

Release Notes

OmniAccess Stellar AP

AWOS Release 4.0.4 - MR5 Release

These release notes accompany the OmniAccess Stellar Operating System (AWOS) Release 4.0.4 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.

Table of Contents

Related Documentation	3
Hardware Supported	4
Fixed Problem Reports Between Build 4.0.4.5094 and 4.0.4.4080	4
Fixed Problem Reports Between Build 4.0.4.4080 and 4.0.4.3066	5
Fixed Problem Reports Between Build 4.0.4.3066 and 4.0.4.2046	6
Fixed Problem Reports Between Build 4.0.4.2046 and 4.0.4.1029	8
Fixed Problem Reports Between Build 4.0.4.1029 and 4.0.4.9	10
Open/Known Problems	13
Limitations and/or Dependencies	14
New Software Feature Descriptions	16
Technical Support	16

Related Documentation

The release notes should be used in conjunction with the associated manuals as listed below.

User manuals can be downloaded at: <https://myportal.al-enterprise.com/>.

Stellar AP Quick Start Guide

The Quick Start Guide assists you in quickly connecting to and configuring the Stellar AP.

Stellar AP Installation Guide

Provides technical specifications and installation procedures for the Stellar AP.

Stellar AP Configuration Guide

Includes procedures for managing and configuring all aspects of the Stellar AP using the built-in web interface.

Technical Tips, Field Notices, Upgrade Instructions

Contracted customers can visit our customer service website at: <https://myportal.al-enterprise.com/>.

Hardware Supported

- AP1101, AP1201, AP1220 series, AP1230 series, AP1251, AP1251-RW-B, AP1261-RW-B, AP1201H, AP1201L, AP1201HL, AP1320 series, AP1360 series, AP1201BG, AP1301, AP1301H, AP1311, AP1331, AP1351.

Fixed Problem Reports Between Build 4.0.4.5094 and 4.0.4.4080

PR	Description
Case: 00620154 ALEISSUE-1294	<p>Summary: SSH weak exchange algorithm detected- Vulnerability analysis with Stellar AP.</p> <p>Explanation: The SSH server was configured to allow weak key exchange algorithms. We added a patch to disabled those weak exchange algorithms.</p> <p>Click for additional information</p>
Case: N/A ALEISSUE-1289	<p>Summary: All Wi-Fi 6 AP13xx-RW should support -IL country code for Israel.</p> <p>Explanation: All the Wi-Fi 6 AP13xx-RW drivers meet this requirement.</p>
Case: 00628502 ALEISSUE-1314	<p>Summary: AP 1331 working in 20 MHz instead of 80 Mhz.</p> <p>Explanation: This is because there was a limit on the 80 MHz mode for specific country code, removed this limitation to solve the issue.</p> <p>Click for additional information</p>
Case: N/A ALEISSUE-1323	<p>Summary: Support for AP1301-JP.</p> <p>Explanation: New model requirement.</p>

Fixed Problem Reports Between Build 4.0.4.4080 and 4.0.4.3066

PR	Description
Case: 00622876 ALEISSUE-1280	<p>Summary: Stellar AP - have log/syslog message for channel utilization.</p> <p>Explanation: This is an enhanced feature to periodically record the channel utilization and band info, meanwhile will be having a log when crossing the setting utilization threshold.</p> <p>Click for additional information</p>
Case: 00612871 ALEISSUE-1263	<p>Summary: Lack of accuracy in ACS-related log descriptions.</p> <p>Explanation: Logs are recorded when the AP detects current high channel utilization, making the log description more accurate and understandable.</p> <p>Click for additional information</p>
Case: 00612342 ALEISSUE-1266	<p>Summary: IP address changed for the URL mentioned in walled garden is not aged.</p> <p>Explanation: There is a TTL field inside the DNS record that describes the time to live of the IP address, we will use this field for the aging time of the IP address, when the client re-generates DNS requests for the domain name AP will clean up those IP addresses with aging DNS records.</p> <p>Click for additional information</p>
Case: 00618311 ALEISSUE-1285	<p>Summary: Client not connecting with WPA3 in dot1x SSID.</p> <p>Explanation: The AP is missing the relevant AKM suite selector for the WPA3 encryption method in 802.1x authentication mode, add the right AKM suite selector for WPA3.</p> <p>Click for additional information</p>
Case: 00620715 ALEISSUE-1288	<p>Summary: AP stuck in boot sequence and reboot because of kernel panic.</p> <p>Explanation: This exception is related to ADME function.</p> <p>Click for additional information</p>
Case: 00620286 ALEISSUE-1290	<p>Summary: Aps are rebooting randomly in the network and showing down in OV2500.</p> <p>Explanation: The CPU is busy due to multicast or broadcast traffic, etc., and cannot handle the application layer's dog feeding operation, causing the AP to restart due to watchdog starve. Adding the functions of driver dog feeding and broadcast multicast speed limit can solve the watchdog</p>

