AOS-W 3.4.1.1
Release Notes

This document describes new features and issues pertinent to the AOS-W 3.4.1.1 release.

What's New in This Release

AOS-W 3.4.1.1 is a product feature release that introduces new software features and hardware platforms. It addresses and provides solutions to a number of known issues. This section describes new features and their capabilities

For details on all of the features described in the following sections, see the *AOS-W 3.4.1 User Guide*, *AOS-W 3.4.1 CLI Reference Guide*, and *AOS-W 3.4.1 MIB Reference Guide*.

See the *AOS-W 3.4.1 Software Upgrade Guide* for instructions on how to upgrade your switch to this release.

In Previous AOS-W 3.4.1 Releases

Previous releases of AOS-W 3.4.1 have introduced new software features for all Alcatel-Lucent Switches. This section describes features and capabilities of AOS-W 3.4.1.1.

Licensing

Licenses Deprecated in AOS-W 3.4.1

- Voice Services Module (VSM)—deprecated beginning with AOS-W 3.4.1. All Voice functionality is now provided within the PEF license.
- The Voice Aware Scan feature is moved to the base OS and therefore does not require a separate license.

Hardware

OAW-AP105

AOS-W 3.4.1 introduces support of the Alcatel-Lucent OAW-AP105. The Alcatel-Lucent OAW-AP105 wireless access point supports the IEEE 802.11n standard for high-performance WLAN. This access point uses MIMO (Multiple-in, Multiple-out) technology and other high-throughput mode techniques to deliver high-performance, 802.11n 2.4 GHz and 5 GHz functionality while simultaneously supporting existing 802.11a/b/g wireless services. The OAW-AP105 access point works only in conjunction with an Alcatel-Lucent Switch.

SNMP Enhancements

There are several new enhancements including a configurable switch SNMP engine ID, new traps and a new MIB object.

Configurable SNMP Engine ID

The SNMP switch engine ID can be changed using the following new CLI command:

```
(host) (config) #snmp-server engine-id ?
<engineid>              Engine ID of SNMP server in HEX (max 24 chars) eg.
                        8000052301A9FEA484.
(host) (config) #snmp-server engine-id 000039e7000000a10a031daa
```

To view the SNMP engine-id setting output, use the following new CLI command:

```
(host) #snmp-server engine-id <engineid>
SNMP engine ID: 000039e7000000a10a031daa
```

If you do not change the engine-id setting then the factory default value displays:

```
(host) #show snmp engine-id
SNMP engine ID: 000039e7000000a10a043e03 (Factory Default)
```

To revert to the factory default engine-id setting, use the following new CLI command

```
(host) #no snmp-server engine-id
```

New SNMP Traps

This release has two new traps:

- wlsxNConnectionResetWithLocal–This trap indicates that the master switch has lost contact with the local switch.
- wlsxNApOnBackupController–This trap is generated when an AP connects to its backup LMS. The trap contains the AP wired MAC address, IP address of the backup switch and the IP address of the primary switch. The trap is generated by the backup switch.

New MIBs

wlsxWlanRadioTable

The objects of the wlsx WLAN Radio table provide information on the access points connected in radios that are known to the Alcatel-Lucent switch. This table is indexed by the MAC address of the AP and the type of the radio.

A new OID has been added to this table:

wlanAPRadioAPName–Indicates the name of the AP to which the radio belongs.

Platform

Mux Enhancements

The Mux port can now be configured as a trunk port. This allows customers to have multiple clients on different VLANs that come through the trunk port instead of having clients on a single VLAN.

Range of VLANS

Multiple VLANS can now be created and added to the switch configuration at once in a range format.

Trusted/Untrusted VLANs

VLANs can be now set in a range as trusted or untrusted. Use the interface command or the WebUI to set a range of VLANs to be trusted. VLANs not included in the trusted range of VLANs will be, by default, untrusted.

Link Aggregation Control Protocol (LACP)

Alcatel-Lucent implementation of Link Aggregation Control Protocol (LACP) is based on the standards specified in 802.3ad. LACP provides a standardized means for exchanging information, with partner systems, to form a link aggregation group (LAG). LACP avoids port channel misconfiguration.

Two devices (actor and partner) exchange LACP data units (DUs) in the process of forming a LAG. Once multiple ports in the system have the same actor system ID, actor key, partner system ID, and partner key, they belong to the same LAG.

