AOS-W 3.3.1.3 Release Notes

This document describes the new features and issues pertinent to the AOS-W 3.3.1.3 release.

NOTE: See the *AOS-W 3.3.1 Software Upgrade Guide* for instructions on how to upgrade your WLAN Switch to this release.

What's New in This Release

AOS-W 3.3.1 is a product feature release that introduces new software features for all Alcatel-Lucent WLAN Switches. This section describes new features and capabilities of AOS-W 3.3.1.

Hardware

AOS-W 3.3.1 supports the following new Alcatel-Lucent hardware products:

OmniAccess Supervisor Card III (OAW-S3)

The OmniAccess Supervisor Card III (OAW-S3) is a hot-swappable management module for use within an OAW-6000 modular based WLAN Switch system utilizing 400 W power supplies. The OAW-6000 is capable of containing up to four OAW-S3 modules, each of which can be configured as a master or local switch. OAW-S3 modules are compatible with existing Alcatel-Lucent line cards and supervisor cards. Specific combinations of these devices can run within the same OAW-6000 WLAN Switch. For more information, see the OmniAccess Supervisor Card Installation Guide.

NOTE: Before installing an OAW-S3 module in an existing OAW-6000 system, any supervisor card in the system must be upgraded to AOS-W 3.3.1.

Network Interfaces

You can install an OAW-S3 in any of the four slots in the OAW-6000 WLAN Switch. In this release of AOS-W, you reference the network interfaces in an OAW-S3 in the format <slot>/<port>. On the OAW-6000 WLAN Switch, the slots are allocated as follows:

- Slot 0 is the lower left slot
- Slot 1 is the lower right slot
- Slot 2 is the upper left slot
- Slot 3 is the upper right slot

An OAW-S3 or supervisor card must always be present in slot 0. You should always populate the lower numbered slots first.

On each OAW-S3, the <port> numbers start at 0 from the left-most position in the module. Ports 0-9 are gigabit ports and ports 10 and 11 are 10-gigabit ports. Both the gigabit and 10-gigabit ports are referred to as gigabitethernet interfaces. For example, enter the CLI command **show interface gigabitethernet 0/11** to view the status of a 10-gigabit port on an OAW-S3 installed in slot 0.

Licensing

OAW-S3 modules are capable of supporting up to 512 campus connected APs with the use of Alcatel-Lucent AP upgrade licenses. Contact your Alcatel-Lucent sales representative for a complete listing of available software licenses.

New and Changed CLI

The following describes new and changed CLI commands for OAW-S3 support:

- **show interface gigabitethernet** *<slot>/<port>* displays the hardware type for the interface, either Gigabit Ethernet or 10 Gigabit Ethernet.
- **show interface gigabitethernet** *<slot>/<port>* **transceiver** displays EEPROM information in the transceiver plugged into the port.
- **show inventory** displays information pertinent to the OAW-S3 module.

  NOTE If you install the OAW-S3 module in the same chassis as a Supervisor Card, running the **show inventory** command from the OAW-S3 displays information about everything in the chassis, including the Supervisor Card. Running the **show inventory** command from the Supervisor Card displays information about everything in the chassis *except* the OAW-S3.

- **show datapath utilization** displays the current CPU utilization of all datapath CPUs (the datapath in the OAW-S3 consists of multiple CPUs).
- **show datapath message-queue** displays statistics of messages received by a CPU from other datapath CPUs (only CPUs that receive messages and non-zero statistics are shown).

- **show datapath frame** displays statistics for the four slots in the OAW-6000 WLAN Switch, as you can install OAW-S3 modules in all slots.

The port monitor function is supported for OAW-S3 ports. You can specify any combination of monitor and monitored ports between Gigabit Ethernet or 10 Gigabit Ethernet ports, for example, **interface gigabitethernet 0/9 port monitor gigabitethernet 0/11**.

OmniAccess WLAN Switches

The OmniAccess WLAN Switches consists of three enterprise-class, wireless LAN switches. These switches connect, control, and intelligently integrate wireless Access Points (APs) and Air Monitors (AMs) into a wired LAN system.

The OmniAccess WLAN Switches consists of the following models:

- OAW-4504
- OAW-4604
- OAW-4704

For more information, see the OmniAccess WLAN Switch *Installation Guide*.

Network Interfaces

The OmniAccess WLAN Switches contain four multi-media (RJ-45 copper or SFP fiber) Gigabit Ethernet network interface ports. In this release of AOS-W, you reference the network interfaces in a WLAN Switches in the format <slot>/<port>, where <slot> is always 1. Port numbers start at 0 from the left-most position. For example, enter the CLI command **show interface gigabitethernet 1/0** to view the status of the left-most port on a WLAN Switch.

Licensing

You can purchase upgrade licenses for the OmniAccess WLAN Switches to increase the supported numbers of APs. Contact your Alcatel sales representative for a complete listing of available software licenses.

New and Changed CLI

The following describes new and changed CLI commands for OmniAccess WLAN Switches support:

- **show interface gigabitethernet** *<slot>/<port>* displays the active connector type for the interface, either RJ-45 or Fiber Connector.
- **show interface gigabitethernet** *<slot>/<port>* **transceiver** displays EEPROM information in the transceiver plugged into the port.
- **show inventory** displays information pertinent to the WLAN Switch.

OAW-AP85 Outdoor Access Points

The OAW-AP85 series consists of environmentally hardened, outdoor rated, dual-band IEEE 802.11a/b/g access points/air monitors, which offer excellent resilience and recovery features. This outdoor access point series is part of Alcatel-Lucent's comprehensive wireless network solution. The OAW-AP85 series works only in conjunction with an Alcatel-Lucent WLAN Switch and each AP can be centrally managed, configured, and upgraded through the switch.

For more information, see the OAW-AP85 *Outdoor Access Point Series Installation Guide*.

NOTE: In this release of AOS-W, you configure and manage the OAW-AP85 in the same way as with other Alcatel-Lucent APs. There are no CLI commands that are specific to configuration and operation of the OAW-AP85 series.

OAW-AP120 Series of Indoor Access Points

The Alcatel-Lucent series wireless access points support the draft standard of IEEE 802.11n / MIMO (Multiple-in, Multiple-out). These MIMO-capable, 802.11a/b/g/n wireless access points are available in versions with one or two radios and with integrated antennas or RP-SMA interfaces that support detachable antennas. The access points work only in conjunction with an Alcatel-Lucent WLAN Switches.

For more information, see the *OAW-120 Series AP Mounting Kit Installation Guide*.

Platform

AOS-W 3.3.1 introduces the following platform features:

Setup Wizard

The AOS-W 3.3.1 release introduces a browser-based Setup Wizard that steps you through the tasks of configuring the WLAN Switch and installing software licenses.

To access the Setup Wizard, your switch must be running AOS-W 3.3.1 in factory-default mode. If you want to use the Setup Wizard, do the following after upgrading your WLAN Switch to AOS-W 3.3.1:

From the WebUI:

1. Navigate to the Maintenance > Switch > Clear Config page.
2. Click **Continue** to return the WLAN Switch to its factory-default state.
3. At the pop-up window, click **Yes** to reboot the WLAN Switch.

From the CLI, execute the following commands:

```
write erase
reload
```

Do not issue the 'write erase all' command if you have previously installed a license in the WLAN Switch, as this command will effectively remove licenses as well as existing configurations. The Setup Wizard will display any installed licenses.

IPv6 Phase I

This release of AOS-W provides wired or wireless clients using IPv6 addressing with services such as firewall functionality, layer-2 authentication, and (with installation of the Policy Enforcement Firewall license) identity-based security. The Alcatel-Lucent WLAN Switches does not provide routing or Network Address Translation to IPv6 clients in this release.

Clients can be wired or wireless and use IPv4 and/or IPv6 addressing. This release of AOS-W requires that the default gateway for the IPv6 clients be an external router that supports IPv6. The WLAN Switch itself has an IPv4 address, and cannot route packets with IPv6 addresses. You can use the WebUI or CLI to display IPv6 client information.

IPv6 clients must be mapped to a VLAN that is bridged to an external router which provides IPv6 services to the clients. On the WLAN Switch, you can configure IPv4 and IPv6 clients on the same VLAN.

For more information about IPv6 features supported in this release, see “IPv6 Client Support” in the *AOS-W 3.3.1 User Guide*.

Packet Mirroring for Layer-2 Traffic

This release allows you to mirror traffic based on MAC flow or Ethertype. You configure the mirroring option in either the MAC or Ethertype ACL and define the destination to which mirrored packets are sent in the firewall policy. If you configure both an IP address and a port to receive mirrored packets, the IP address takes precedence. Packets can be mirrored in multiple ACLs, so only a single copy is mirrored if there is a match within more than one ACL.

This enhancement provides additional troubleshooting and debugging capabilities to monitor and debug your network.