	<p>starve reboot caused by untimely dog feeding or burst traffic. This feature is turned off by default and can be configured to turn on.</p>
<p>Case: 00621712 ALEISSUE-1295</p>	<p>Summary: Stellar AP remains in channels width 20 MHz when RF Profile is set to 80 MHz.</p> <p>Explanation: DRM code update in order to take into account the regulation of Israel country and a maximum of width set to 160MHz.</p> <p>Click for additional information</p>
<p>Case: N/A ALEISSUE-1167</p>	<p>Summary: Assa Abloy Integration - Lock wrongly displayed as offline.</p> <p>Explanation: ZCS Code logic updated in order to judge if the device is offline or down.</p>
<p>Case: 00620093 ALEISSUE-1286</p>	<p>Summary: Stellar Aps sending CDP frames with system OS information.</p> <p>Explanation: For 802.11ac devices, the native CDP protocol is supported and carries native system information.</p> <p>Click for additional information</p>

Fixed Problem Reports Between Build 4.0.4.3066 and 4.0.4.2046

PR	Description
<p>Case: 00606263 ALEISSUE-1239</p>	<p>Summary: Download Syslog from AP returns an empty file from Web AP UI.</p> <p>Explanation: This feature is useless and will be removed in this AWOS releases. In order to collect syslog messages, you can go thru OV -> Administration -> Collect Support Info -> select AP and download logs or thru AP UI -> Tools -> Collect snapshot logs.</p> <p>Click for additional information</p>
<p>Case: 00608473 ALEISSUE-1248</p>	<p>Summary: 802.1x users with Dynamic VLAN not able to connect to Stellar AP.</p> <p>Explanation: 802.1x users with Dynamic VLAN are not able to connect to Stellar AP randomly, workaround is to reboot the AP. The application Access Guardian, which is responsible for creating dynamic VLANs, has limitation for 64 for maximum supported VLAN number, the counter increased incorrectly even same VLAN applied multiple times and failed to create new VLAN when the counter reached 64.</p>

	<p>Click for additional information</p>
<p>Case: 00605141 ALEISSUE-1235 ALEISSUE-1251</p>	<p>Summary: Stellar internal DHCP server stops responding to DHCP discover after AP reboot.</p> <p>Explanation: This issue is observed only on WIFI5 Aps. The interface of the AP is not yet up after the DHCP server application starts which result of DHCP application does not start.</p> <p>Click for additional information</p>
<p>Case: 00607780 ALEISSUE-1233</p>	<p>Summary: AP MAC is learnt on all client VLAN.</p> <p>Explanation: Issue is triggered by the IVP6 multicast packet sent on all client VLAN.</p> <p>Click for additional information</p>
<p>Case: 00594340 ALEISSUE-1201</p>	<p>Summary: When deploying 2 SSIDs configured with different GTTS Tunnel IDs, the associated tunnel ID is randomly wrongly assigned.</p> <p>Explanation: The issue is being triggered by wrong mac-VLAN mapping getting created due to an exception caused.</p> <p>Click for additional information</p>
<p>Case: 00612465 ALEISSUE-1253</p>	<p>Summary: There is a lot of logs about IoT when enabled IoT and no clients connected.</p> <p>Explanation: When the IoT function is enabled, there are lot of errors logs <code><iot_sta_info_report mqtt disconnect or is empty></code>. The solution is to reduce the printing of logs in this scenario when there is no client connection.</p> <p>Click for additional information</p>
<p>Case: 00607267 ALEISSUE-1238</p>	<p>Summary: Kernel error logs generated by 802.11AX Stellar Aps.</p> <p>Explanation: Some AX series AP because there is a dedicated scan radio, will generate a lot of FW level log, these logs are basically useless and confusing.</p> <p>Click for additional information</p>
<p>Case: 00604900 ALEISSUE-1229</p>	<p>Summary: Express mode - if AP fails to download the configuration file from PVC it will result into config failure and AP is stuck into Initializing state.</p> <p>Explanation: The cause of the problem is a high network latency and downloading the configuration from PVCs exceeds the set 30s timeout time resulting in failure. Change the timeout for</p>