The maximum number of supported port-channels is 8. With the introduction of LACP, this number remains the same. In essence, a port-channel group (LAG) is created either statically or dynamically via LACP.

Wireless

Beacon Rate

Both a-beacon-rate and g-beacon-rate parameters can now be configured using the wlan-ssid-profile command. Configuring the 802.11a and 802.11g beacon rates should only be used in conjunction with Distributed Antenna Systems (DAS). Configuring beacon rates during normal operation may cause connectivity problems.

Dynamic Multicast Optimization

You can now configure AOS-W to reliably and efficiently stream multicast traffic over wireless LAN (WLAN). This new method allows you to stream video traffic reliably without much loss. To ensure that video data is transmitted reliably multicast video data is transmitted as unicast.

See the *Video and Voice QoS* chapter in the AOS-W 3.4.1.1 User Guide for more information.

In AOS-W 3.4.1.1, this feature is supported only on the Alcatel-Lucent 4306 Series, 4X04 Series, and OAW-S3 switch platforms.

Mesh Enhancements

Starting with AOS-W 3.4.1, if a mesh point using the startup-subthreshold or subthreshold-only mode reselects a more distant parent because its original, closer parent falls below the acceptable threshold, then as long as that mesh point is connected to that more distant parent, it will seek to reselect a parent at the earlier, shorter distance (or less) with good link quality. For example, if a mesh point disconnects from a mesh parent 2 hops away and subsequently reconnects to a mesh parent 3 hops away, then the mesh point will continue to seek a connection to a mesh parent with both an acceptable link quality and a distance of two hops or less, even if the more distant parent also has an acceptable link quality.

Authentication

Stateful NTLM authentication

NT LAN Manager (NTLM) is a suite of Microsoft authentication and session security protocols. When you enable the stateful NTLM authentication feature, the switch will monitor the NTLM authentication messages between a client and a Windows authentication server. If the client successfully authenticates

via an NTLM authentication server, the switch can recognize that the client has been authenticated and assigns that client a specified user role.

Authentication for Wireless Internet Service Provider roaming (WISPr)

WISPr authentication allows a "smart client" to authenticate on the network when they roam between Wireless Internet Service Providers, even if the wireless hotspot uses an ISP for which the client may not have an account.

If you are a hotspot operator using WISPr authentication, and a client that has an account with your ISP attempts to access the Internet at your hotspot, then your ISP's WISPr AAA server authenticates that client directly, and allows the client access on the network. If, however, the client only has an account with a partner ISP, then your ISP's WISPr AAA server will forward that client's credentials to the partner ISP's WISPr AAA server for authentication. Once the client has been authenticated on the partner ISP, it will be authenticated on your hotspot's own ISP, as per their service agreements. Once your ISP sends an authentication message to the switch, the switch assigns the default WISPr user role to that client.

Adaptive Radio Management (ARM) Enhancements

Starting with AOS-W 3.4.1, the ARM band steering feature supports both campus APs and remote APs that have a virtual AP profile set to tunnel, split-tunnel or bridge forwarding mode.

Increased User Scalability for 4306 Series and 4X04 Series Switches

The limit of maximum supported platform users has been increased on the Alcatel-Lucent 4306 Series and the Alcatel-Lucent 4X04 Series switches.

Table 1 *Maximum Supported Users*

Switch	Number of Users
4306	256
4306G	512
4504	2048
4604	4096
4704	8192

Issues and Limitations Fixed in AOS-W 3.4.1.1

This release contains all fixes up to and including those in AOS-W 3.4.1.0. The following issues and limitations have been fixed in the AOS-W 3.4.1.1 release:

Table 2 *Fixed Issues in AOS-W 3.4.1.1*

Bug ID	Description
21869, 34966	SNMP wlsxSysExtCardTable reports the correct number of FE and GE ports.
22057, 26616	Prior to contacting the switch, an AP will now only report syslog messages that are errors or great to prevent prevent the syslog from becoming flooded with informational and warning messages.