NOTE: This feature only mirrors non-IP traffic. To mirror IP traffic, configure the mirroring option in the session ACL. You also define the destination to which mirrored packets are sent in the firewall policy. To configure session ACLs, you must install the Policy Enforcement Firewall license.

To configure mirroring for Layer-2 traffic using the WebUI, navigate to the **Configuration > Security > Access Control > Policies** page. Edit an existing Ethertype or MAC ACL or create a new one, and select the mirroring option. To add the destination IP address or port, navigate to the **Configuration > Advanced Services > Stateful Firewall > Global Setting** page. At the Session Mirror Destination field, enter the valid IP address or the destination port.

To configure mirroring for Layer-2 traffic using the CLI:

```
ip access-list eth permit (<ethtype> [<bits>]|any} mirror
ip access-list mac permit {<macaddr> [wildcard>]|any|host <macaddr>} mirror
firewall session-mirror-destination {ip-address <ipaddr>|port <slot>/<port>}
```

Location API Management Role

This release introduces the location-api-mgmt role. This role permits access to location API information only. This role does not allow the user to log in to the CLI nor does it allow the user to perform any action such as copying files or rebooting the WLAN Switch.

NOTE: For backward compatibility with previous AOS-W releases, existing user roles that have access to location API information will continue to do so.

To create a location API management role using the WebUI, navigate to the **Configuration > Management > Administration** page and click Add. Under Conventional User Accounts, enter a user name, password, and select location-api-mgmt from the Role drop-down menu. When you are finished, click **Apply**.

To create a location API management role using the CLI:

```
mgmt-user <username> location-api-mgmt <password> <password>
```

You are prompted to enter and confirm the password.

Using a third-party location appliance, you can gather information about the location of 802.11 stations. To log in to the WLAN Switch using a third-party location appliance, enter **`http[s]://<ipaddress>[:port]/screens/wms/wms.login`**. You are prompted to enter your username and password (for example, the username and password associated with the location API management role). Once authenticated, you can use an API call to request location information from the WLAN Switch, for example:
`http[s]://<ipaddress>[:port]/screens/wms/wms.cgi?opcode=wlm-get-spot&campus-name=<campus id>&building-name<building id>&mac=<client1>,<client2>...`.

VRRP Interface Tracking

This release supports VRRP interface tracking. If configured, you can track multiple VRRP instances to prevent asymmetric routing and dynamically change the VRRP master to adapt to changes in the network. VRRP interface tracking can alter the priority of the VRRP instance based on the state of a particular VLAN or Layer-2 interface. The priority of the VRRP instance can increase or decrease based on the operational state of the specified interface. For example, interface transitions (up/down events) can trigger a recomputation of the VRRP priority, which can change the VRRP master depending on the resulting priority. You can track a combined maximum of 16 interfaces.

NOTE: You must enable preempt mode to allow a WLAN Switch to take over the role of master if it detects a lower priority WLAN Switch currently acting as master.

To configure VRRP interface tracking using the WebUI, navigate to the **Configuration > Advanced Services > Redundancy** page and add a new VRRP instance or select an existing VRRP instance. At the Virtual Router page, configure the VLAN or port to track.

- To configure the VLAN, under Tracking VLAN, click New and enter the VLAN ID, enter a value to either add or subtract from the VRRP priority, and click Add.
- To configure the port, under Tracking Interface, click New and select a port from the drop-down list, enter a value to either add or subtract from the VRRP priority, and click Add.

To configure VRRP interface tracking using the CLI:

```
vrrp <id> tracking interface {fastethernet <slot>/<port>|gigabitethernet
   <slot>/<port>} {add <value>|sub <value>}
vrrp <id> tracking vlan <vlanid> {add <value>|sub <value>}
```

Disable Local Management Accounts

This release introduces the option to disable local authentication of management accounts; however, you can log in with a local management account if the authentication servers are available.

In previous versions of AOS-W, if the configured RADIUS or TACACS+ servers returned an invalid role, failed to authenticate the user, or the authentication request timed out, management users were authenticated by the local database.

In AOS-W 3.3.1, you can disable local database authentication for management users based on the results returned by the authentication servers. When enabled, locally-defined management accounts (for example, admin) are not allowed to log in if the user entry is not found in the authentication server. In this situation, if the RADIUS or TACACS+ servers return an error or fail to authenticate a user, local authentication is not used. If the authentication attempt times out, local authentication is used and you can log in with a locally-defined management account.

To disable local management authentication using the WebUI, navigate to the **Configuration > Management > Administration** page. Under Management Authentication Servers, check (select) the Local Authentication Mode checkbox.

To disable local management authentication using the CLI:

```
mgmt-user localauth-disable
```

To verify if local management authentication is enabled or disabled, use the following command:

```
show mgmt-user local-authentication-mode
```

RF Plan AP Status and Down AP Icon

This release introduces an AP status column and a down AP icon in the AOS-W RF Plan WebUI.

The status column displays the current status of each AP for the floor you are viewing within a live network.

- **Up:** AP is up (live). The corresponding AP icon on the floor map will display a live AP icon.

- **Down:** AP is down. The corresponding AP icon on the floor map will display with a red “X” over the AP icon symbolizing that the AP is down.

WebUI RF Plan Support

This release introduces planning of 802.11n high-throughput (HT) deployments, as described in D02.05 of the proposed IEEE 802.11n/MIMO (Multiple-in, Multiple-out) standard.

NOTE: In order for the WebUI RF Plan tool to import and read a standalone plan that incorporates 802.11n draft standard APs and was originally created in the Java-based standalone RF Plan tool, the plan must be exported out from the standalone tool using the WLAN Switch WebUI Format (version 3.0).

OAW-AP120 Series Support

Support of the 802.11n draft standard comes in unison with the release of OAW-AP120 Series of Indoor Access Points, which are 802.11n draft standard compliant APs. These APs can now be planned for in this release of RF Plan.

WebUI RF Plan Changes/Modifications

The following areas of the WebUI RF Plan application have been modified to support 802.11n (HT) planning (refer to the *AOS-W 3.3.1 User Guide* for complete details):

- Building Specifications Overview Page
- AP Modeling Parameters Page
- AM Modeling Parameters Page
- Floors Planning Page (including Deployed Floors Page)
- AP Planning Page
- AM Planning Page
- Area Editor Dialog Box (includes new 802.11n Zone)
- Suggested Access Point Editor Dialog Box
- Suggested/Deployed Access Points and Air Monitors Table
- Coverage Map Selections (HT Mode, Rates, Channels)

Supported Planning

This version of the WebUI RF Plan tool will aide you in the planning of legacy and/or 802.11n draft standard compliant deployments. The term legacy refers to APs that are not 802.11n draft compliant and support 802.11a and/or 802.11b/g networks only.

This version of WebUI RF Plan supports planning of the following deployment types:

- **Legacy Deployments:**

  RF Plan allows you to plan for legacy environments. Legacy refers to APs that are not 802.11n draft compliant and support 802.11a and/or 802.11b/g networks only. Planning for these environments works in the same way as previous versions of RF Plan.

- **802.11n Deployments:**

This version of RF Plan now supports planning of network environments that wish to utilize the OAW-AP120 series of indoor access points, which are 802.11n draft compliant. RF Plan supports the planning of these APs in the following capacity: 802.11a/n, 802.11b/g/n, or 802.11a/b/g/n.

NOTE: 802.11n only deployments are not supported at this time.

- **802.11n Hotspot Deployment within an Existing Legacy Environment:**

  This version of RF plan allows you to plan for an 802.11n hotspot deployment within an existing legacy environment. This type of environment requires that legacy AP/AM locations be fixed at the building level. If you set and fix the location of legacy APs prior to planning for the 802.11n APs, the legacy APs will not move when you initialize/optimize the 802.11n AP locations.

- **802.11n Hotspot Deployment and New Legacy Environment:**

  This version of RF Plan allows you to plan for a new deployment that will utilize an 802.11n hotspot and 802.11a and/or 802.11 b/g support outside of the hotspot.

  To plan for this type of deployment, start by planning your 802.11n hotspot. When you initialize and optimize the APs planned for the hotspot, the 802.11n APs will be placed within the hotspot area. However, the same AP type will also be placed outside of the hotspot area with 802.11n support disabled. RF Plan will deploy APs outside of the hotspot area based on the 802.11a and/or 802.11b/g rates defined by the system. For the system to define 802.11a and/or 802.11b/g rates, the system looks at the defined 802.11n rate and the distance covered by the defined rate; it then selects corresponding 802.11a and/or 802.11b/g rates based on the distance covered. Since the APs outside of the 802.11n hotspot area utilize 802.11a/b/g rates only, you can deploy legacy APs in their place if desired.

SSH Client from WebUI Diagnostics Page

In this release, you can perform full troubleshooting and diagnostics using the CLI through an SSH client application in the WebUI. This SSH application is available without any licensing requirement for management users in root, read-only, and network operations roles. You may be prompted to install Java software if it is not already installed in your PC.