	<p>downloading configuration from PVC from 30s to 60s to as defense mechanism against the network latency.</p> <p>Click for additional information</p>
--	--

Fixed Problem Reports Between Build 4.0.4.2046 and 4.0.4.1029

Notes: All the customer issues fixed in AWOS 4.0.3 MR5 are contained in this build.

PR	Description
Case: N/A ALEISSUE-1210	<p>Summary: Configured AP-name not sent in the LLDP Packets.</p> <p>Explanation: Current AP LLDP program use AP model name as System Name of LLDP packets. Modify the LLDP program parameter to make the AP name as System Name of LLDP packets.</p> <p>Click for additional information</p>
Case: N/A ALEISSUE-1205	<p>Summary: Stellar AP does not switch channel after rf profile has been applied.</p> <p>Explanation: The current working channel is not inside the channel list in the new RF profile, meanwhile according to the automatic channel selection algorithm it cannot switch to the selected channel list because of the selected channel list and the bandwidth setting. To fix this issue, when applying a new RF profile, if the currently working channel is not in the list of newly selected channels, one of the new channels is randomly selected to apply.</p> <p>Click for additional information</p>
Case: N/A ALEISSUE-1203	<p>Summary: Command <code>sudo ME_5G enable disable</code> to be supported on AP1360-ME.</p> <p>Explanation: WLAND module set country code incorrectly when setting ME_5G enable, fix that by setting country code to IL.</p> <p>Click for additional information</p>
Case: N/A ALEISSUE-1206	<p>Summary: Packet dropped by AP stellar in root mesh mode.</p> <p>Explanation: In the case of several modules operating iptables rules at the same time, those rules created by EAG before client authentication are still not deleted after authentication, so after client re-connect these rules for the client still exist, causing the client traffic to be discarded. We add lock in the internal iptables library and iptables instance to protect race access and to ensure that iptables rules are created and deleted correctly.</p>

	<p>Click for additional information</p> <p>https://myportal.al-enterprise.com/alebp/s/tkc-redirect?000065931</p>
<p>Case: N/A</p> <p>ALEISSUE-1130</p> <p>ALEISSUE-1194</p>	<p>Summary: SR# 00592179: Wifi user did not get the portal page.</p> <p>Explanation: Because of clients concurrent association of Aps, this leads to race between WAM and EAG, and individual instances of iptables, resulting in incorrect processing of iptables rules. Added lock in the internal iptables library and iptables instance to protect race access.</p> <p>Click for additional information</p>
<p>Case: N/A</p> <p>ALEISSUE-1106</p>	<p>Summary: Nessus scan discovered a few vulnerabilities for stellar APs.</p> <p>Explanation: Remove cipher suites ECDHE-RSA-RC4-SHA RC4-SHA RC4-MD5 ECDHE-RSA-DES-CBC3-SHA DES-CBC3-SHA of MQTT broker service due to those with MD5 and DES are not secure.</p> <p>Click for additional information</p>
<p>Case: N/A</p> <p>ALEISSUE-1204</p>	<p>Summary: Bridge between 2 AP is randomly disconnected / connected many times in a few minutes.</p> <p>Explanation: The issue is fixed by ignoring the beacon miss event by Client AP and then it will not deauth from Root AP.</p> <p>On 4.0.4 MR2, the ignoring beacon miss event needs to be enabled manually through support account if needed.</p> <p>Click for additional information</p>
<p>Case: N/A</p> <p>ALEISSUE-1198</p>	<p>Summary: SR# 00596479: AP 1101 rebooted due to “Watchdog starve”.</p> <p>Explanation: Added feeding watchdog on 9ernel space layer and broadcast multicast speed limit function, which can solve the watchdog starve restart caused by not feeding watchdog in time or huge burst traffic happen in some specific network.</p> <p>Click for additional information</p>
<p>Case: N/A</p> <p>ALEISSUE-1028</p>	<p>Summary: 802.11 Frame Aggregation and Fragmentation Vulnerabilities.</p> <p>Explanation: Add vendor-specific patches for addressing Frame Aggregation and Fragmentation Vulnerabilities.</p> <p>Click for additional information</p>