Table 2 *Fixed Issues in AOS-W 3.4.1.1*

Bug ID	Description
23154, 27433	The local switch's hostname is no longer incorrectly changed to the host IP address, defined in the netdestination command on the master, after the switch is rebooted.
31976	When a halt command is issued on an S3 or 4X04 Series switch, the Power LED is solid green, the Status LED is solid red, and any active LEDs are off.
32097, 35616	An authorization memory leak was causing unexpected behavior when executing the `show memory auth` command. The memory leak has been fixed.
33362, 35170, 35576, 36562	A flash backup can be completed successfully, when enough free space is available, using the `backup flash` command.
33771, 33791, 36470	An auth module crash that occured when a `show user` command was executed has been fixed.
34581, 35515, 36771, 35232	When the TX rate (such as g-tx-rate org-basic-rate) is changed in the SSID profile, the change no longer requires the radio to be reset to take effect.
34679	When a switch is being used as a DHCP server (to provide option 252), an extraneous space is no longer added by the switch to the option 252 URL.
34975, 37034, 36814	An auth crash occuring in handle_tunnel_id_update has been fixed.
35514, 36257, 37363, 37382, 37383	When using Mozilla Firefox, the WebUI will no longer continuously display the "successfully uploaded" message after uploading an RF Plan file.
36183	Encrypted H323 traffic was not handled correctly (denies in the datapath) and has now been corrected.
36248	On the **Monitoring > Network > All WLAN Switches** page, the links to all listed local switches now work.
36380	Unexpected switch behavior caused by a control processor exception has been fixed.
36452	A mismatch between the running-config and the startup-config on the local switch has been fixed.
36459, 36947, 36997, 37032, 37827, 28508	Datapath timeout issue have been fixed.
36479	RTLS Server configuration changes take effect immediately and do not require APs to reboot.
36508	OAW-AP125s can send CTS-to-self when 11g protection is active and any g-tx-rates are selected.
36560	SAPM no longer tries to generate a config message for an AP that has been marked for full reconfiguration.

Table 2 *Fixed Issues in AOS-W 3.4.1.1*

Bug ID	Description
36675	When the link is lost on a GigE port an Alcatel-Lucent 4324, the 4324 does not have to be power-cycled to reestablish the link
36752	IPv6 multicast frame (converted to unicast) are no longer leaked to the client when using VLAN pooling and battery boost is enabled.
36817	The asterisk(*) is no longer accepted in usernames and passwords used for LDAP authentication.
36819	When seven or more clients are connected to a single OAW-AP125, clients are no longer disassociating and associating when additional clients are added.
36836	The WebUI and the CLI now both generate 8 character passwords.
36864, 36958	The traps wlsxAccessPointIsUp and wlsxAccessPointIsDown now disply the coreect information in the correct fields.
36871	The default account start to end time for guest provisioning is now set to 8 hours.
37091, 37736, 37951, 38124	Unexpected switch behavior caused by a datapath timeout has been fixed.
37131	A kernal panic issue on S3 or 4X04 Series switches has been fixed.
37139	User counts displayed by `show user-table` and `show aaa state configuration` now correctly display the same number of users.
37183	When VLAN Pooling is enabled, IPv6 router advertisements (RA) are sent via unicast to ensure that clients see the RA of a spcific VLAN only.
37302	Alcatel-Lucent switches now correctly send traps pertaining to auth failures.
37703, 37499	Clients are can now succesfully authenticate against configured 802.1x profiles and the associated auth module crash has been fixed.
38042, 37742	Bandwidth contracts are now deleted when the associated user is deleted.

Table 3 *Fixed Issues in AOS-W 3.4.1*

Bug ID	Description
29749	A replay counter mismatch issue causing client connectivity problems has been fixed.
30707, 33778, 33777, 36010	Unexpected switch behavior caused by a datapath exception due to a double free issue has been fixed.
31309	SNMP MIBs wlanAPRxDataPkts and wlanAPRxDataBytes now correctly display the appropriate value.
31862, 31863	All Voice Service Module (VSM) related features are included in the PEF license.

