Release Notes - Maintenance

OmniAccess Stellar

AWOS Release 4.0.3.3067 Maintenance Release

These release notes accompany the OmniAccess Stellar Operating System (AWOS) Release 4.0.3 software for the Stellar APs. This document provides important information on individual software and hardware features. Since much of the information in the release notes is not included in the hardware and software user manuals, it is important to read all sections of this document before installing new hardware or loading new software.

Contents

Hardware Supported

- AP1101, AP1201, AP1220 series, AP1230 series, AP1251, AP1251-RW-B, AP1261-RW-B, AP1201H, AP1201L, AP1201HL, AP1320 series, AP1360 series, AP1201BG, AP1301, AP1311, AP1351

Fixed Problem Reports Between Build 2054 (MR2) and Build 3067 (MR3)

PR	Description
Case: 00571232 ALEISSUE-1145	**Summary:** AP can't get IP address when a lot of multicast traffic. **Explanation**: Optimize the DHCP performance and add a mechanism to avoid AP missing DHCP packets process. Click for additional information
Case: 00547651 ALEISSUE-1029	**Summary:** Enhance the sta_list command output security type display. **Explanation**: Based on clients' authentication method to classify the WPA type to enhance the command. Click for additional information
Case: 00571463 ALEISSUE-1140	**Summary:** WLAN WIPS - Clients fails several times the WLAN Authentication and is not added into the blacklist **Explanation**: Background scanning service (bg-s) didn't receive the client's wireless packets, hence no client info existed in database. Adding a mechanism to make bg-s create a client entry if there is no corresponding client info when getting notification. Click for additional information
Case: 00584195 ALEISSUE-1176	**Summary:** Problems with final roal length in external server Filter-ID. **Explanation:** Fix the problem with correct character processing. Click for additional information
Case: 00582830 ALEISSUE-1163	**Summary:** LACP issue, when AP connected Cisco switch SG200, can't be pingable.

	Explanation: Root cause: AP mistakenly entered the link aggregation mode when connecting to Cisco SG200. Fix solution: AP will check the aggregation specific state instead of receiving any LACP packet. Click for additional information
Case: 00589099 ALEISSUE-1181	**Summary:** After AP reboot, trap display AP Radio Failure error **Explanation:** For 11ax AP with dedicated scanning radio, incorrect logic was effective after AP rebooting. Adapt the AP Radio Failure trap logic for AP with dedicated scanning radio to fix this problem.

Fixed Problem Reports Between Build 1042 (MR1) and Build 2054 (MR2)

PR	Description
Case: 00573056 ALEISSUE-1139	**Summary:** AP series 13xx sends wrong value DTIM. **Explanation:** Root Cause: The DTIM value was conflict configured by two software modules and one with wrong values. Fix Solution: Modify the software module to utilize correct value. Click for additional information
Case: N/A ALEISSUE-1153	**Summary:** Wired mac address (aa:aa:aa:03:00:00) was found at ethX port in the network. **Explanation:** Root Cause: When received multicast packets from wireless interfaces with multicast optimization enabled, the multicast packets were modified at WLAN driver when being forwarded at bridge, and then the modified packets were forwarded to ethX port. Fix Solution: Change the forwarding logic to avoid this problem. Click for additional information
Case: 00570925, 00550230, 00540308, 00573972 ALEISSUE-1001 ALEISSUE-1044 ALEISSUE-985 ALEISSUE-1038 ALEISSUE-1135 ALEISSUE-1129	**Summary:** APs were stuck, suddenly stopped communicating with OVC. **Explanation:** Root Cause: Invalid client data was not deleted correctly when client roaming between 2.4G band and 5G band on an AP, cause AP stuck when the amount of invalid data became large amount. Fix Solution: Modify to clear the invalid client data after 2.4G/5G band roaming to fix this problem. Click for additional information
Case: 00571044 ALEISSUE-1150	**Summary:** No WAM syslog messages generated **Explanation:** Adding support of generating clients association/disassociation, authentication/de-authentication logs into syslog messages Click for additional information