Fixed Problem Reports Between Build 4.0.4.1029 and 4.0.4.9

Notes: No customer issues reported on 4.0.4.9 (GA release dedicated to new model OAW-AP1301H), All the customer issues fixed in AWOS 4.0.3 MR4 are contained in this build.

PR	Description
<p>Case: 00590006 ALEISSUE-1190</p>	<p>Summary: AP can't work at 802.11ax mode in Russia country code.</p> <p>Explanation: Modify AP board data to support 802.11ax mode in Russia country code.</p> <p>Click for additional information</p>
<p>Case: 00592179 ALEISSUE-1194</p>	<p>Summary: WiFi user can't get portal page at sometimes.</p> <p>Explanation: Sometimes when the client does not interact with the AP by sending 802.11 messages, AP cannot obtain information about the client and cannot delete the relevant access policy resulting of issue when redirecting to Captive Portal page.</p> <p>Click for additional information</p>
<p>Case: 00588845 ALEISSUE-1169</p>	<p>Summary: AP send death to clients with reason 2 when clients disassociated with AP.</p> <p>Explanation: When AP received clients offline event, it wrongly didn't clear relevant resource, and after the client's resource timer expired AP send death reason 2 to this client.</p> <p>Click for additional information</p>
<p>Case: N/A ALEISSUE-1158</p>	<p>Summary: Record Syslog message after AP crashed.</p> <p>Explanation: Generate a Syslog message "[sysreboot]: =Power Off" after rebooting and detecting AP crash. This kind of reboot is usually observed when a LANPOWER defect is observed on switch, for OmniSwitch please ensure the capacitor-detection is disabled.</p> <p>Click for additional information</p>
<p>Case: 00586612 ALEISSUE-1175</p>	<p>Summary: AP-1201BG management SSID not able to disable.</p> <p>Explanation: The front-end page is missing the relevant configuration, as a workaround we can add any Stellar AP model supporting Wi-Fi within the cluster, once this AP will be elected as PVM administrator can disable the Management SSID. As of AWOS 4.0.4 MR-1 if all Aps models are AP1201BG we expose on the Cluster management page the possibility for deactivating the Management SSSID.</p> <p>Click for additional information</p>

<p>Case: 00582383 ALEISSUE-1192</p>	<p>Summary: WiFi clients traffic are forwarded to Management VLAN.</p> <p>Explanation: IP forward function is turned on in the AP, the use's broadcast traffic will be the AP's management vlan, discard such traffic on the management bridge.</p> <p>Click for additional information</p>
<p>Case: N/A ALEISSUE-1159</p>	<p>Summary: No Syslog message generated when client is added to blocklist.</p> <p>Explanation: Adding following syslog message when client's MAC Address is added in the blocklist: <NOTICE> [AP <AP_MAC_Address>@<AP_IP_Address>] : [tid:xx] [Add blacklist mac is <device_mac_address>]</p>
<p>Case: 00574007 ALEISSUE-1138</p>	<p>Summary: Vulnerability check.</p> <p>Explanation: The vulnerability exists in DHCP Server service, in this release DHCP Server service is running only when this is enabled, by default, AP does not run this service.</p> <p>Click for additional information</p>
<p>Case: 00573237 ALEISSUE-1136</p>	<p>Summary: callhome_hash.json file is empty.</p> <p>Explanation: Call home configuration file is found empty, it is enhanced by adding backup mechanism when previous configuration is empty, backup file will recover.</p> <p>Click for additional information</p>
<p>Case: 00571709 ALEISSUE-1131</p>	<p>Summary: Radius Shared Secret with special characters doesn't work after AP reboot.</p> <p>Explanation: It is due to character '\ ' and ':' are not supported on AWOS 4.0.3 builds, it is solved by adding support for those characters.</p> <p>Click for additional information</p>
<p>Case: 00570454 ALEISSUE-1126</p>	<p>Summary: OmniVista does not allow backslash as PSK/Passphrase.</p> <p>Explanation: It is due to character '\ ' and ':' are not supported on AWOS 4.0.3 builds, it is solved by adding support for those characters.</p> <p>Click for additional information</p>
<p>Case: 00564932 ALEISSUE-1106</p>	<p>Summary: Nessus scan discovered a few vulnerabilities for stellar Aps.</p>

