

ARM

Table 5: *ARM Known Issues*

Bug ID	Description
121815	**Symptom::** When client match is enabled on an OAW-IAP, some clients that prefer to connect to the 2.4 GHz band are frequently deauthenticated due to band steering. **Scenario**: When client match is enabled on the OAW-IAP, the OAW-IAP tries to direct the clients that support dual-band to use 5 GHz. If some clients such as Huawei Honor 6 Plus support dual band and yet prefer to connect to 2.4 GHz, the OAW-IAP deauthenticates the client and forces the client to reconnect frequently. This issue is found in OAW-IAPs running 6.4.3.1-4.2.0.0 or earlier releases. **Workaround**: Reduce the frequency of client match trigger by increasing the client match calculating interval and virtual beacon report (VBR) entry age (**client-match calc-interval <interval>** and **client-match vbr-entry-age <age>** parameters under the **arm** command) to a higher value.

Mesh Configuration

Table 6: *Mesh Configuration*

Bug ID	Description
122099	**Symptom**: When the 5 GHz radio profile of an OAW-IAP is configured to run in the legacy-mode (non-802.11n mode), the 802.11ac mesh link still works in the VHT mode. **Scenario**: Although the 11ac mesh link does not work in the legacy mode, the BSSID functions are not affected. This issue is found in OAW-IAP-2xx access points running 6.4.3.1-4.2.0.0 release version. **Workaround**: None