Case: N/A ALEISSUE-1177	**Summary:** Have syslog messages generated when the STA connection limit is reached **Explanation:** In case of maximum counters reached for Radio or VAP, clients cannot associated to WLAN SSID. Following syslog messages are generated for tracking these counters and when limit is reached: "Per radio Associated STA limit reached!" "calculate real_client_cnt:" "Associated STA limit reached!" "calculate sta_count:
Case: 00570941 ALEISSUE-1127 ALEISSUE-619	**Summary:** Randomly ACL (Policy list) stop working, need to reboot AP to have them back working **Explanation:** Because of a memory leak, randomly policies let the traffic flowing when it should be blocked or sometimes all connected client have no longer access to services, ACL (policy) block all traffic. In order to restore the services, after reboot of the problematic AP services are restored to normal. This was noticed right after updating the policies with new rules. Click for additional information
Case: N/A ALEISSUE-1143	**Summary:** AP will disassociate inactivity clients (medical devices, Smart TVs) when running in cluster mode. **Explanation:** When clients didn't have activity with AP for a long time, AP would set it inactivity status and send disassociation to it. Fix Solution : For cluster mode, adding timeout configuration, only after timeout and a client has no activity with AP, it will be disassociated.
Case: 00571709 ALEISSUE-1131	**Summary:** Radius Shared Secret with special characters doesn't work. **Explanation:** Adding support of '\' character in the password configuration. Click for additional information
Case: 00566949 ALEISSUE-1112	**Summary:** APs are intermittently not accessible, and status is going down in OV.

	Explanation: Root cause: AP's conntrack table is full in a short period of time, resulting in some network service anomalies. Fix solution: Introduce conntrack table extending method to fix this issue. Click for additional information
Case : 00533038 ALEISSUE-972	**Summary:** Users were unable to connect to the AP - need to reboot AP to have them associated again **Explanation:** Root Cause: Clients can't get DNS response sometimes. Fix Solution: Adding mechanism to detect and fix this issue when happens. Click for additional information
Case: N/A ALEISSUE-457	**Summary:** Partial of support commands not supported on 4.0.2. build. **Explanation**: tech_support_command command should add 'ssudo' before it at support account.
Case: 00571683, 00571064 ALEISSUE-1130	**Summary:** Some clients didn't get internet access even after successful portal authentication. **Explanation:** Root cause: when the client connect to SSID before it passed the portal authentication, there will be some rules added to the block list which according to the source and destination MAC address of client, and when the clients passed the authentication ,the related rules will be cleared ,in case of the software module operate(write & modify) the iptables at the same time, it caused the rules not cleared successfully and generate dirty data. Later when the client reconnected to the SSID, the rules added repeatedly, even the client passed the authentication, the dirty data still there and caused the client http traffic blocked and cannot get the portal page. Fix solution: 1. When software module has a conflict operation for iptables, a sleep/wait mechanism will be added to avoid the situation which cleared the rules unsuccessfully. 2. Before the rules added to the block list, AP will check if the related rules existed in the iptables, if yes, the rules will not added again, this will also avoid the issue in other cases. Click for additional information

Case: N/A OVE-10773	**Summary:** Increase the number of static routes to 128 with RAP local breakout
Case: 00582830 ALEISSUE-1163	**Summary:** LACP issue, cannot ping AP1301 when the AP is on Cisco SG220 switch. **Explanation:** The root cause is that AP mistakenly entered the link aggregation mode when any LACP packets is received. Fix solution: AP will check the aggregation specific state instead of only judging on LACP packet received. Click for additional information

Fixed Problem Reports Between Build 4.0.3.1042 (MR-1) and 4.0.3.28

AWOS 4.0.3 MR-1 was a maintenance release for releasing new Stellar AP1261-RW-B model.

Fixed Problem Reports Between Build 4.0.3.28 and 4.0.2.2048

Notes: All the customer issues fixed in AWOS 4.0.2-MR1 and AWOS 4.0.2-MR2 are contained in this build.

PR	Description
Case: 00572393, 00564678, 00514204 ALEISSUE-882	**Summary:** Throughput issue with Wifi6 APs when using encryption type WPA3. **Explanation:** This issue is related to Chipset driver that is updated from release AWOS 4.0.3. Click for additional information
Case: 00566203 ALEISSUE-1111	**Summary:** OmniAccess Stellar AP 1301 stops broadcasting SSID after Ookla Speed Test. **Explanation:** This issue is related to Chipset driver that is updated from release AWOS 4.0.3. Click for additional information
Case: N/A ALEISSUE-990	**Summary:** OmniAccess Stellar AP Wifi6 Users deassociated with reason 34 (Disassociated because excessive number of frames need to be acknowledged, but are not acknowledged due to AP transmissions and\/or poor channel conditions). **Explanation:** This issue is related to Chipset driver that is updated from release AWOS 4.0.3.