To start the application, navigate to the **Diagnostics > General > SSH Terminal** page. When the page is loaded, the SSH Terminal application automatically sets up a connection to the switch through port 22. You must log in with the same username and password that you are currently using to access the WebUI.

NOTE: If the login does not appear, make sure that the browser cache is cleared. (In IE, go to the Tools > Internet Options page, and click the Delete Files button under Temporary Internet files.)

This feature has been tested on the following: Windows XP (IE6, IE7, Firefox 1.5, Firefox 2.0), Vista (IE7, Firefox 2.0), Redhat Linux (Firefox 2.0), Java SDK versions 1.4.2, 1.5.0 and 1.6.0.

NOTE: Command completion using the spacebar or tab does not work within the SSH client application in Mozilla Firefox browsers.

Clear Counters

This release allows you to reset additional counters/flags/state using the CLI. In addition to individual counters, the **clear counters all** command allows you to reset all relevant counters/flags.

The following are new **clear** commands in this release

```
clear aaa state messages
clear aaa state configuration
clear aaa authentication-server all
clear aaa authentication-server internal statistics
clear aaa authentication-server radius statistics
clear aaa state debug-statistics
clear aaa radius-server
clear acl hits
clear arp <ip address>
clear datapath application counters
clear datapath bridge counters
clear datapath bwm table
clear datapath crypto counters
clear datapath debug dma counters
clear datapath frame counters
clear datapath ip-reassembly counters
clear datapath maintenance counters
clear datapath message-queue counters
clear datapath route counters
clear datapath route-cache counters
clear datapath session counters
clear datapath station counters
clear datapath tunnel counters
clear datapath user counters
clear datapath wmm counters
clear dot1x counters
clear dot1x supplicant-info statistics
clear fault all
clear port link-event
clear port stats
```

Option to Disable Inter-VLAN Routing

On the WLAN Switch, you can map a VLAN to a layer-3 subnetwork by assigning a static IP address and netmask or by configuring a DHCP or PPPoE server to provide a dynamic IP address and netmask to the VLAN interface. The WLAN Switch, acting as a layer-3 switch, routes traffic between VLANs that are mapped to IP subnetworks; this forwarding is enabled by default. In this release, you can optionally disable layer-3 traffic forwarding to or from a specified VLAN.

To disable inter-VLAN routing in the WebUI, navigate to the **Configuration > Network > IP > IP Interface** page and edit the VLAN. Deselect (uncheck) the Enable Inter-VLAN Routing checkbox.

To disable inter-VLAN routing using the CLI:

```
interface vlan <id>
   ip address {<ipaddr> <netmask>|dhcp-client|pppoe}
   no ip routing
```

'show poe' Diagnostics Command

This release provides a new CLI command **show poe** that displays Power over Ethernet (PoE) information for each port on the WLAN Switch. This output returns PoE status (on or off), voltage (in mV), current (in mA), and power (in mW).

View-Only Operator Management Role

AOS-W 3.1 introduced predefined user roles (root, read-only, and guest-provisioning) that you can assign when configuring management users on the WLAN Switch. This release provides an additional network-operations role that permits access to Monitoring, Reports, and Events pages in the WebUI; this role does not allow log in to the CLI.

WebUI Usability Improvements

This release provides the following enhancements in the WebUI:

- The **Maintenance > Switch > Image Management** page shows the current software images stored in switch partitions as well as the default boot partition. This page is refreshed whenever a partition is successfully upgraded with an image file.
- The AP Provision page (available from Configuration > Wireless > AP Installation) allows you to set a fully-qualified location name (FQLN) during the AP provisioning process. Specify an FQLN in the format *<APname>.<Floor>.<Building>.<Campus>*.
- The **Configuration > Network > VLANs** page no longer displays IP address information. Refer to the **Configuration > Network > IP** page for IP address information on VLANs.

Asymmetric Bandwidth Contracts

You can manage bandwidth utilization by assigning maximum bandwidth rates, or *bandwidth contracts*, to user roles. This release allows you to configure bandwidth contracts, in kilobits per second (Kbps) or megabits per second (Mbps), for the following types of traffic:

- from the client to the WLAN Switch ("upstream" traffic)
- from the WLAN Switch to the client ("downstream" traffic)

You can assign different bandwidth contracts to upstream and downstream traffic for the same user role. You can also assign a bandwidth contract for only upstream or only downstream traffic for a user role; if there is no bandwidth contract specified for a traffic direction, unlimited bandwidth is allowed.

To create a bandwidth contract using the WebUI, navigate to the **Configuration > Advanced Services > Stateful Firewall > BW Contracts** page. Navigate to the **Configuration > Security > Access Control > User Roles** page to create or edit a user role and apply the bandwidth contract.

To create and apply a bandwidth contract using the CLI:

```
aaa bandwidth-contract 128_up kbits 128
user-role web-guest
   bw-contract 128_up per-user upstream
```

For more information about configuring bandwidth contracts, see "Configuring Roles and Policies" in the *AOS-W 3.3.1 User Guide*.

OVMM Support for All Features

All new features in this release are supported by the OmniVista Mobility Manager Appliance (OVMM).

Secure Copy for File Transfer

This release provides Secure Copy (SCP) for transferring AOS-W image file to or from the WLAN Switch, or for transferring files between the flash file system on the WLAN Switch and a remote host. The SCP server or remote host must support SSH version 2 protocol.

For information, see "Managing Files on the WLAN Switch" in the "Configuring Management Access" chapter in the *AOS-W 3.3.1 User Guide*.

Static GRE Tunnel Keepalive

This release allows the WLAN Switch to determine the status of a GRE tunnel by sending periodic keepalive frames on the tunnel. If you enable tunnel keepalives, the tunnel is considered to be "down" if there is repeated failure of the keepalives. If you configured a firewall policy rule to redirect traffic to the tunnel, traffic is not forwarded to the tunnel until it is "up". Whenever the tunnel comes up or goes down, an SNMP trap and a logging message are generated.

To enable this feature:

```
interface tunnel id
   tunnel keepalive [interval retries]
```

‘show tech-support’ Enhancement

In this release, the **show tech-support** output obscures customer-sensitive information such as passwords, encryption keys, secrets, and SNMP community strings.

Consolidated Client Integrity Module and ESI License

With this release, the features of the Client Integrity Module (CIM) and the External Services Interface (ESI) modules are available with a single ESI license. The ESI license now enables wireless and wired client remediation services before network access is granted.

Controllers running AOS-W 3.3.1 with either a CIM or ESI license already installed will be treated as though both licenses were installed. If both licenses were already installed, the system will show only a single ESI license.

Licensing Information

A new CLI command **show license limits** displays the maximum number of licensed entities supported on the WLAN Switch. This command is applicable to all switch models.

Security

AOS-W 3.3.1 introduces the following security feature and capability:

Certificate-Based Site-to-Site VPN Interoperability

This release supports certificate-based site-to-site VPN interoperability with a Cisco IOS router. The configuration is similar to configuring VPN settings between WLAN Switches, with the following requirements:

- On the Alcatel-Lucent WLAN Switch, configure a fixed lifetime under the IKE policy:

  ```
  crypto isakmp policy 1
    auth rsa-sig
    lifetime 86400
  ```

  The site-to-site VPN capabilities of AOS-W have been enhanced for this feature. You can define multiple IPSec maps for the same peer VPN device. These maps must have unique Destination-networks that do not overlap. These maps can have overlapping Source-networks.

- On the Cisco IOS router, configure the ISAKMP identity to be Distinguished Names (DN):

`crypto isakmp identity dn`

This is required for the Cisco router to send the Subject-name of the certificate as the IKE-ID. (This is standard behavior for most vendors' routers and is expected by the WLAN Switch.) This allows AOS-W to validate the digital signature during IKE Main mode negotiation.

Dynamic AAA Server Selection

In this release, the WLAN Switch can dynamically select an authentication server from a server group based on the user information sent by the client in an authentication request. For example, an authentication request can include client/user information in one of the following formats:

- <domain>\<user> — for example, corpnet.com\darwin
- <user>@<domain> — for example, darwin@corpnet.com
- host/<pc-name>.<domain> — for example, host/darwin-g.finance.corpnet.com (this format is used with 802.1x machine authentication in Windows environments)

When you configure a server in a server group, you can optionally associate the server with one or more match rules. A match rule for a server can be one of the following:

- The server is selected if the client/user information *contains* a specified string.
- The server is selected if the client/user information *begins* with a specified string.
- The server is selected if the client/user information *exactly* matches a specified string.

To configure a match rule for a server using the WebUI, add a server to a server group on the **Configuration > Security > Authentication > Servers** page. For Match Type, select **Authstring**. For Operator, select contains, equals, or starts-with, and enter the Match String.

