Release Notes

OmniAccess Stellar AP

AWOS Release 5.0.5 GA – Release

These release notes accompany the OmniAccess Stellar Operating System (AWOS) Release 5.0.5 GA 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.

Release Notes
Part Number 033838-00 Rev. A

Alcatel-Lucent.
Copyright © 2026. All rights reserved.

Table of Contents

Related Documentation **3**
Hardware Supported **4**
Supported Mode **4**
New Software Features and Enhancements **4**
Fixed Problem Reports Between Build 5.0.4.3042 and 5.0.5.14 ..... **4**
Open/Known Problems **6**
Limitations and/or Dependencies **8**
New Software Feature Descriptions **11**
Technical Support **12**

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, AP1311BG, AP1331, AP1351, AP1411, AP1431, AP1451, AP1501, AP1501S, AP1511, AP1521, AP1561, AP1570 series，AP1540 series.

Supported Mode

- The AWOS 5.0.5.14 is applicable for Express mode, OmniVista 2500, OmniVista Cirrus 4, OmniVista Cirrus 10, and OmniVista Terra.

New Software Features and Enhancements

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

Feature	Platform Support
New hardware AP1501S	WiFi 7
Support CoA and DM for 1x or MAC auth	WiFi 6 and WiFi7
LDAP optimization	WiFi 6 and WiFi7
RAP support OVTX	All
Support enable/disable TSO	All

Fixed Problem Reports Between Build 5.0.4.3042 and 5.0.5.14

PR	Description
ALEISSUE-2136 SR # 00766306	**Summary:** AP-1221 Crashing when DPI is enabled. **Explanation:** Fixed AP crash when DPI is enabled. Click for additional information
ALEISSUE-2327 SR # 00846301	**Summary:** OAW-stellar AP 1301H: client traffic is not forwarding out from AP. **Explanation:** Fixed client traffic forwarding failure on AP 1301H. Click for additional information
ALEISSUE-2413 SR # 00861912	**Summary:** Issue regarding the CoA Posture assessment **Explanation:** Fixed CoA posture assessment issue on OV2500. Click for additional information
ALEISSUE-2425 SR # 00865329	**Summary:** AP fails to read option 138 info **Explanation:** DHCP timeout issue fixed.

	Click for additional information
ALEISSUE-2430 SR # 00869106	**Summary:** Airtime Fairness (ATF) not working **Explanation:** Fixed Airtime Fairness (ATF) not working on Stellar APs. Click for additional information
ALEISSUE-2440 SR # 00868247	**Summary:** Alerts received for APs in OVNA **Explanation:** Fixed unexpected alerts received for APs in OVNA. Click for additional information
ALEISSUE-2445 SR # 00874424	**Summary:** Incorrect 2.4 GHz Channel Values (0 and 100) Observed on OV and AP GUI **Explanation:** Fixed incorrect 2.4 GHz channel values (0 and 100) shown on OV and AP GUI. Click for additional information
ALEISSUE-2455 SR # **00861611**	**Summary:** Stellar AP Sending traffic with random unknown MAC address **Explanation:** Fixed AP 1321 sending traffic with random unknown MAC addresses. Click for additional information
ALEISSUE-2465 SR # 00882041	**Summary:** Client failing DSPSK authentication **Explanation:** Fixed DSPSK authentication failure on APs. Click for additional information
ALEISSUE-2468 SR # 00885956	**Summary:** After modification in channel list AP do not change channel without reboot **Explanation:** Fixed AP not switching channel after channel list modification without rebooting. Click for additional information
ALEISSUE-2479 SR # 00879410	**Summary:** Stellar APs send multiple RADIUS request with username testuser **Explanation:** Fixed Stellar APs sending multiple RADIUS requests. Click for additional information
ALEISSUE-2485 SR # 00882302	**Summary:** ARP Proxy Process Stuck Causing ARP Forwarding Failure, Client Connectivity Loss, and AP Management Issues **Explanation:** Fixed ARP proxy process stuck causing ARP forwarding failure and client connectivity loss. Click for additional information