Case: 00547651 ALEISSUE-1029	**Summary:** OmniAccess Stellar – Enhance the sta_list command output with authentication + encryption information. **Explanation:** Enhance the sta_list command output with "802.1x - WPA2" if authenticated with WPA2-AES, "802.1x - WPA3" if authenticated with WPA3-AES / WPA3-AES-256. Click for additional information
Case: 00547162 ALEISSUE-1038	**Summary:** OmniAccess Stellar – Rest-API ap.getClient returns a list of strings instead of a dictionary. **Explanation:** HTTPs REST-API ap.getClient returns a list of strings instead of a dictionary per user. Click for additional information
Case: 00543033 N/A	**Summary:** OmniAccess Stellar – 160MHz channel width is not available in Express mode. **Explanation:** Option for setting the Channel Width 160MHz on 5Ghz band is not available. Click for additional information
Case: 00542487 ALEISSUE-1009	**Summary:** OmniAccess Stellar – Wifi Users unable to login to Employee sponsor page with Windows Active Directory credentials. **Explanation:** Customer expects restrict access to Employee sponsor page based on Windows AD. Click for additional information
Case: 00516835 ALEISSUE-913	**Summary:** OmniAccess Stellar Wifi6 APs Multicast/Unicast packets are dropped. **Explanation:** This issue is related to Chipset driver that is updated from release AWOS 4.0.3. Click for additional information
Case: N/A ALEISSUE-935	**Summary:** Upgrade dnsmasq version on AP for fixing vulnerability. **Explanation:** Vulnerability named DNSpooq is found in current dnsmasq v2.80, it is fixed by using official patch 2.80-dnspooq.patch.v3 on current version.
Case: N/A ALEISSUE-936	**Summary:** Upgrade Busybox version on AP for fixing vulnerability. **Explanation:** 11AX products uses busybox v1.25.1 which is reported some vulnerabilities on CVE, it is fixed by upgrading busybox version to 1.30.1.

Case: ALEISSUE-1030	**Summary**: Stellar AWOS 4.0.3 // WPA3-Enterprise is doing fallback in WPA2-Enterprise whatever we select Authentication type WPA3_AES or WPA3_AES_256. **Explanation**: In current AP build, when create WLAN with WPA3_AES or WPA3_AES_256, if client does not support WPA3, it can also connect with WPA2, in 403 GA build, it provides an option for PMF to prevent WPA3 fallback, this can be configured if necessary.
Case: 00558026 ALEISSUE-1091	**Summary**: LACP connection between the switch and the Eth1 port of the AP doesn't work. **Explanation**: When both uplink ports connecting to switch and link-aggregation formed, after rebooting AP enters a stuck state and not working correctly. Correct the LACP process logic to fix this problem. Click for additional information

Open Problem Reports and Known Issues

The problems listed here include problems known at the time of the product's release. Any problems not discussed in this section should be brought to the attention of the Service and Support organization as soon as possible. Please contact customer support for updates on problem reports (PRs) where no known workaround was available at the time of release.

ALEISSUE-990	Deauthentication reason 34(Disassociated because excessive number of frames need to be acknowledged, but are not acknowledged due to AP transmissions and\/or poor channel conditions). Use the command `grep deauth /proc/kes_debug` for listing the deauthentication messages	Will be fixed in AWOS 4.0.4
ALEISSUE-1169	Deauthentication reason 2(IEEE80211_REASON_AUTH_EXPIRE(Previous authentication no longer valid)) Use the command `grep deauth /proc/kes_debug` for listing the deauthentication messages	Will be fixed in AWOS 4.0.4
ALEISSUE-973	Guest users cannot authenticate over Captive Portal when a Proxy Server is enabled. Click for additional information	In current 403 build, HTTP Captive Portal redirection over proxy is supported, but not HTTPS. Will be supported in AWOS 4.0.4.