To configure a match rule for a server using the CLI:

```
aaa server-group corp-serv
   auth-server radius-1 match-authstring starts-with host/ position 1
   auth-server radius-2 match-authstring contains abc.corpnet.com position
2
```

For more information, see "Configuring Server Groups" in the *AOS-W 3.3.1 User Guide*.

Fail-Through Authentication

This release allow you to enable *fail-through* authentication for a server group so that if the first server in the ordered group list returns an authentication deny, the switch attempts authentication with the next server in the list. The WLAN Switch attempts authentication with each server in the list until either there is a successful authentication or the list of servers in the group is exhausted.

To enable fail-through authentication for a server group using the WebUI, navigate to the **Configuration > Security > Authentication > Servers** page to configure the server group, and select the Fail Through checkbox.

To enable fail-through authentication for a server group using the CLI:

```
aaa server-group corp-serv
   auth-server ldap-1 position 1
   auth-server ldap-2 position 2
   allow-fail-through
```

For more information, see "Configuring Server Groups" in the *AOS-W 3.3.1 User Guide*.

Certificates for VPN Authentication

This release supports L2TP/IPSec with PPP/EAP-TLS using a backend RADIUS server for EAP passthrough. This release supports digital certificate authentication for site-to-site VPNs between Alcatel-Lucent WLAN switches. You can assign server and CA certificates for XAuth client authentication and for site-to-site VPNs.

For more information, see "Configuring Virtual Private Networks" in the *AOS-W 3.3.1 User Guide*.

Captive Portal Certificate Management

This release allows you to import a server certificate for captive portal into the WLAN Switch using the **Configuration > Management > Certificates > Upload** page. You can then select the certificate to be used with captive portal.

To select the server certificate for captive portal using the WebUI, navigate to the **Configuration > Management > General** page. Under Captive Portal Certificate, select the name of the imported certificate from the drop-down list.

To specify the server certificate for captive portal using the CLI:

```
web-server
   captive-portal-cert <certificate>
```

For more information, see "Configuring Captive Portal" in the *AOS-W 3.3.1 User Guide*.

‘show ap’ Enhancement

In this release, the **show ap debug system-status** output displays the reason for an AP rebootstrap.

VPN Dialer for Windows Vista Clients

This release allows you to configure a VPN dialer for Windows Vista clients. A VPN dialer is a Windows application that configures a Windows client for use with the VPN services in the WLAN Switch. Configuring a VPN dialer for Windows Vista clients is identical to configuring a dialer for Windows 2000 or Windows XP clients.

For more information about configuring a VPN dialer, see “Configuring Virtual Private Networks” in the *AOS-W 3.3.1 User Guide*.

Wireless

AOS-W 3.3.1 introduces the following wireless features and capabilities:

AP Maintenance Mode

You can configure APs to suppress traps and syslog messages related to those APs. Known as AP maintenance mode, this new setting in the AP system profile is particularly useful when deploying, maintaining, or upgrading the network. AP maintenance mode is disabled by default. If enabled, APs stop flooding unnecessary traps and syslog messages to network management systems or network operations centers during a deployment or scheduled maintenance.

To configure AP maintenance mode using the WebUI, navigate to the **AP Configuration** page, select either the AP group or specific AP, and then select the AP system profile. Under Profile Details check (select) the Maintenance Mode checkbox to enable AP maintenance mode, or clear (deselect) the Maintenance Mode checkbox to disable AP maintenance mode.

To configure AP maintenance mode using the CLI:

To enable AP maintenance mode:

```
ap system-profile <profile>
   maintenance-mode
```

To disable AP maintenance mode:

```
ap system-profile <profile>
   no maintenance-mode
```

Viewing AP maintenance mode information

To view the maintenance mode status of APs, use the following commands:

```
show ap config
show ap debug system-status
```

On the local WLAN Switch, you can also view maintenance mode status using the following commands:

```
show ap details
show ap active status
show ap database
```

For more information see "AP Maintenance Mode" in the *AOS-W 3.3.1 User Guide*.

Configurable WMM AC to DSCP Mapping

The IEEE 802.11e standard defines the mapping between Wi-Fi Multimedia access categories (WMM ACs) and the Differentiated Services Codepoint (DSCP) tags. In previous Alcatel-Lucent AOS-W releases, WMM AC to DSCP mapping used the fixed mapping defined by the IEEE 802.11e standard. Beginning with AOS-W 3.3.1.3, you can use the WMM AC mapping commands to customize the mapping between WMM ACs and DSCP tags. You apply and configure WMM AC mappings to a WMM-enabled SSID profile.

NOTE: The user-configured mapping only takes effect when WMM is enabled for the SSID profile.

To configure WMM mapping using the WebUI, navigate to the applicable SSID profile in the **Virtual AP** profile. Under **Profile Details**, select the Advanced tab. Scroll down to the Wireless Multimedia (WMM) option to enable WMM. After enabling WMM, modify the DSCP mapping by entering the desired value in the DSCP mapping for voice, video, best-effort, and background fields. Click **Apply**.

To configure WMM mapping using the CLI:

```
wlan ssid-profile <profile>
   wmm
   wmm-be-dscp <best-effort>
   wmm-bk-dscp <background>
   wmm-vi-dscp <video>
   wmm-vo-dscp <voice>
```

For more information, see "Optional Configurations" in the "Configuring QoS for Voice" chapter in the AOS-W 3.3.1.3 User Guide.

NOTE: You can also see the bug ID 24605 for more information.

IEEE 802.11n Draft Standard Support

This release introduces core 802.11n high-throughput (HT) functionality, as described in D02.05 of the proposed IEEE 802.11n/MIMO (Multiple-in, Multiple-out) standard.

MIMO technology, an imminent IEEE standard of 802.11n, is an unlicensed band Wi-Fi ODFM modulation technology, operating in the 2.4-2.5 GHz and 5 GHz bands, that leverages multiple 802.11 radios on a single radio chip (up to three),

simultaneously transmitting and receiving to improve RF signal integrity. This enhanced signal integrity dramatically reduces the effects of multi-path and increases both the usable coverage area as well as overall wireless throughput.

NOTE: Support of the 802.11n draft standard comes in unison with the release of the OAW-AP120 Series of Indoor Access Points, which are 802.11n draft standard compliant APs.

The following items from the 802.11n draft standard are supported in this release of AOS-W:

- Spatial Multiplexing with two streams
- A-MPDU aggregation/de-aggregation
- Block Acknowledgements
- 40 MHz Channel Operation in both 2.4 GHz and 5 GHz bands
- Short Guard Interval in 40 MHz Operation
- MIMO Power-Save

New Profiles/Commands
Configuration of HT functionality is split into two new profiles, the high-throughput radio profile, and the high-throughput SSID profile. The radio profile contains parameters that apply to all SSIDs on a given radio. The SSID profile contains parameters applicable to a specified SSID.

- rf ht-radio-profile
- wlan ht-ssid-profile

Modified Profiles/Commands

The following profiles/commands have been modified to support 802.11 (HT) configuration and operation:

- ap enet-link-profile
- ap regulatory-domain-profile
- ids dos-profile
- ids unauthorized-device-profile
- rf arm-profile
- rf dot11a-radio-profile
- rf dot11g-radio-profile
- wlan ssid-profiles
- wlan virtual-ap

Troubleshooting and Display Commands

The following commands have been extended or added to show information about 802.11 (HT) configuration and operation:

- show ap configuration
- show ap debug received-config
- show ap association
- show ap bss-table
- show ap debug system-status
- show ap debug radio-stats
- show ap debug client-stats
- show ap debug client-table
- show station-table
- show user-table
- show ap ht-rates bssid

Mesh

This release supports the Alcatel-Lucent secure enterprise mesh solution. Mesh is an effective way to expand your network by bridging multiple Ethernet LANs or extending your wireless coverage. As traffic traverses across Alcatel-Lucent APs configured for mesh, the mesh network automatically reconfigures around broken or blocked paths. This self-healing feature provides increased reliability and redundancy: the network continues to operate if an AP goes faulty or a connection fails.

To configure the secure enterprise mesh solution, you must install a mesh software license on a switch as a software license key. There are several mesh software licenses available that support different maximum number of APs and AP types. Depending on your deployment, you purchase Secure Enterprise Mesh licenses for indoor and outdoor APs.

For more information, see the "Configuring Secure Enterprise Mesh" chapter in the *AOS-W 3.3.1 User Guide*.

Remote AP Split Tunneling

This release supports remote AP split tunneling. This feature allows you to optimize traffic flow by directing only corporate traffic back to the WLAN Switch, while Internet access and printer traffic remains local. With split tunneling, a remote user associates with a single SSID, not multiple SSIDs, to access corporate and local resources. The remote AP examines session ACLs to distinguish between corporate traffic destined for the WLAN Switch and local traffic.