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
AP stateful IPv6 address	The IPv6 address of the dual-stack 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.	No workaround.
WCF	WCF does not support L3 roaming scenarios.	No workaround.
Option82	After enabling option82 feature, in some scenarios, user roaming and reacquiring IP addresses can cause a brief broadcast storm.	Will be fixed in future release.
6G wIPS	6G radio does not support wIPS feature.	Will be supported in future release.
mDNS	AP1411/AP1431 does not support mDNS feature.	Will be supported in future release.
DPI	DPI memory leak issue.	Will be fixed in future release.
Captive Portal	The client can access the network without CP authentication in roaming scenarios.	Set a default ARP in Authentication Strategy.
Enhanced Open	Modify Enhanced OSpen WLAN to Open, Client can't obtain IP address, this issue happens only on AP1101.	Disable/Enable WLAN. Will be fixed in future release.
Client Isolation	If the wired client is configured with a static IP, the wired isolation function for this client will not take effect	Will be fixed in future release.
Roaming	AP will not resend client information to its neighbors after they restart for some reason. This can lead to some roaming failure issues.	Will be fixed in future release.
DRM	DRM will not trigger active scanning if the current channel is not in the user configured channel list. This will lead to uneven distribution of channels.	Will be fixed in future release.
Wi-Fi 7 MLO	Simultaneously enabling MLO and 11R roaming will cause the client's 11R roaming to fail for WiFi7 devices.	Will be fixed in future release.
Wi-Fi 7 MLO	Clients that do not support the 'BIP-GMAC-256' algorithm cannot connect to MLO+WPA3 WLAN	Will be fixed in future release.
mDNS	When mDNS clients and servers are in different VLANs, clients can discover shared services but cannot access it.	Will be fixed in future release.
MESH	When the root AP restarts abnormally or the mesh becomes disabled, the BE devices under the root are offline for a long time	Will be fixed in future release.
WLAN	The Beacon Interval configuration for MLO WLAN devices on the BE platform will not take effect	Will be fixed in future release.

Multicast Optimization	The multicast optimization function of devices on the AX/BE platform is abnormal	Will be fixed in future release.
PG-PSK	After successful roaming of PGPSK Layer 3 or Layer 2 80211r, if the ARP assigned to the client in AP2 is incorrect, the client will go offline and reconnect when roaming to AP1 again.	Will be fixed in future release.
MLO	Frequent modifications to the MLO switch of the mesh root AP may cause mesh subordinate devices to experience kernel panic and restart.	Will be fixed in future release.
MESH	In the 6G mesh configuration environment, upgrading the AP1521 model device leads to a lower negotiation rate.	Will be fixed in future release.
Trust VLAN	Enabling the trust VLAN may cause the AP1201H device's CPU to become overloaded and freeze when identical VLANs exist within the same tunnel.	Will be fixed in future release.
Policy	The WiFi7 device can't configure Layer4 service group.	Will be fixed in future release.
Policy	When multiple "Policy" are bound to the same "Network Group", the rules do not take effect when the group is modified.	Will be fixed in future release.
IoT Enforcement	Enable the IoT Enforcement function and enable Dynamic VLAN and configure it as "Priority VLAN-ID over ARP". The client does not obtain the correct Access Role assigned by IoT Enforcement.	Will be fixed in future release.
WLAN	Some WLANs fail to be created when WiFi 7 APs switch Group for the first time in the OmniVista Cirrus 10 environment.	Will be fixed in future release.
Connectivity	iPhone 15 Plus loses connection after roaming in certain scenarios.	Will be fixed in future release.
Roaming	The iPhone 12 experiences failed 1x authentication roaming in specific scenarios.	Will be fixed in future release.
Power Consumption	There is a probability that configuring the 160M bandwidth of AP1331 through the Power Consumption function will not take effect.	Will be fixed in future release.
OWE Transition Mode	When configuring 16 ESSIDs, enabling OWE Transition mode will cause the interface creation to fail.	Will be fixed in future release.
Power Consumption	After frequently switching the turned-off radio, there is a probability that the radio's status is inconsistent with the configuration.	Will be fixed in future release.
Macsec	When the switch enables 1x authentication and disables Macsec authentication, while the AP side enables both 1x authentication and Macsec authentication, the AP cannot obtain an IP address.	Will be fixed in future release.
Option 82	Option 82 feature not supported in Management VLAN and VLAN poll scenarios	Will be fixed in future release.