Table 3 *Fixed Issues in AOS-W 3.4.1*

Bug ID	Description
32803, 35350, 35134	An auth hang issue due to frequent RAND number generation has been fixed.
33890	A new parameter type netmask was added to support subnet mask 240.0.0.0. This parameter type validates that the netmask added is a valid IP address.
35591, 36949, 38050	An auth module crash due to a MAC authentication issue has been fixed.
35665, 33635	The speed of the FE ports on the Alcatel-Lucent 800 can be successfully hardcoded when connected to a Cisco 2950.
35703	Cisco SCCP used with AOS-W 3.4 no longer results in dropped or denied RTCP packets.
35758	The inconsistencies between `show wms monitor-summary` and the WMS database have been fixed, ensuring that the correct number and classification of APs are displayed.
35774	The switch no longer hangs during SCP file transfer after 504 copies. However, any copies after 503 will fail because the system runs out of memory.
35842	SNMP error messages are no longer incorrectly generated after disabling SNMP traps and hosts.
35983	The maximum character number for the `guest email-id` has been increased from 31 to 64.
36084	Pre-configured static entries (such as IPaddr, Netmask, Gatewayip, DNS-serverip, External antenna gain values) are retained and properly read in AP Installation Wizard for Provisioning the AP.
36126	Nortel GBIC works correctly on switches running AOS-W 3.4.
36383	Multicast over VLAN pooling now works correctly on all VLANs.
36469	The maximum logon wait in Captive Portal time has been changed from 10 seconds to 30 seconds.
36527, 36528	A new counter has been added to `show ap debug bss-stats bssid <MAC Address>` which tracks the number of data frames received from an STA that is not associated.
36561	Unexpected switch behavior caused by a datapath exception has been fixed.
36599, 36262	An issue in which AP-125s reboot/bootstrap at random has been fixed.
36642	AP-12x does no longer turns back on immediately after converting to APM mode.

Known Issues and Limitations in AOS-W 3.4.1.1

The following are known issues and limitations for this release of AOS-W. Applicable bug IDs or workarounds are included:

Table 4 *Known Issues and Limitations*

Bug ID	Description
36507	When OAW-AP15 is deployed as a Remote AP in bridge or split-tunnel mode, it is possible to observe an occasional AP kernel crash when the AP is submitted to a very large amount of UDP traffic. This is mostly a concern for throughput testing and is extremely unlikely to happen in any real usage scenario.
35349	The “Access Point Status” LED on a switch does not work unless rogue APs are detected.
35305	When disable scanning option is set for SIP ACLs, SIP packets are not reaching the ALG and hence ports are not being opened for RTP
35174	After an extended online session with the carrier, a cellular modem's communication port may become unresponsive and cause redial attempts to be unsuccessful. Unplug the USB data card and re-insert to remedy the problem.
35173	The VLAN map configuration is not propagated to a new local switch when it is configured on an existing master switch. Execute write memory on the master switch to remedy this issue.
34830	High re-associations are seen for Spectralink handsets connected to Mesh points.
34829	An error message is displayed when an OAW-AP60 is provisioned as mesh node.
34759	Do not manage or configure RFportect sensors using AOS-W 3.4. Doing so will cause unexpected switch behavior.
34615	The 4306 series switches freeze if the EVDO modem is plugged out while passing traffic through it
34408	The 4306 series switches may not behave normally if the RF-band is changed when the internal AP is in AM mode.
34103	PTT does not work on Spectralink phones when battery boost is enabled.
33898	Occasionally a Windows client prompts for a password to access the NAS disk although there is no password set for disk access. When this occurs, the user can access the NAS disk after closing the password prompt or by entering a random password.
32066	When the country code of a running AP is changed because its regulatory domain profile changed, the AP needs to be rebooted.
28983, 31509	Legacy APs operating on channels 52, 56, 60, and 64 often detect spurious radar while other APs, placed in same vicinity, do not.
20194	If Static WEP is used with split or bridge mode VAP’s, key slots 2-4 on the switch should be used. Key slot 1 should be used with VAP’s in tunnel mode only.

Documents in This Release

New revisions of the following documents are available with this release:

- *AOS-W 3.4 User Guide*
- *AOS-W 3.4 Command Line Interface Reference Guide*
- *AOS-W 3.4 Quick Start Guide*

- *AOS-W 3.4 MIB Reference Guide*
- *AOS-W 3.4 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	esd.support@alcatel-lucent.com
Telephone Numbers	
North America	1-800-995-2696
Latin America	1-877-919-9526
Europe	+33 (0) 38 855 6929
Asia Pacific	+65 6240 8484

www.alcatel-lucent.com

26801 West Agoura Road
Calabasas, CA 91301