You must install the Policy Enforcement Firewall license in the WLAN Switch.

For more information, see "Split Tunneling" in the "Configuring Remote APs" chapter in the *AOS-W 3.3.1 User Guide*.

Remote AP Backup Configuration

This release allows you to define a backup configuration in the virtual AP profile on the WLAN Switch. This configuration operates the remote AP if the WLAN Switch is unreachable. The remote AP checks for configuration updates each time it establishes a connection to the WLAN Switch. If a change is detected, the remote AP downloads the configuration changes.

To define the backup configuration in the WebUI, navigate to the **Configuration > Wireless > AP Configuration** page, select either an AP group or individual AP, select Wireless LAN, then Virtual AP. Under Profile details, select a mode of operation from the Remote-AP Operation drop-down list.

To define the backup configuration using the CLI:

```
wlan virtual-ap <name>
   rap-operation {always|backup|persistent|standard}
```

For more information, see "Backup Configuration" in the "Configuring Remote APs" chapter in the *AOS-W 3.3.1 User Guide*.

Remote AP DNS-Based Controller Setting

This release supports provisioning remote APs with the master WLAN Switch host name. If the remote AP gets multiple IP addresses in response to a host name lookup, the remote AP can use one of them to establish a connection to the WLAN Switch.

To provision the remote AP with the master WLAN Switch host name in the WebUI, navigate to the **Configuration > Wireless > AP Installation > Provision** page and enter the host name of the WLAN Switch.

To provision the remote AP with the host name of the master WLAN Switch using the CLI:

```
provision-ap
   master <name>
```

For more information see the "Configuring Remote APs" chapter in the *AOS-W 3.3.1 User Guide*.

Remote AP ACLs

This release introduces support of the following ACLs for remote APs:

- Standard ACLs—Permit or deny traffic based on the source IP address of the packet. You apply these ACLs to a user role.
- Ethertype ACLs—Filter traffic based on the Ethertype field in the frame header. You apply these ACLs to a user role.
- MAC ACLs—Filter traffic on a specific source MAC address or range of MAC addresses. You apply these ACLs to user roles.

- Firewall policy (session ACLs)—Identifies specific characteristics about a data packet passing through the Alcatel-Lucent switch and takes some action based on that identification. You apply these ACLs to a user role and an uplink port.

For more information, see the "Configuring Remote APs" chapter in the *AOS-W 3.3.1 User Guide*.

AP Slow Link Support

This release provides enhancements for APs operating over high-latency or low-bandwidth WAN connections. Alcatel-Lucent recommends the following in such environments:

- Connect APs and WLAN Switches over a link with a capacity of 1 Mbps or greater.
- Maintain a minimum link speed of 64 Kbps per GRE tunnel and per bridge-mode SSID. This is the minimum speed required for downloading software images.
- Prioritize AP heartbeats to prevent losing connectivity with the WLAN Switch.

  To prioritize AP heartbeats in the WebUI, navigate to the AP system profile page. Under profile details, enter a value in the Heartbeat DSCP field.

  To prioritize AP heartbeats using the CLI:

  ```
  ap system-profile <profile>
    heartbeat-dscp <number>
  ```

For more information, see "Deploying APs Over Low-Speed Links" in the "Configuring Access Points" chapter in the *AOS-W 3.3.1 User Guide*.

AP Failback Mechanism

The AP failback feature allows an AP associated with the backup WLAN Switch (backup LMS) to fail back to the primary WLAN Switch (primary LMS) if it becomes available.

To configure this feature you must:

- Configure the LMS IP address
- Configure the backup LMS IP address
- Enable LMS preemption
- Configure the LMS hold-down timer

To configure AP failback in the WebUI, navigate to the AP system profile page. Under profile details, enter the LMS and backup LMS IP addresses, click (select) the LMS Preemption checkbox, and enter a value in the LMS Hold-down period field.

To configure AP failback using the CLI:

```
ap system-profile <profile>
   lms-ip <ipaddr>
   bkup-lms-ip <ipaddr>
   lms-preemption
   lms-hold-down-period <seconds>
```

For more information see “Layer-3 Redundancy” in the “Configuring Access Points” chapter in the *AOS-W 3.3.1 User Guide*.

Layer-3 Redundancy Options for APs

In earlier AOS-W releases, Layer-3 redundancy was accomplished using a backup LMS IP address. The AP would learn that IP address after associating with a WLAN Switch and downloading its configuration. However, if the AP was unable to initially associate with a WLAN Switch, the AP would not boot or learn the backup LMS IP address.

In this release of AOS-W, in addition to the backup LMS IP address, the AP can learn multiple WLAN Switch IP addresses. The AP attempts to boot using the first learned IP address. If there is no response, the AP continues with other discovery methods until it finds an available WLAN Switch with which to establish a connection. The AP attempts to find an available WLAN Switch IP address, as described below:

- When using DNS, the AP can learn multiple IP addresses to associate with a WLAN Switch. If the primary WLAN Switch is unavailable or does not respond, the AP continues through the list of learned IP addresses until it establishes a connection with an available WLAN Switch.
- When using DHCP option 43, the AP accepts only one IP address. If the IP address of the WLAN Switch provided by DHCP is not available, the AP can use the other IP addresses provisioned or learned by DNS to establish a connection.

For more information, see “Deploying APs” in the “Deploying a Basic Alcatel-Lucent User-Centric Network” chapter in the *AOS-W 3.3.1 User Guide*.

Ekahau Tag Interoperability

This release supports integration of the Ekahau real-time asset location services (RTLS).

To enable APs to send RFID tag information to an Ekahau server, enter the IP address, port number, key, and station message frequency for the server in the AP system profile. Ekahau, Pango and Aeroscout RFID tags are supported.

Support for OVMM as an RTLS Server

This release supports integration of the Mobility management system as a real-time asset location services (RTLS) server. Ekahau, Pango and Aeroscout RFID tags are supported.

To enable APs to send RFID tag information to the OVMM server, in the Management General profile enter the port number that OVMM will use to receive RTLS information, and the transmission interval, as part of the Mobility Manager Servers configuration. The port number and interval must match what is configured on the OVMM server. The default is port 8000, and an interval of 60 seconds.

Multicast Rate Optimization

This release provides a new option to the SSID profile to enable scanning of all active stations currently associated to an AP to select the lowest transmission rate for broadcast and multicast frames. By default, this option is disabled. This option only applies to broadcast and multicast data frames; 802.11 management frames are transmitted at the lowest configured rate.

NOTE: Do not enable this option unless instructed to do so by your Alcatel-Lucent representative.

Voice

This release of AOS-W introduces the following voice features and capabilities:

H.323 ALG

This feature allows H.323 clients to register to the gatekeeper and make and receive calls through the gateway using H.323 protocol suites. H.323 is an International Telecommunications Union (ITU) standard for multimedia communications across IP-based networks. This feature requires the Voice Services Module license.

Additional network services svc-h323-udp and svc-h323-tcp allow H.323 message exchanges on ports 1718 (UDP), 1719 (UDP and TCP), and 1720 (TCP). You can configure these services in user role policies.

Voice Monitoring for Non-SIP Protocols

Prior to this release, Call Detailed Report (CDR) and Quality Reports (including Transmission Rating Value calculations) were generated for Session Initiation Protocol (SIP)-enabled calls only. With this release, this data is also available for non-SIP enabled calls, such as calls enabled through protocols such as NOE, SVP, SCCP, Vocera, etc. The following CLI commands now provide an optional protocol identifier that identifies the VoIP protocol that a client uses to make or receive calls:

```
show voice client-status proto <proto_id>
show voice call-cdrs proto <proto_id>
show voice call-counters proto <proto_id>
show voice call-quality proto <proto_id>
show voice call-perf proto <proto_id>
show voice call-density proto <proto_id>
```

```
show voice call-stats proto <proto_id>
```

Issues and Limitations Fixed in AOS-W 3.3.1.3

The following issues and limitations have been fixed in the AOS-W 3.3.1.3 release:

Bug ID	Description
25345	The issue with clients not able to authenticate in a LEAP setup using Cisco ACU version 4.x has been fixed.

Issues and Limitations Fixed in AOS-W 3.3.1.2

The following issues and limitations have been fixed in the AOS-W 3.3.1.2 release:

Bug ID	Description
25244	The issue with the command show datapath user looping when an IPv6 and IPv4 user are on the same hash chain has been fixed.
25238	The issue with IPv6 packets looping between auth and SOS when there is no station entry in auth has been fixed.
25232	The WLAN Switch rebooting due to datapath timeout has been fixed.
25030	The switch now reloads with the Alcatel-Lucent setup wizard.
25001	The WLAN Switch rebooting due to a watchdog time out has been fixed.
24950	The issue with random AP reboot has been fixed.
24828	The issue with low bandwidth while running in split-tunnel mode has been fixed.
24704	When a wireless phone roams to another AP, it sends ARP and DHCP requests. In a large VoWLAN deployment, this generates heavy broadcast traffic in the air resulting in a drop of broadcast and multicast traffic in the air. You can now enable the ***voip-proxy-arp*** option to convert all broadcast ARP requests to unicast and prevent traffic loss.
24598	The issue with the **show ap monitor debug status** command displaying incorrect AP scanning status has been fixed.
24596	APs attached to switches with different time settings would not detect inactive GRE tunnel after failover tests. This issues has been fixed.
24417	When the controlled is reloaded, the **show wms general** command now displays correct value for ***classification-server-ip*** option.
24415	The issue with the **snmp-server host** command being removed from the running config after the **snmpd** is restarted has been fixed.