WLAN	In some scenarios, when the MLO interface is disabled and then enabled again, it does not take effect.	Will be fixed in future release.
DSCP Mapping	The DSCP Mapping not working for MLO client.	Will be fixed in future release.
Performance	For better performance, it is recommended that WiFi7 devices do not create more than 8 WLANs per band.	Will be fixed in future release.
WIDS/WIPS	The channel of the rogue AP obtained by the Wi-Fi7 AP does not match the actual one, which affects the functions of WIDS and WIPS.	Will be fixed in future release.
Mesh	The None-root MLO mesh client fails to associate in certain scenarios, so it is not recommended to use the MLO mode to create a mesh connection.	Will be fixed in future release.
WIPS	Cross-channel suppression on Wi-Fi 7 devices has problems	Will be fixed in future release.
Remote Capture	In some scenarios, the failure to switch channels on 40MHz bandwidth leads to the termination of packet capture.	Will be fixed in future release.
Access	Some terminals experience probabilistic PSK handshake failures, resulting in access failures.	Will be fixed in future release.
WLAN	Creating 256 VLANs on AP1540/AP1541 takes approximately 10 to 20 minutes to complete.	Will be fixed in future release.
Downlink Port	AP1361 fails to load the configuration for eth1 under certain scenarios when eth1 operates as a downlink port.	Will be fixed in future release.
WIFI7 AP	Certain STA clients can trigger stability problems on the AP.	Will be fixed in future release. Workaround: disable UAPSD in WLANSerivce.
IPv6	Cluster wizard configuration is unavailable in single-stack IPv6 mode.	Will be fixed in future release.

Limitations and/or Dependencies

Feature	AP Model	Limitations and/or Dependencies
WCF	All	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 5. If the mobile device has already cached the DNS for the corresponding URL, the WCF functionality will not take effect. 6. WCF Feature is not supported when WLAN Client enabled secure DNS (DoT or DoH).
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.
Mesh	All	Multicast to unicast is not supported in Mesh mode.
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.
Management VLAN Static IP LACP	AP1351/AP1451	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 cannot connect to Stellar AP running this new build, upgrade SSH client version will avoid this problem.
ALEISSUE-1343/ALEISSUE-2104	AP1201H(L/AP1201/AP1231)	VLAN 4090-4094 is not allowed configured.
11K	Aps without scan radio	To make sure 11k function work as expected, we should configure the AP background scanning on “Working Channel and Non-working Channel”.
Client Isolation	All	1. Client A connect to WLAN1 with ARP1, and Client B connect to WLAN2 with ARP2, in this case, If Client A and B needs to communicate to each other, both of the two clients need to be added into whitelist, either one of Clients add into whitelist can’t ensure communication between these two clients. 2. In case of Express moe, configure WLAN using internal portal + external MAC authentication, client isolation will not work, suggest using internal or external portal authentication only.
Express mode WLAN number	All	Starting with AWOS 4.0.5 in Express mode, we can create 15 user SSIDs on clusters with following models. • AP1301H, AP132x, AP1331, AP136x, AP1351 & AP1451, AP1511, AP1521, AP1561, AP157x, AP154x If a cluster has any of the following models, limit remains at 7 user SSIDs. • AP1501, AP1311, AP1301, AP12xx and AP1101
ALEISSUE-1367	All	OV IP was not supposed to be included in the local breakout IP range.
RAP wired downlink port	All Stellar AP with downlink wired port.	1. Trust tag VLAN ID should not be same as Mac VLAN ID. 2. After enabled trust tag, should not use VLAN0. 3. Don’t support authentication and policy rules.
Certificate management	All	In express mode, the password of the certificate does not support special characters.
WPA3+11r	All	Some clients do not support WPA3+11r.
Enhanced Open Transition Mode	All	Mobile devices with Android OS connect to Enhanced Open Transition Mode WLAN, sometimes it connects to Open WLAN and sometimes it connects to OWE WLAN and some Andriod OS or Windows 10 device can’t connect to Enhanced Open WLAN, When the issue happens AP works as expected broadcasting beacons with related Transition mode info IE. It is suggested to upgrade mobile devices to latest software version.
802.1x	All	AP doesn't support CoA messages in case of 802.1x authentication.
Wi-Fi 7 MLO	Wi-Fi7 APs	Clients that support Wi-Fi 7 MLO features may not be able to access the MLO 6G radio configured on Wi-Fi7 AP due to compatibility issues.
Wi-Fi 7 MLO	Wi-Fi7 APs	WPA3 encryption is required for WLAN configured with MLO.
Wi-Fi 7 MLO	Wi-Fi7 APs	Enhanced Open (Transition Mode) WLAN does not support MLO configuration.
Second Radius Server	All	The current logic of switching from backup server to primary server has issues with adapting to RadSec scenarios.

