AOS-W 3.4.5.1

Release Notes

This document describes new features and issues pertinent to the AOS-W 3.4.5.1 release.

What's New in This Release

AOS-W 3.4.5.1 is a patch release that introduces new enhancements. It addresses and provides solutions to a number of known issues. This section describes new enhancements and their capabilities.

See the *AOS-W 3.4.2 Software Upgrade Guide* for instructions on how to upgrade your switch to this release.

Even VLAN Pool Assignments

This feature allows for even distribution of VLAN pool assignments. Even VLAN Pool assignment maintains a dynamic latest usage level of the each VLAN ID in the pool. Therefore, as users age out, the number of available addresses increases. The previous implementation of VLAN Pool assigning uses a hash based mechanism, based on the station MAC address, to map stations to VLAN IDs. However, this can lead to multiple stations being mapped to a small number of VLAN IDs instead of utilizing all those that are available. This causes the IP addresses associated with those few VLANs to be assigned, preventing new stations from coming up.

Even VLAN Pool Assignment is not allowed for VLAN pools configured directly under a virtual-ap. It should only be used under named VLANs.

L2 Mobility does not work with the existing implementation of Even VLAN pool assignment.

The following CLI command allows you to set the VLAN assignment. The `hash` value is set by default and is used for all VLAN unless configured as `even`.

```
(config) #vlan-name <vlan-name> pool assignment {even | hash}
```

You can view the current VLAN assignment configuration by executing the `show vlan mapping` command.

Issues and Limitations Fixed in AOS-W 3.4.5.1

This release contains all fixes up to and including those in AOS-W 3.4.5.0. The following issues and limitations have been fixed in the AOS-W 3.4.5.1 release:

Table 1 *Fixed in AOS-W 3.4.5.1*

Bug ID	Description
49910, 53933, 56010, 56193, 57843, 54695	An unexpected AP reboot caused by a memory leak that occurred when an AP in air monitor mode was upgraded has been fixed.
50578	An AP STM memory leak initiated by a switch deauth has been fixed.
52492, 53600, 56561, 54231, 57302, 55620, 61152, 61155, 56928	An unexpected switch reboot due to a hard watchdog accompanied by “reason for reboot: unknown” has been fixed. Additionally, a change has been made to AOS-W to prevent the use of “reason for reboot: unknown” for unexpected reboots. Unknown reboots we caused by flash write failures. Now, the flash write is retried by performing an erase followed by another write.
52758	Issue that occur when the switch's SNMPD module does not respond to the AMP's SNMP requests has been fixed.
53497, 56022, 58185, 57411, 59249, 61210	An unexpected switch reboot caused by an fpapps module crash due to a PAPI corruption has been fixed.
53897, 52825, 55118, 53365, 59274, 61930	An OAW-AP125 crash caused by a node leak has been fixed.
54191, 55794	FTP data transfer and reuse of a stray session no longer triggers a race condition and datapath timeout exception.
54343	An STM module crash due to an STM memory leak caused by voice client call session being created but not deleted after the session ends has been fixed.
54847	AOS-W no longer does DFS detection on channels 36-48 and 149-165 for Mexico and Vietnam.
56747	A buffer leak caused by wi-fi encrypted jumbo frames which lead to a disruption in client connectivity and AP heartbeats has been fixed. Additionally, a new counter, called **WIFI Jumbo Denied**, has been added under `show datapath frame`.
57249	Support has been for APs to operate in 40 MHz for the ZA country code, making new data rates available.
57613	An issue in which SCCP signaling packets were being dropped by the AP datapath, prevent Cisco phones from registering on the network, has been fixed.

Table 1 *Fixed in AOS-W 3.4.5.1 (Continued)*

Bug ID	Description
57831, 59911, 61737	An unexpected switch reboot caused by a datapath exception has been fixed.
60102	When a previously authenticated and now timed-out user reauthenticates, the cached current VLAN is changed to the assigned VLAN during the initialization of MAC authentication. This prevents the cached L2 entry from being reused.
60667	Authentication process no longer times out if there is a roundtrip delay for 400 ms or less between the switch and a TACACS accounting server.

Table 2 *Fixed in AOS-W 3.4.5.0*

Bug ID	Description
40032	An AP-105 with its country code set to JP3 will experience improved connectivity on DFS channels, as the AP no longer frequently detects spurious radar on channels 52, 56, 60, and 64.
40822	The Internet Explorer 6 browser no longer fails to respond when you try to delete a user through a guest-provisioning account.
44309	APs are no longer susceptible to DoS attacks that are initiated by injecting malformed 802.11 authorization or association requests with an invalid station MAC address.
44942	Instead of displaying single bit ECC error in the error log, these errors are counted and displayed as a counter in `show memory debug`.
49267	Improvements to the internal httpd process on the switch allow Captive Portal users to log in without errors during periods of peak Captive Portal utilization.
51965, 52714	Wireless clients now correctly receive IPv6 addresses.
53189	Improvements to the syslog process allow you to change user roles through the Extended Services Interface (ESI).
53192	AP-120 series APs support the Kenya regulatory domain.
53953	Aggregated Medium Access Control Service Data Units (AMSDU) packets are no longer dropped by default. This change resolves an issue that prevented some Apple MAC OS X devices from passing TCP traffic.
54199	APs running AOS-W 3.4.5.0 and later support the **JP** and **JP2** Japan country codes.
54981, 54220	Named VLAN pool configuration information is no longer lost when upgrading to AOS-W 6.1.x.
55536	Support for the new Aruba Organizational Unique Identifier (OUI) 6c:f3:7f in Aruba product MAC addresses.