Bug ID	Description
24394	The Hello packets will not send fixed and provisioning information as strings in request. This fixes the issue of APs with longer **`ap-name`** or **`ap-group-name`** not starting
24365	An AP is sometimes classified as a suspect-rogue even though it should be a rogue AP. This happened due to the presence of the gateway MAC address in the APs' wired MAC table. This is now fixed and further checks are implemented to classify the AP as a rogue AP.
24358	The ARM power upgrade issue has been fixed.
24350	If the mac or eth ACL is deleted from a role, the deletion is now propagated to a remote AP.
24343	If a wired user plugs a machine into the port before the AP has downloaded its config from the WLAN Switch, the wired user would not be assigned to the correct AP group and thus the rules that were AP group specific would not apply. This is now fixed to update the AP group on existing wired users.
24211	The duplicate ID problem in the **`show login sessions`** command output has been fixed.
24209	The **`show audit-trail`** [***`value`***] command has been fixed to accept only a numeric value.
24153	The issue with the switch rebooting at large bursts of un-encrypted traffic has been fixed.
24119	RAP upload speeds have been increased, eliminating an occasional cause of watchdog timeouts at high upload rates.
24076	Fragmented data are now re-assembled after decryption as a single PDU enabling AP to forward the re-assembled data.
24064	A bug on the WLAN Switch leaks the broadcast frames after conversion to unicast to other VLAN. This has been fixed to forward unicast frames only to clients on VLAN of the broadcast packet.
24041	The captive portal redirect URL now uses the Common Name found in an uploaded SSL certificate.
24008	Under some conditions, transmitting greater than 7Mbps of upstream UDP traffic may cause Remote APs to reboot. This issue has been fixed.
23956	The issue with dbsync memory leak has been fixed
23918	Path MTU value is reduced to allow RAP to function properly.
23868	The a-tx rates and g-tx rates from the mesh-radio-profile can be applied on mesh points and mesh portals, making the base rates identical to the tx-rates
23754, 23915, 23916	Multiple issues with Remote Mesh Portal has been fixed.
23753	An AP will now accept two or more PMKIDs contained in an association request as per the 802.11i specification.

Bug ID	Description
23704	The issue with a switch randomly re-booting with the "Datapath Time Out" cause message has been fixed.
23662	SNMP will now clear the memory when OVMM is removed from a WLAN Switch.
23606	The issue with OAW-AP65 rebooting during a packet capture has been fixed.
23570	A radius server disabled in a 2.x config is automatically enabled in 3.x config. This issue has been fixed
23569	The 2.5 to 3.2 configuration upgrader has been fixed to correctly migrate settings for ARM minimum and maximum transmit power
23472	A session initiated from the call manager is allowed to the client in addition to the one initiated by the client. This fixes the QoS issue for a call from a land line phone to a wireless handset
23436	The issue with an AP61 not connecting with a Cisco 3550 after upgrading to AOS-W 3.2 has been fixed
23370	The max EIRP value for SG (Singapore) country code is set to 23 dBm for 2.4 GHz in all APs
23367	The max EIRP value for MY (Malaysia) country code is set to 27 dBm for the 2.4 GHz band in all APs
23321	SOS adds a route cache entry only if it is an ARP response.
23302	If a RAP was not connected to any switch with the UP state, on a switch tunnel directive, it would now try to switch over to the next switch instead of rejecting that RAP.
23273	A problem has been repaired that caused the AP's CPU to become overloaded under some conditions.
23223	The AP debug show commands now properly report GRE tunnel heartbeats sent and received.
23203	The Enet1 port on a Remote OAW-AP70 will now properly autonegotiate their link at all times.
23141	The RAP watchdog timeout issue while attaching clients has been fixed.
23115	The issue with the "show netstat" command not working when the "ip name server" is configure is fixed
23090	Wired devices are now able to pass traffic properly to the Enet1 port on a Remote OAW-AP70.
23088	The filter search option for MAC/CP authenticated under Monitoring > Switch > Clients have been fixed.
23076	The WebUI Policy configuration screen is now displayed properly.
23075	After a Remote OAW-AP70 reboot, wired devices attached to the Enet1 port will now authenticate correctly.
22957	Remote APs will now correctly establish a connection with the LMS-IP and backup LMS-IP.

Bug ID	Description
22930	The out of memory issue due to high throughput has been fixed.
22911	Under some conditions, bulk provisioning of Remote APs would cause a portion of those APs to fail to boot. This has been fixed.
22902	A switch reboot issue has been fixed.
22898	An AP crash has been fixed.
22867	WebUI error messages displayed when configuring AP groups have been fixed.
22616	Wired port session ACL information is now displayed correctly in the “show acl hits” command.
22559	Air Monitors and Access Points can be configured to not ignore the HSRP MAC address for Rogue AP detection
22354	The issue with high packet loss occurring on the OAW-S3 and WLAN Switch while sending AES-CCM and TKIP encrypted fragmented "ping" packets to the WLAN Switch's IP address has been fixed.
22303	PPPoE was not used on APs as it might have caused frequent AP reboots.
21821	Call status is now reported correctly in the output of the “show ap association voip-only” command.
21405	Discrepancies in rogue confidence level information in the CLI and WebUI have been fixed
21108	The issue with SNMP query for user phy type has been fixed.
21098	If a virtual AP in bridge mode were used as a remote AP and the SSID name was changed on the virtual AP, the group key was not created, which would block some traffic.
21006	When SVP was enabled, background data traffic could degrade voice quality.
20929	When a new VLAN is created and added to two existing ports, they were not added to the two trunk ports of an allowed VLAN list. Instead, one of the ports would become an access port for the VLAN. This issue has been fixed.
19913	The number of clients reported via SNMP was not correct.
19494	The issue with excess bi-directional UDP traffic causing the mesh wireless link to flap has been fixed.
18651	When using Internet Explorer 7, line cards in the OAW-6000 WLAN Switch were not displayed correctly in the WebUI Monitoring > Switch > Ports page.
18530	If you enabled stateful dot1x, users might not always be assigned the correct role.
18449	When connecting APs across low-speed links, such as 64 Kbps WAN connections, the image download process that occurs when the switch software is upgraded may fail to complete using FTP. This caused the AP to fall back to TFTP, which takes much longer to complete.

Bug ID	Description
18331	With AAA FastConnect (EAP termination) enabled, a client that reboots and comes back up on the same AP may experience connectivity problems for up to 120 seconds. This was caused by the switch attempting to use the previous encryption key rather than restarting full authentication.
18276	From a local switch, issuing a “ping” to the master switch's IP address followed immediately by a “ping” to the master switch's VRRP address (for redundant configurations) caused the second ping to fail.
18268	WebUI performance was unacceptably slow.
18047	If a station authenticated using WPA or WPA2 moves to a different SSID on the same physical AP, and the new SSID is also configured for WPA or WPA2, the switch attempted to use the previous encryption key and sent EAPOL-KEY messages rather than restarting full authentication using EAPOL START messages. This behavior occurred only when AAA FastConnect was enabled, and caused authentication to fail for this station for approximately 120 seconds.
17096	A server certificate could not be uploaded in DER format.
17020	Using Internet Explorer, the WebUI was very slow when displaying a large number of virtual AP profiles on the All Profiles page.
16165	When the “Send null packets” option was selected for location tracking, only APs sent null frames. Air Monitors (AMs) did not send null frames.
16110	The `deny-time-range` parameter in the Virtual AP profile did not work correctly.
15883	Under some conditions, ARM did not properly maintain a full list of neighboring APs.
15836	A compatibility problem existed between an Alcatel-Lucent WLAN Switch and an Oracle Internet Directory version 9.02 server when performing LDAP over SSL authentication.
14926	If the administrator made a change to an L2TP pool, existing L2TP sessions were disconnected. Under some circumstances, this could cause remote APs to not re-establish connectivity properly in a timely manner.
11570	When AAA FastConnect (EAP Termination) was enabled on a profile applied to wired ports, wired 802.1x did not work.
7641	Ad-hoc containment was much less effective on the OAW-AP60/61 than it was on dual-radio APs such as the OAW-AP65 and OAW-AP70.