Wired Port	All Stellar AP with downlink wired port.	The scenario where the AP wired downstream port is connected to a switch and the switch is connected to a wired PC is currently not supported, which will cause the 1x authentication of the PC under the switch to fail.
BLE	All Stellar AP with BLE chip	When the Discover all Devices/iBeamonRawData configuration is issued to an old version AP, it may result in no scan data reporting due to the AP's inability to parse the configuration.
Dynamic VLAN	ALL	Client does not apply dynamic VLAN ID after connecting to WLAN in some scenarios.
WCF	ALL	UCC service exception or delayed WCF response can prevent clients from accessing web pages due to DNS resolution failure.
AP Bridge	ALL	The Stellar AP Bridge Mode—both PTP (Point-to-Point) and PTMP (Point-to-Multipoint)—is supported in Express Mode, OmniVista 2500, and OmniVista Cirrus 10. However, it is not supported in OmniVista Cirrus 4. The Bridge PTMP feature will be introduced in OmniVista Cirrus 10 version 10.5.1. It has not been available in any of the previous OVC 10 releases, where only the PTP Bridge Mode was supported.
WPA3 backward	Wi-Fi7 AP	When the "WPA3 backward" function is enabled for WLAN, the 11r roaming of clients may fail if they use different types of encryptions.
AP Bridge	ALL	Before configuring to AP Bridge mode, need to clear the "save to running" configuration.
Power consumption	Wi-Fi6/Wi-Fi7 AP	To use the Power Consumption wired port speed limit function, it is necessary to ensure that the speed configurations of the switch and the AP are consistent.
LDAP	ALL	Avoid using double quotes in LDAP parameter values.
RAP	ALL	The RAP environment does not support RadSec feature
MLO	Wi-Fi7 AP	Do not turn off the EHT function when the MLO interface is enabled.
SFP	AP1570 series	The AP1570 series electrical/SFP port mode is determined at power-on and cannot be dynamically switched after startup. If no SFP module is inserted during power-on, the system defaults to electrical port mode (electrical port for power supply only). Inserting an SFP module after startup will not switch the port to SFP mode. Please insert the SFP module before power-on to ensure proper SFP port operation.
LACP	AP1230 series, AP1301, AP1311, and AP1320 series	AP1230 series, AP1301, AP1311, and AP1320 series do not support simultaneous power supply through two ethernet ports. If the switch is restarted, it will cause the AP to fail to power on. It is necessary to ensure that the POE power supply of one of the ethernet ports is turned off on the switch side.
160M bandwidth	AP145x	When the AP operates in low-power mode, it only supports 2×2 operation and cannot use a 160 MHz channel bandwidth.
TOS mapping	ALL	The TOS mapping over GRE feature only supports untagged VLAN traffic at present.

New Software Feature Descriptions

CoA and DM support 802.1x and MAC auth

This release extends the Change of Authorization (CoA) and Disconnect Message (DM) capabilities. In prior releases, CoA and DM were only supported for portal authentication. This update enables full CoA and DM support for both 802.1X authentication and MAC address authentication.

