AOS-W 3.3.3.2
Release Notes

This document describes new features and issues pertinent to the AOS-W 3.3.3.2 release.

See the AOS-W *3.3 Software Upgrade Guide* for instructions on how to upgrade your switch to this release.

What's New in This Release

AOS-W 3.3.3.2 is a patch release that addresses and provides solutions to a number known issues. The list of outstanding known issues for AOS-W 3.3.3 begin on page 3.

Alcatel-Lucent OAW-AP105

AOS-W 3.3.3.1 introduces support of the Alcatel-Lucent OAW-AP105 access point. 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 Queries Over IPsec Tunnel

This command was added in AOS-W 3.3.3.1 as a fix to bug #35902.

A command has been added to the CLI to force the use of the switch's IP address when sending SNMP responses. This will ensure that packets are sent to the tunnel interface.

```
(config) #snmp-server source switch-ip
```

SIP Midcall Request Timeout

This feature was added in AOS-W 3.3.3.1 as a fix to bug #35288

This feature allows the switch to determine whether or not a call is still active in scenarios where a voice session does not exist, such as when a call is placed on hold. When enabled, if a client does not send responses for a mid-dialog requests, ALG will clear the status of the call and generate an ABORTED call record.

```
(config) #voip sip-midcall-req-timeout  <enable/disable>
```

Issues and Limitations Fixed in AOS-W 3.3.3.2

This release contains all fixes up to and including those in AOS-W 3.3.3.0. The following issues and limitations have been fixed in the AOS-W 3.3.3.2 release:

Table 1 *AOS-W 3.3.3.2*

Bug ID	Description
N/A	This release contains fixes for issues found internally.

Table 2 *AOS-W 3.3.3.1*

Bug ID	Description
30707, 33778, 33777, 36010	Unexpected switch behavior caused by a datapath exception due to a double free issue has been fixed.
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.
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.
36165	The Airwave Management Platform (AMP) is able to successfully poll or perform an snmpget from a switch.
36220	The VAP registration queue is no longer getting stuck, resulting in active APs no longer being incorrectly displayed as inactive in the CLI.
36642	OAW-AP12x no longer turns back on immediately after converting to APM mode.

Table 3 *AOS-W 3.3.3.0*

Bug ID	Description
30962	Reason code messages have been added for Alcatel-Lucent reason codes. Therefore, when a reason code is displayed in a log messages, the corresponding message is displayed if one is available.
32120, 34782	User-entries can be added, through the WebUI, with email addresses containing white-space.
32827	Infrom traps are successfully delivered to Airwave when the SNMP protocol version is SNMPv2c.
33759	ACL blacklisting and ip-access-list session blacklist no longer require the WIPS license.
34240	Errors are no longer logged after successful execution of `mobility-manager` command.
34417	Dst-nat works with Cisco VPN clients using version 5.0 or greater.

Table 3 *AOS-W 3.3.3.0*

Bug ID	Description
35885	Sequence anomaly check and disconnect station check have been added. Both are diabled by default and must be manually enabled by the user.

Known Issues and Limitations in AOS-W 3.3.3.2

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 (if any)	Description
36117	RFprotect Sensors: Shielding fails when SSID is using WEP encryption.
36105	RFprotect sensors are unable to run wireless rouge checks.
33343	The TX queue prioritization on an AP is per-session for Static-WEP, but is per-station for TKIP/AES encryption.
23929	Direct SNMP GET requests have been discontinued, despite the fact that an SNMP profile can still be configured under the AP system profile.
27834	Apple Macintosh laptops running OS X are unable to roam when OKC is enabled. To work around this, disable OKC (it is enabled by default).
27873	With some clients, client authentication can sometimes take from 30 seconds to 2 minutes.
27565	RF Plan imports do not always work with Firefox.
25351	PEF rules do not always pause ARM scanning.
26643	Some AP models do not display the master swicth IP and the DHCP assigned IP in the AP boot message log.
24956	Wired 802.1x on Alcatel-Lucent 4308 trunk port is not supported.
27069	When “enfore machine authentication” is enabled for 802.1x clients, the master switch(es) track the authentication state of every device on the master. However, if the master goes down, there is no place to check if a client passed machine authentication and thus impacts user connectivity. A workaround is enable the local switch’s internal database to store machine authentication states.
27613	The UI displays only one firewall ACL with a “time range” parameter.
25265	Valid user ACLs are not supported for IPv6 addresses.
25787	If the `best-effort-acm` parameter is set to 1, Cisco 7921g phones cannot associate. To work around this, set the `best-effort-acm` parameter to 0 (which is the default value).
27669	If a roaming client has difficulty maintaining connectivity, set the dot1x key retry count to 5 using the `aaa authentication dot1x wpa-key-retries 5` command.
27371	An error is generated in RF Plan when you create a new building in the main campus the first time after a WMS reinitdb. The new building is created and you can ignore the error. To work around this reload the browser.
27309	After applying the upgrade license to allow AP-120 series a/b/g APs to support 802.11n, the affected APs must be rebooted for the change to take effect.
27498	Clients using a Linksys WPC600N 802.11n NIC are unable to pass traffic on 40 MHz channels over a back-up virtual AP. Clients are able to associate and get an IP address via DHCP, but cannot pass traffic. To work around this, use the 20 MHz channels for the back-up VAP.