Known Issues and Limitations in AOS-W 3.3.1.2

The following are known issues and limitations for this release of AOS. Where bug IDs or workaround are applicable, they are included.

Bug ID (if any)	Description
25162	In this release, OAW-S3 and WLAN Switches do not support VRRP pre-emption. Workaround: After both VRRP pairs return to operational state, manually "shutdown" and "no shutdown" the current VRRP master instance to trigger VRRP backup instance with higher priority to take over.
25134	Setup Wizard: If there are any configuration errors when the user clicks the Finish button, an error message appears in a dialog box and the wizard stops sending configuration commands to the WLAN Switch. Workaround: Power down the WLAN Switch, then power it on again. Restart the wizard.
25132	After upgrading Alcatel-Lucent WLAN Switches to AOS-W 3.3.1 software release, the "Acceptable Coverage Index" value should be left as-is and the “Ideal Coverage Index" value should be set to 10, under the "rf arm-profile". This is required to allow Alcatel-Lucent APs to utilize max-power settings, if allowed by the Adaptive Radio Management (ARM).
25114	Adhoc containment for 802.11a/b/g APs is not functional in the 5GHz band.
25109	ACL new hits and total hits may show incorrect values for "redirect src-nat" enabled session ACLs.
25107	Setup Wizard: Changes to the default speed and duplex mode for a port are not applied. Workaround: After completing the Setup Wizard and rebooting the switch, use the CLI or WebUI to change the speed or duplex mode for a port.
25057	User may temporarily get assigned to the logon role instead of the initial role in the AAA profile. Workaround: Reauthenticate the client device.

Bug ID (if any)	Description
25043	Without active AP licenses on the M3 and 3000 platforms, it is not possible to provision a remote AP. Workaround: Temporary AP licenses on the same WLAN Switch can be used to enable remote AP provisioning. Another WLAN Switch with available AP license limit can also be temporarily used to provision the correct parameters on the remote AP.
25042	SIP calls are allowed even if the voip-cac-profile configuration has the VoIP SIP Call capacity set to "0".
25031	When users select a different server group for the authentication server group, the WLAN Switch WebUI will display a message; this message can be ignored.
25022	The **`show auth-tracebuf`** command may not work as expected after "user debugging" is enabled and then disabled
25017	Adhoc network detection will also trigger interfering ap detection against the adhoc network devices; this alarm can be ignored.
24995	Setup Wizard: If the user moves the port on which the Setup Wizard is connected from VLAN 1 to a new VLAN, the web browser window will hang after the user clicks the Finish button. Workaround: The user just needs to close the browser window. The configuration is written properly to the WLAN Switch.
24951	This release does not support wireless containment on the OAW-AP124 and OAW-AP125 802.11n access points.
24942	Setup Wizard: The month, day, and year in the Date & Time drop-down menus do not reflect changes made with the calendar icon. Workaround: Enter the month, day, and year using the drop-down menus.
24882, 24685	State of APs terminated on the local WLAN Switch can sometimes be reported differently on the master WLAN Switch. Workaround: Use the **`show ap active`** command in the local WLAN Switch CLI to monitor AP states that are terminated on the local WLAN Switch.
24778	Not able to configure the role-based reauthentication interval from the WLAN Switch CLI. Workaround: Use the WLAN Switch WebUI to configure the role-based reauthentication interval.
24761	Enabling port mirroring on a 1 Gbps port to a 100 Mbps port is not supported on OAW-S3 and WLAN Switches. Port mirrors should be disabled whenever not in use in order to prevent performance impact on these type of WLAN Switches.

Bug ID (if any)	Description
24749	The 40MHz channel cannot be enabled against the "KR" country code for the OAW-AP124 and OAW-AP125.
24748	Not able to add channels to the regulatory domain using the WLAN Switch WebUI. Workaround: Use the WLAN Switch CLI to add channels to the "ap regulatory-domain" configuration.
24628	The following relates to bridging devices connected to the wired Ethernet ports of a mesh portal or mesh point: ■ Wired AP profile—If a parameter in the Wired AP profile is modified, it will not take effect until the user toggles the “wired-ap-enable” flag. To do this, you must use the “no wired-ap-profile” command followed by the “wired-ap-enable” command for the change to be applied. ■ Native VLAN in the AP system profile—If the user connects the mesh portal to a trunk port on the WLAN Switch and the trunk native VLAN of that port has a value other than the default of 1, you must also set the native VLAN in the AP system profile to that value.
24601, 24724	The WLAN Switch WebUI may show the number and state of APs and AMs incorrectly. Workaround: Use the **`show ap active`** command in the local WLAN Switch CLI to monitor AP states that are terminated on the WLAN Switch.
24428	When all of the servers in a server group time out, the next authentication attempt will wait until the "dead timer" expires.
24330	Failed captive-portal authentication attempt shows the default captive portal page and not the customized background.
24234, 23496	During Alcatel-Lucent WLAN Switch upgrade, FTP and SCP should be used as the preferred image transfer methods. Using TFTP as the image transfer method may cause transfer timeouts to occur.
24219	User VLAN may not show correctly in the WLAN Switch WebUI. Workaround: Use the **`show user`** command in the WLAN Switch CLI to verify correct client VLAN assignment.
24178	The WLAN Switch's DHCP server may not send a DHCP NAK when the client roams from a different layer-3 subnetwork and tries to renew its old IP address on the new VLAN. When this happens, the client is unable to obtain the IP address on the new subnetwork. This issue does not occur when an external DHCP server is used or layer-3 mobility is enabled on the WLAN Switch. Workaround: When using the WLAN Switch's DHCP server, force a release/renew of the DHCP lease on the client.

Bug ID (if any)	Description
24148	Atheros 11n chipset installed clients may associate at the 54Mbps 802.11 rate after "stm kick-off station" command or after OAW-AP124/OAW-AP124 channel change. Workaround: Reassociate the client to the OAW-AP124/OAW-AP125.
24147	VLAN assignment might be wrong during MAC authentication. Workaround: Disable dos-prevention if this problem is observed.
24108	The WebUI and the CLI prevents configuration of an OAW-AP70 to use internal antennas for one radio and external antennas for the other radio.
24063	For APs that discover the master WLAN Switch using DNS, WLAN Switch discovery will fail if the DHCP server returns more than one domain name.
24061	WebUI/CLI: Radius server status is always "Up" or "Inservice". Workaround: Use "ping" or other mechanisms to verify network connectivity with the RADIUS server and verify that RADIUS service is still enabled and running on the server in case of authentication timeouts.
24042	Changing the IPSEC key on a master/local deployment with VRRP enabled causes a loss of connectivity until the master WLAN Switch is rebooted. Workaround: Manually trigger a VRRP state change from master to backup, then return it to master.
24017	When using an 802.11e-capable device with TSPEC, the AP does not respond properly to an ADDTS request.
23957	The association table of the OAW-AP80M configured for static WEP may fill up with invalid entries over time, preventing further client association.
23949	PPPoE should not be used on remote APs operating in split-tunnel mode or if it has offline (backup/always) mode virtual APs. If clients connect to split-tunnel or offline (backup/always) virtual APs on a PPPoE remote AP, traffic is not passed to bridged destinations.
23929	APs do not respond to SNMP queries even though SNMP has been enabled.
23907	This release does not support Xsec opmode SSIDs for the OAW-AP124 and OAW-AP125.
23893	Bandwidth contracts do not work properly on the OAW-S3 and WLAN Switches.
23880	Radius uptime may reset to 0:0:0 after a few minutes of high load of 802.1x authentication; no service outage will be observed.

Bug ID (if any)	Description
23859	Forced classification of "suspect-unsecure AP" to "interfering AP" may fail. Workaround: Change state of the AP to classification type "unsecure" and then re-classify as "interfering".
23792	Some packet loss might be observed on OAW-AP70 eth1 port.
23736	Wired rogue AP containment does not work properly if multiple VLANs have been trunked to an AP. The AP will only perform wired-side rogue containment for an AP on its own VLAN.
23735	Single-radio APs may take an excessive amount of time to detect rogue APs on their non-preferred band, due to the amount of time it takes the internal radio to change between 2.4GHz and 5GHz bands. Workaround: Use dedicated air monitors or deploy dual-radio access points.
23719	After changing the IP address of a master WLAN Switch, local WLAN Switches may not re-build their IPSEC tunnel to the master. Workaround: Reboot the local WLAN Switch.
23713	Checkbox selections may get lost after WebUI auto refresh.
23690	APs will only show up under the WebUI “unprovisioned” link if the following is true: ■ The AP is using external antennas and no gain values have been provisioned. ■ The AP’s group does not exist on the WLAN Switch. ■ The AP has the same name as another AP which is up. For this reason, most APs such as the OAW-AP60 or OAW-AP65 will never show up as “unprovisioned.”
23669	SNMP total AP count will not include APs that do not have VAPs enabled. Workaround: Use the "show ap active" command on the WLAN Switch to monitor the total AP count
23631	LDAP authentication does not differentiate between server unreachable and user unauthorized. If local management authentication is disabled, and the LDAP server used to authenticate management users is unreachable, use password recovery to log into the WLAN Switch and revert to the local database for authentication. For information about password recovery, see "Resetting the Admin or Enable Password" in the *Alcatel-Lucent AOS-W 3.3.1 User Guide*.