This enhancement allows administrators to remotely perform real-time access control actions such as active session termination, user logout, and dynamic authorization adjustment for 802.1X and MAC-authenticated wired and wireless clients. It unifies dynamic policy management across portal, 802.1X, and MAC authentication scenarios, greatly improving post-authentication security enforcement and network management flexibility.

Support RAP registration to OVTX platform

The RAP establishes connectivity and registers to the OVTX platform via callhome communication with the AS. When the RAP initiates certificate-based callhome communication to the OVC AS, the response returned by the OVC AS indicates OVTX as the management platform. Upon receiving this indication, the RAP shall automatically apply registration configurations, switch itself to OVNG mode, restart callhome attempts toward the new OVTX AS, and ultimately complete registration with the OVTX platform.

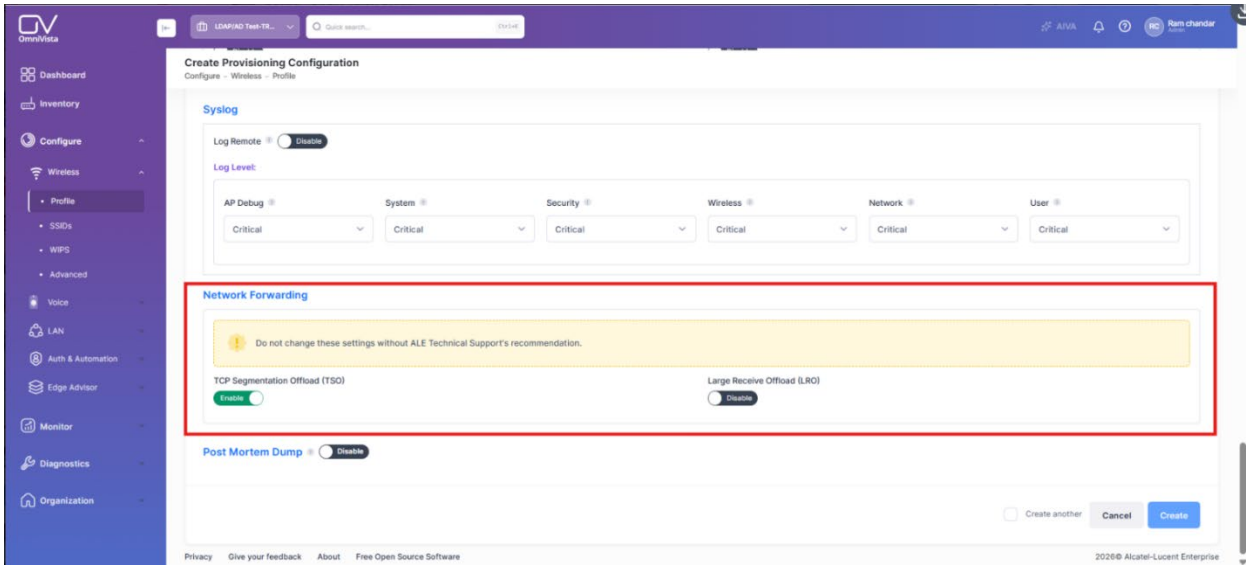
Support TSO Enable / Disable on OVNG

Support TSO enable/disable toggle on APs.

TSO defaults to Enabled and can be configured independently under Network Forwarding.

Note: Cluster/OVC can enable or disable TSO using the tech_support_command:

tech_support_command 37 guest_tunnel_option tos_status <enable | disable>



Disable 6G radio by default for Wi-Fi 7 RW series outdoor models or indoor models with external antennas

Due to regional regulatory restrictions, the 6GHz radio is disabled by default on partial devices (AP1570-RW & AP1561-RW & AP1542-RW). You may enable the 6GHz radio via “AP Configuration Update” or “CLI” commands only after confirming full compliance with local radio spectrum regulations.

Technical Support

Alcatel-Lucent 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

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 2024 ALE International, ALE USA Inc. All rights reserved in all countries.