ALEISSUE-1028	802.11 Frame Aggregation and Fragmentation Vulnerabilities.	Will be fixed in AWOS 4.0.4.
ALEISSUE-1027	Guard Interval can't be changed on the WIFI6	Will be fixed in AWOS 4.0.4
WCF limitations	Cache is done at the AP level and is limited to 2000 entries, cache is removed every 12 hours, this is not configurable. An AP will allow any URL to be accessed by the first time a user visits that URL, while the AP tries to determine whether this URL is to be restricted for this Access Role Profile or not. If the URL is to be restricted, subsequent users belonging to the same Access Role Profile will then be blocked from visiting this restricted URL. So, on any given AP, Web Content Filtering will not be effective for the first visitor of a restricted URL. Web Content Filtering rules will be effective for such first visitors only after DNS cache expires on the user device • if we consider only one user is connecting behind RAP or AP, this user will never be restricted if we consider the above limitation, every 12 hours one user will be able to access the website	There is no known workaround at this time.
WCF limitations	When a client tries to access a website (category) that is restricted for access by admin, the client will see the page fails to load, and the browser will finally display a generic error.	There is no known workaround at this time.
Management VLAN	When the management VLAN is enabled, setting the static IP may fail	The static IP must be set first, and then enable the management VLAN.
DPI	[reflexive] configure link tracking. DPI_DROP does not take effect.	After modifying the reflexive rules, the client needs to go online and offline again, which can return to normal.
AP stateful ipv6 address	The ipv6 address of the dual-stack AP, AP is a stateful address. After configuring the open type of WLAN, to associate the WLAN, with the wireless network card of win 7 11n set to single-stack V6, check the network on-off condition of the V6 address.	When you manually configure a IPv6 address of the same network segment on the client as the gateway address, you can communicate with the same network address.

DPI FTP policy	Create one policy list binding and two policies, results that the user cannot access the ftp	There is no known workaround at this time.

New Features Introduced – 4.0.3.3067

The following software features are new with this release, subject to the feature exceptions and problem reports described later in these release notes:

None.

Limitations and/or Dependencies

Feature	AP Model	Limitations and/or Dependencies
Wired Port	AP1201HL	AP1201HL switches to a Group with downlink configuration, wired client cannot access it.
DRM	All	In some cases, when the channel utilization reaches more than 90%, the channel does not switch automatically, which seriously affects the user experience.
IGMP Snooping	AP1301/AP1311/AP1320 Series /AP1360 Series	For 11AX devices, if there is no multicast querier in the environment, the conversion from multicast to unicast may fail. We recommend that the switch of IGMP Snooping feature be turned on by default.
Mesh	All	Multicast to unicast is not supported in Mesh mode. Because root AP to non-root AP does not implement the function of multicast to unicast in mesh mode, even if the client on non-root AP implements multicast to unicast, the efficiency is still not high.
DPI	AP1201 AP1220 series, AP1251	When DPI function is enabled, it is recommended to have an initial free memory size of about 30MB after AP booting up for system stable running. If the booting up free memory size is far less than 30MB, suggest removing unnecessary WLAN/VLAN/Policy/DPI rule on AP1201/AP1220/AP1251.
Bypass VLAN	AP1201H/AP1201HL	If the bypass VLAN function is enabled, setting VLAN id A, and setting the management VLAN to tag VLAN id is also A, which will cause the AP itself to be inaccessible and affect the operation of AP. Therefore, there is a restriction here that the tag for managing VLAN cannot be the same as bypass.
mDNS	AP1201H/AP1201HL	AP1201H/1201HL Downlink Terminal does not support mDNS message forwarding.
Show device name	All	When some clients connect to wlan, there is no option12 field in the dhcp message, so its hostname cannot be displayed.
DPI	AP1311/AP1301	DPI is not supported on AP1301 & AP1311 products in this release.
Management VLAN Static IP	AP1351	When configure LACP + Management VLAN + Static IP for AP1351, the network will not be reachable after AP reboot if LACP aggregated link is formed, the workaround of this issue should be disable LACP on switch side.

LACP		
Link aggregation	All	Link aggregation with management VLANs has a certain probability of failure

Technical Support

Alcatel-Lucent Enterprise technical support is committed to resolving our customer's technical issues in a timely manner. Customers with inquiries should contact us at:

Region	Phone Number
North America	1-800-995-2696
Latin America	1-877-919-9526
Europe Union	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484

Email: ebg_global_supportcenter@al-enterprise.com

Internet: Customers with Alcatel-Lucent service agreements may open cases 24 hours a day via Alcatel-Lucent's support web page at: https://myportal.al-enterprise.com/.

Upon opening a case, customers will receive a case number and may review, update, or escalate support cases on-line. Please specify the severity level of the issue per the definitions below. For fastest resolution, please have telnet or dial-in access, hardware configuration—module type and revision by slot, software revision, and configuration file available for each switch.

Severity 1 - Production network is down resulting in critical impact on business—no workaround available.

Severity 2 - Segment or Ring is down or intermittent loss of connectivity across network.

Severity 3 - Network performance is slow or impaired—no loss of connectivity or data.

Severity 4 - Information or assistance on product feature, functionality, configuration, or installation.