Known Issues and Limitations in AOS-W 3.4.5.1

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

Table 3 *Known Issues and Limitations*

Bug ID	Description
44208, 40777	An AP may refuse call admission even if the configured Call Admission Capacity (CAC) limit has not been reached. For example, if the call count CAC limit is set to **n**, only **n-1** calls may be allowed on that AP. **Workaround:** Upgrade to AOS-W 6.0. There are two procedures to work around this issue in AOS-W 3.4.5.1: • For call count based CAC: Set the call capacity to (*n* + *1*) to ensure that *n* calls are allowed. • For bandwidth based CAC: Set the bandwidth capacity to the capacity required by (*n+1)* calls to ensure that *n* calls are allowed.
40858	Client devices are not evenly distributed across the bands when a group of clients attempts to associate simultaneously. The clients will associate on the band that is better in terms of load. However, if a client has an affinity for a particular band, they will be allowed to associate on that band. **Workaround:** None.
38398	Only one Virtual AP per AP group can support the band steering feature. Enabling band steering on multiple Virtual APs may not give expected results for clients connecting to all Virtual APs. **Workaround:** Upgrade to AOS-W 5.0.3.3 or later. To avoid this issue in AOS-W 3.4.5.1, do not enable band steering on multiple Virtual APs in a single AP group.
39768	Kerberos authentication settings can only be configured through the command-line interface, not the WebUI. **Workaround:** You must use the CLI to configure Kerberos.
39620	Users can delete the **default** user role even if it is referenced being by a stateful Kerberos authentication profile. This can lead to misconfiguration. **Workaround:** Upgrade to AOS-W 6.0 or later. To avoid this issue in AOS-W 3.4.5.1, ensure that the role being deleted is not being referenced by an authentication profile before deleting it.
	Stateful Kerberos authentication currently does not work with NAT or PAT. **Workaround:** Do not use Stateful Kerberos with NAT or PAT.
39072	If you enable token-caching and use a RADIUS server for authentication, the output of the CLI command `show user-table verbose` may incorrectly label the server as “Internal” instead of “RADIUS.” This is a display issue only and will not alter your server configuration. **Workaround:** None.
36507	If an OAW-AP105 deployed as a Remote AP in bridge or split-tunnel mode and subjected to a very large amount of UDP traffic, the AP kernel may stop responding. Although this issue may be a concern for laboratory throughput testing, it is extremely unlikely to happen in any real network usage scenario. **Workaround:** None.

Table 3 *Known Issues and Limitations (Continued)*

Bug ID	Description
35305	For a VoIP Application-level gateway (ALG) to work properly, do not use the **disable scanning** option in the VoIP ACLs. If scanning is disabled, RTP ports are not dynamically opened in the firewall for VoIP clients. **Workaround:** Upgrade to AOS-W 6.0 or later. To avoid this issue in AOS-W 3.4.5.1, do not select **disable scanning** in VOIP ACLs. Additionally, if you choose to disable ARM scanning during an active call, enable **voip aware-scan** under the ARM profile.
34830	PolyCom SpectraLink telephones connected to mesh points may reassociate to their mesh point when a call is initiated from that phone. This behavior is caused by the SpectraLink handsets, not AOS-W. **Workaround**: None.
34829	When an AP-60 with an external antenna is provisioned as a mesh node using the AP Wizard in the WebUI, an *configuration failed* error message may appear in the AP's status column even if the AP has been successfully provisioned. **Workaround:** None.
34408	If the internal AP in an OmniAccess 4306GW switch is in Air Monitor mode, changing the RF band of the internal AP may cause the AP to stop responding. **Workaround:** There is no need to change the RF band when the internal AP is in AM mode since the software scans both bands.
33898	Some Windows and Mac clients may prompt for a password to access a disk attached to a 4306 Series switch, even though the switch does not support a password for NAS access. **Workaround:** Ignore the prompt. You can access the NAS disk after closing the password prompt or by entering a random password.
32066	When you change the country code of a running AP in its regulatory domain profile, you must reboot the AP. **Workaround:** Reboot the AP after changing its country code in regulatory domain profile. Other parameters in the regulatory domain profile can be changed without the need for a reboot.
28983, 31509	AP-70 and AP-60 series operating on channels 52, 56, 60, and 64 with the JP3 country code often detect spurious radar while other AP models placed in same vicinity, do not. **Workaround:** To avoid this issue when using the country code JP3, use non-DFS channels or replace AP-70 and AP-60 series with newer AP models, such as the OAW-AP125, OAW-AP105, AP-90 Series.
20194	In a Static WEP configuration, key slot 1 can only be used in tunnel mode. **Workaround:** Avoid using Static WEP. If Static WEP is used with split or bridge mode Virtual APs (VAP), use key slots 2-4 on the switch.

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