Table 4 *Known Issues and Limitations*

Bug ID (if any)	Description
27340	If a client connects via VPN using a different SSID (for example, if the client loses their wireless connection), the client is categorized as a new user. Thus, until the earlier entry ages out, the client is seen as two discrete users, each counting toward the total for your VPN license. To force an L2TP user entry to age out, use this command for the inner IP address: aaa user logout Use this command for the outer IP address: aaa user delete You cannot force a PPTP user entry to age out.
26898	RF Plan currently supports planning for the AP-124 only in the 20 MHz channel.
26699	You cannot use the native Windows XP L2TP IPSec dialer if you install the Alcatel-Lucent dialer. To work around this, uninstall the Alcatel-Lucent dialer and reboot Windows.
25109	ACL new hits and total hits may show incorrect values for “redirect src-nat” enabled session ACLs.
25031	When users select a different server group for the authentication server group, the 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.
24761	Enabling port mirroring on a 1 Gbps port to a 100 Mbps port is not supported on M3 and 3000 series Alcatel-Lucent switches. Port mirrors should be disabled whenever not in use in order to prevent performance impact on these type of mobility switches.
24748	Not able to add channels to the regulatory domain using the mobility switch webUI. Workaround: Use the mobility switch CLI to add channels to the “ap regulatory-domain” configuration.
24601	The mobility switch WebUI may show the number and state of APs and AMs incorrectly. Workaround: Use the **`show ap active`** command in the local mobility switch CLI to monitor AP states that are terminated on the switch.
24108	The WebUI and the CLI prevents configuration of an AP-70 to use internal antennas for one radio and external antennas for the other radio.
24063	For APs that discover the master switch using DNS, switch discovery fails if the DHCP server returns more than one domain name.
23929	APs do not respond to SNMP queries even though SNMP has been enabled.
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.
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 AP-70 eth1 port.
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 2.4 GHz and 5 GHz bands. Workaround: Use dedicated air monitors or deploy dual-radio access points.

Table 4 *Known Issues and Limitations*

Bug ID (if any)	Description
23713	Checkbox selections may get lost after WebUI auto refresh.
23669	SNMP total AP count will not include APs that do not have VAPs enabled. Workaround: Use the `show ap active` command on the switch to monitor the total AP count.
23437	In some cases voice call admission control load balancing may not function correctly. Workaround: Retry call request or association on the voice client.
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.
22925	The AP-124 and AP-125 might fail to boot up across a 100 MB half duplex link.
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.
22346	If the switch reboots while a call is in progress, the “show voice call-cdrs” command may show incorrect data for the call after the switch is back up. For example, the direction and called party information may be incorrect.
22283	Extensive amount of syslog messages may be observed after changing the role of the mobility switch from master to local. Workaround: Before changing the role of the mobility switch from master to local, use the `clean wms-db` command on the mobility switch.
22203	The switch cannot authenticate users with special UTF-8 characters in their username.
22190	L2 ACLs (MAC and Ethertype) only work if the user table has any entry for the station. L2 ACLs do not work in an untrusted station has not sent an IP frame, but an L2 frame.
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 AOS-W. This provisioning must be done from MMS.

Table 4 *Known Issues and Limitations*

Bug ID (if any)	Description
21338	The WIP module may be logging “Disconnect Station Attacks” for mesh nodes incorrectly. If this occurs, disable detection of “Disconnect Station Attacks”.
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.
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, 23778	Wired authentication support on ENET1 of an AP-70 remote access point is not supported if “split-tunneling” is enabled.
20134	An “sapd” error message may be seen on switches 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.
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 S3 and the Alcatel-Lucent 4X04 series.
17688	To deny access to a specific switch when traffic travels across another 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, 16565	A wired client connected to an Alcatel-Lucent 4308 or Alcatel-Lucent 4324 fails 802.1x authentication. The message “Dropping EAPOL packet” appears in the logfile of the Alcatel-Lucent 4308/4324. Workaround: Configure the MUX client as master and disable 802.1x.
14119	The switch does not perform NAT for traffic originated by the 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 switch IP address.
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 AP-124 and AP-125 may not function as expected in 10 Mbps mode.

Table 4 *Known Issues and Limitations*

Bug ID (if any)	Description
	This release does not support the secure enterprise mesh functionality on the AP-124 and AP-125.
	If local management authentication is enabled and you are unable to log into the switch, use password recovery to log into the 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 AP-80M uses only approved outdoor channels; however, the administrator can configure any channel using the CLI and the WebUI. If this occurs, the AP-80M 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

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

- *AOS-W 3.3.2 User Guide*
- *AOS-W 3.3.2 Command Line Interface Reference Guide*
- *AOS-W 3.3.2 Quick Start Guide*
- *AOS-W 3.3.2 MIB Reference Guide*
- *AOS-W 3.3.2 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 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