	<p>Explanation: Remove TLS1.0 and TLS1.1 support of MQTT broker service due to TLS1.0 and TLS1.1 is not secured.</p> <p>Click for additional information</p>
Case: 00544344 ALEISSUE-1017	<p>Summary: RADIUS Authentication Requests are not redirected to OV/UPAM HA Active Node when back into service.</p> <p>Explanation: Adding the support of RADIUS Server preemption, AP is checking every 5 minutes (introduced Radius Authentication Server Down timer) the status of the Radius Primary Server. Once active back, Primary Radius Server will preempt over Backup.</p> <p>Click for additional information</p>

Open/Known Problems

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.

PR	Description	Workaround
ALEISSUE-1265 ALEISSUE-1241	Poor Wifi connection when a high channel utilization is noticed on Stellar AP 802.11ax models (lot of Tx retries observed on OV 2500 -> WLAN -> Wireless Client List -> List of Clients on All Aps)	Disable the High Efficiency at the RF Profile level
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).	Will be fixed in AWOS 4.0.5
WCF	WCF Feature is not supported when WLAN Client is running behind an HTTP Proxy	No workaround
WCF	WCF Feature is not supported when WLAN Client is using mobile applications, there is no restrictions (packets are not dropped by AP, no redirection to Restricted Web page)	No workaround
WCF	WCF Feature is not supported when WLAN Client is running IPv6	No workaround
DSCP	DSCP downlink direction does not take effect on 11AX products.	Will be fixed on AWOS 4.0.5
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, 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 V6 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.
ALEISSUE-1274	L2 GRE Tunnel issue	Will be fixed on AWOS 4.0.5
ALEISSUE-1310	Policy memory leak after enable L2 isolation.	Will be fixed on AWOS 4.0.5

ALEISSUE-1308	Interface vlan configuration lost when WLAN access timer is configured	Will be fixed on AWOS 4.0.5
---------------	--	-----------------------------

Limitations and/or Dependencies

Feature	AP Model	Limitations and/or Dependencies
Trust Tag	AP1301H	It's not supported in this release, will be supported in next AWOS 4.0.5
Bypass VLAN	AP1301H	It's not supported in this release, will be supported in next AWOS 4.0.5
WCF	All	<ol style="list-style-type: none"> 1. WCF does not support http over proxy scenario. 2. WCF does not support blocking mobile applications access. Client's packets are not restricted (packet not dropped by AP, no redirection to Restricted Web Page) 3. WCF does not support RAP scenario. 4. When using Iphone roaming between Aps, reject page can't be redirected when using Safari, but it works ok for other browser such as Chrome
RAP	All	RAP does not support tagged VLAN on the Downlink ports
HTTPs CP over proxy	All	For iOS does not support to configure URL to bypass the proxy, this function does not work on iOS devices.
AP 802.1x client	All	Wireless clients can't connect to internet on untag VLAN with AOS switch due to AOS switch treat all untag devices as 802.1x client.
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	All Stellar Wi-Fi 6 AP Models	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	<p>Multicast to unicast is not supported in Mesh mode.</p> <p>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.</p>
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 /AP1261- RW-B	AP1201H/1201HL/AP1261-RW-B 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.
Management VLAN Static IP LACP	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.
Link aggregation	All	Link aggregation with management VLANs has a certain probability of failure
ALEISSUE-1294	All	This improvement might cause some lower version of SSH clients can not connect to Stellar AP running this new build, upgrade SSH client version will avoid this problem.

New Software Feature Descriptions

There is no new feature in this release.

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.

www.al-enterprise.com The Alcatel-Lucent name and logo are trademarks of Nokia used under license by ALE. To view other trademarks used by affiliated companies of ALE Holding, visit: www.al-enterprise.com/en/legal/trademarks-copyright. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. © Copyright 2022 ALE International, ALE USA Inc. All rights reserved in all countries.