Bug ID (if any)	Description
23437	In some cases voice call admission control load balancing may not function correctly. Workaround: Retry call request or association on the voice client.
23327	A blacklisted client will only remain blacklisted for a maximum of 3600 seconds, even when the block time has been set to zero.
23297	Spaces in filenames are not allowed for floorplan images uploaded to RF Plan.
23275	MAC authentication may not immediately take place if a user account is recently added to the internal local database. Workaround: Retry after 5 minutes if the MAC authenticated user was missing from the database during the first try.
23234	The WebUI does not properly permit resetting of custom captive portal pages to factory defaults.
23220	The following SNMP MIBs incorrectly report zero at all times: wlanAPFrameReceiveErrorRate, wlanAPFrameFragmentationRate, wlanStaFrameReceiveErrorRate, wlanStaFrameFragmentationRate.
23175	This release does not support the RF Troubleshooting functionality (RFT) on the OAW-AP124 and OAW-AP125.
22960	Local bridging on enet1 does not work for OAW-AP70 access points that are not remote APs or Mesh nodes.
22925	The OAW-AP124 and OAW-AP125 might fail to boot up across a 100 MB half duplex link.
22849	Creating firewall policies with spaces in the names may cause the user's web browser to hang when displaying firewall policies.
22678	The "%" character may not be used in a password in the local user database.
22672	An SSID configured for xSec and WMM will not function properly. This combination should not be used in this release.
22524	When configuring passwords and keys in the WebUI, non-alphanumeric characters (for example, %, ^, &) are silently discarded, resulting in incorrect passwords being stored. Workaround: Use the CLI to configure passwords and keys that contain non-alphanumeric characters.
22475	This release does not support per-SSID bandwidth contracts on the OAW-AP124 and OAW-AP125.
22346	If the WLAN Switch reboots while a call is in progress, the “show voice call-cdrs” command may show incorrect data for the call after the WLAN Switch is back up. For example, the direction and called party information may be incorrect.

Bug ID (if any)	Description
22283	Extensive amount of syslog messages may be observed after changing the role of the WLAN Switch from master to local. Workaround: Before changing the role of the WLAN Switch from master to local, use the "clean wms-db" command on the WLAN Switch.
22227	L3 mobility across WLAN Switches that are configured with VRRP redundancy may not work as expected. Workaround: Disable VRRP pre-emption in this configuration scenario.
22203	The WLAN Switch cannot authenticate users with special UTF-8 characters in their username.
22199	AAA FastConnect for EAP-TLS may fail if the authentication profile is configured before the CA certificate is loaded. To work around this problem, load all certificates before configuring the authentication profiles.
22190	L2 ACLs (MAC and Ethertype) do not work properly on the OAW-S3 and the WLAN Switches.
21897	Microsoft Vista VPN Dialer behind a NAT device does not fail to establish a VPN session with the WLAN Switch.
21820	Disconnected calls are not reported as such in the output of the “show ap association voip-only” and “show voice sip client-status” commands. The calls are properly disconnected and this is a benign problem with the output.
21673	The WIP module may be logging "Signature Match Detected. SignatureName=Null-ProbeResponse" for some mesh nodes during the time the mesh nodes are starting up. This message is harmless.
21633	It is not possible to provision the antenna type for outdoor APs using Alcatel-Lucent AOS-W. This provisioning must be done from OVMM.
21338	The WIP module may be logging "Disconnect Station Attacks" for mesh nodes incorrectly. If this occurs, disable detection of "Disconnect Station Attacks".
20797	Multicast streaming will not work if DTIM is not equal to 1. Workaround: To support multicast streaming applications, configure DTIM period under the SSID profile to "1".
20603	Users using WZC or MACbook 802.1x supplicant fail authentication with Steel-Belted Radius servers or the internal database if both AAA FastConnect (EAP termination) and trim FQDN are enabled.
20456	L3 roaming of wireless clients with static IP addresses across WLAN Switches is not supported.
20274	GRE tunnel endpoint cannot be the VRRP IP address of a VRRP redundant pair of WLAN Switches.

Bug ID (if any)	Description
20242	When an AAA profile is configured with a reauthentication interval and AAA FastConnect is enabled, reauthentication may fail. Workaround: Disable reauthentication.
20214, 22187	Changing a bandwidth contract while a large number of users are active on the system and subject to that bandwidth contract may result in the message "Module Authentication is busy. Please try later". Workaround: Change the bandwidth contract when there are a low number of active users on the system.
20143	Wired authentication support on ENET1 of an OAW-AP70 remote access point is not supported if "split-tunneling" is enabled.
20134	A "sapd" error message may be seen on WLAN Swatches terminating remote APs that states "An internal system error has occurred at file messenger.c function msgr_papi_send_status_callback line 1590 error". This error message is harmless.
19602	The AP must be rebooted after WMM is disabled for Spectralink Voice Protocol to work with an acceptable retry rate.
17857	When `logging level debug system` is set during system bootup or during a VRRP failover, APs may take a long time to come up. Workaround: Only set `logging level debug system` during an active debugging session. Turning off debugging restores normal operation.
17784	The default behavior of Windows XP may cause AP load balancing not to function correctly by allowing any Windows XP station to associate to an AP after three minutes.
17701	The "show memory fpapps" command does not work on the OAW-S3 and the WLAN Switches.
17688	To deny access to a specific WLAN Switch when traffic travels across another WLAN Switch in the same master-local topology, ACLs must be added to the user's session ACL. Port ACLs are bypassed.
17394	When you first display the Reports page in the WebUI in an Internet Explorer version 7 browser window, a warning message about allowing scripting appears.
16046	A wired client connected to an *Aruba 8E or Aruba 24E* will fail 802.1x authentication. The message "Dropping EAPOL packet" appears in the logfile of the *Aruba 8E or Aruba 24E*. Workaround: Configure the MUX client as master and disable 802.1x.
14119	The WLAN Switch does not perform NAT for traffic originated by the WLAN Switch itself, such as RADIUS requests, syslog, and SNMP. Workaround: Put a loopback or VLAN interface on a public subnet. If that is not possible, configure the WAN VLAN interface IP address to be the same as the WLAN Switch IP address.

Bug ID (if any)	Description
12732	Load balancing does not work properly when local probe responses are enabled.
8684	When a mobile client is on a foreign network in a mobility domain, multicast traffic is not tunneled back to the home network.
	The Ethernet port on the OAW-AP124 and OAW-AP125 may not function as expected in 10 Mbs mode.
	This release does not support the secure enterprise mesh functionality on the OAW-AP124 and OAW-AP125.
	This release does not support the remote AP functionality on the OAW-AP124 and OAW-AP125.
	This release does not support FCC DFS on the OAW-AP124 and OAW-AP125.
	ETSI DFS is supported but not yet fully certified on the OAW-AP124 and OAW-AP125 at this time.
	If local management authentication is enabled and you are unable to log into the WLAN Switch, use password recovery to log into the WLAN Switch to disable local management authentication. For information about password recovery, see "Resetting the Admin or Enable Password" in the *AOS-W 3.3.1 User Guide*.
	The OAW-AP80M uses only approved outdoor channels; however, the administrator can configure any channel using the CLI and the WebUI. If this occurs, the OAW-AP80M randomly selects a valid outdoor channel.
	In multi-switch networks, save your mesh cluster configuration before provisioning the mesh nodes. To save your configuration in the WebUI, at the top of any page click **Save Configuration**. To save your configuration in the CLI: `write memory`

Documents in This Release

The following new documents are available with this release:

- Alcatel-Lucent OAW-120 Series Indoor Access Point Installation Guide
- *OAW-AP120 Series AP Mounting Kit Installation Guide*

New revisions of the following documents are also part of the documentation set for this release:

- *AOS-W 3.3.1 User Guide*

- *AOS-W 3.3.1 Command Line Interface Reference Guide*
- *AOS-W 3.3.1 Quick Start Guide*
- *AOS-W 3.3.1 MIB Reference*
- *AOS-W 3.3.1 Software Upgrade Guide*

The documentation library is updated continuously. You can download the latest version of any of these documents from:

https://service.esd.alcatel-lucent.com

For More Information

To contact Alcatel-Lucent, refer to the information below:

Web Site Support	
Main Site	http://www.alcatel-lucent.com/enterprise
Support Site	https://service.esd.alcatel-lucent.com
Support Email	support@ind.alcatel.com

Telephone Support	
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