

Release Notes

OmniAccess Stellar AP

AWOS Release 5.0.3 GA - Release

These release notes accompany the OmniAccess Stellar Operating System (AWOS) Release 5.0.3GA 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
Supported Mode	4
New Software Features and Enhancements	4
Fixed Problem Reports Between Build 5.0.2.2035 and 5.0.3.13	4
Fixed Problem Reports Between Build 5.0.2.1023 and 5.0.2.2035	5
Fixed Problem Reports Between Build 5.0.2.11 and 5.0.2.1023	6
Fixed Problem Reports Between Build 5.0.1.1066 and 5.0.2.11	8
Fixed Problem Reports Between Build 5.0.1.27 and 5.0.1.1066	10
Fixed Problem Reports Between Build 4.0.7MR6 and 5.0.1.27	11
Open/Known Problems.....	13
Limitations and/or Dependencies.....	16
New Software Feature Descriptions.....	19
Technical Support.....	21

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, AP1451, AP1431, AP1411, AP1511, AP1521, AP1311BG.

Supported Mode

- The AWOS 5.0.3.13 is applicable for Express mode and OmniVista Cirrus 10.

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
Ethernet-over-USB	WiFi6 and WiFi7 APs
MACsec	AP1320 Series, AP1360 Series
Power consumption	WiFi6 and WiFi7 APs

Fixed Problem Reports Between Build 5.0.2.2035 and 5.0.3.13

PR	Description
ALEISSUE-2133	Summary: AP1321 stops forwarding GTTS traffics. Explanation: Fix the issue where GTTS stops working when the device's IP address changes. Click for additional information
ALEISSUE-2161	Summary: Client RSSI showing -2dBm in OV2500. Explanation: Fix the RSSI display issue. Click for additional information
ALEISSUE-2175/ ALEISSUE-2178/ ALEISSUE-2192/ALEISSUE-2172	Summary: Stellar AP managed by OVNG have issues with CCI LDAP Query in BYOD Setup. Explanation: Fix the issue where LDAP does not work in certain scenarios. Click for additional information
ALEISSUE-2184 Case number: 00816975	Summary: LLDP location disappears once changing friendly name. Explanation: Fix the issue where the LLDP location missing. Click for additional information

ALEISSUE-2193	Summary: AP1521 on UNP port fails to get the correct IP. Explanation: Fix the issue where LLDP is not sent in a timely manner when the AP starts up. Click for additional information
ALEISSUE-2196	Summary: Wrong EIRP display in OVC10. Explanation: Fix the issue where the txpower not include gain value. Click for additional information

Fixed Problem Reports Between Build 5.0.2.1023 and 5.0.2.2035

PR	Description
ALEISSUE-2017 Case number: 00788118	Summary: It takes more than 100ms sometimes during 802.11r roaming. Explanation: Optimization has been made to accept second auth request from a known client. Click for additional information
ALEISSUE-2111 Case number: 00802956	Summary: OAW-AP1360-ME U-NII-3 max power need to change. Explanation: Modify the maximum power for IL. Click for additional information
ALEISSUE-2129 Case number: 00808834	Summary: Query regarding roaming context log message in AP syslog. Explanation: Fix the problem of incorrect log display. Click for additional information
ALEISSUE-2137 Case number: 00811442	Summary: Option to check the sta count if its more than 1000. Explanation: Fix the problem of incorrect log display. Click for additional information
ALEISSUE-2145 Case number: 00813164	Summary: AP Model name missing from LLDP for AP1511. Explanation: Fix the issue that LLDP does not carry the AP model name.

	Click for additional information
ALEISSUE-2166 Case number: 00816446	Summary: Stellar AP1361D: Bridge mode not working in 5.0.1/5.0.2 versions. Explanation: Fixed the problem that the wireless bridge could not be used. Click for additional information
ALEISSUE-2177 Case number: 00820832	Summary: AP1511: APs rebooted due to kernel panic. Explanation: Fix kernel panic issue. Click for additional information
ALEISSUE-2182 Case number: 00811644	Summary: Clarification on Null point in wam log. “ERROR: NULL Pointer ap_get_ft_ds_ml_sta:131” Explanation: Remove unnecessary logs. Click for additional information
ALEISSUE-2189 Case number: 00820257	Summary: AWOS 5.0.2.11 Upgrade Causes Blank "Upgrade All Firmware" Page. Explanation: Fix the AP web https redirection issue. Click for additional information

Fixed Problem Reports Between Build 5.0.2.11 and 5.0.2.1023

PR	Description
ALEISSUE-2105/ ALEISSUE-2144 Case number: 00796681	Summary: Client not able to connect SSID,when Load balance is enabled. Explanation: The load balancing function incorrectly rejected the Probe request, resulting in the inability of users to access the WLAN with a hidden SSID in some scenarios. Click for additional information
ALEISSUE-2124 Case number: 00807210	Summary: Stellar AP1521 wam module issue. Explanation: Support disable DTLs via AP configuration update. Click for additional information
ALEISSUE-2131 Case number:	Summary: APs Not Responding on SNMP Port 161.

00807867	Explanation: Fix the problem of the SNMP process abnormally exiting in some scenarios. Click for additional information
CVE-2025-52687	Summary: Java Script injection vulnerability in the OmniAccess Stellar web management interface. Incorrect checking of the text field in payloads that are input through the WebUI of the OmniAccess Stellar Access Point allows an attacker with administrator credentials for the access point to improperly inject Java script in the payload of web traffic. Severity: Low Express mode: Impacted. No workaround. Enterprise mode (OVC4, OVC10, OV2500): Impacted. Workaround: Manage OmniAccess Stellar AP with OmniVista management platform and disable web interface access on the OmniAccess Stellar AP. Explanation: Fixed related vulnerability.
CVE-2025-52687	Summary: Command injection vulnerabilities in the OmniAccess Stellar web management interface. The web management interface of the OmniAccess Stellar AP contains multiple vulnerabilities that allow improper command injections. Weakness in the processing of JSON methods submitted using the web interface allows an attacker to inject commands that are executed with root privilege on the access point. Severity: Critical Express mode: Impacted. No workaround. Enterprise mode (OVC4, OVC10, OV2500): Impacted. Workaround: Manage OmniAccess Stellar AP with OmniVista management platform and disable web interface access on the OmniAccess Stellar AP. Explanation: Fixed related vulnerability.
CVE-2025-52689	Summary: Weak session ID check in the OmniAccess Stellar web management interface. The web management interface of the OmniAccess Stellar AP uses a hard coded key to generate the API signature. This vulnerability could allow an attacker to craft a payload such that “/api/login” accepts the spoofed login request and returns a valid session ID with administrator privilege even though the attacker does not know the network administrator credentials. Severity: Critical Express mode: Impacted. No workaround. Enterprise mode (OVC4, OVC10, OV2500): Impacted. Workaround: Manage OmniAccess Stellar AP with OmniVista management platform and disable web interface access on the OmniAccess Stellar AP. Explanation: Fixed related vulnerability.
CVE-2025-52690	Summary: Command injection vulnerabilities in the OmniAccess Stellar over UDP service. Improper checking of the packets received on the AP cluster interface causes the AP to be vulnerable to command injection attacks. Severity: High Express mode: Impacted. No workaround. Enterprise mode (OVC4, OVC10, OV2500): Not Impacted. Explanation: Fixed related vulnerability.

Fixed Problem Reports Between Build 5.0.1.1066 and 5.0.2.11

PR	Description
ALEISSUE-1908 Case number: 00761695	Summary: CVE-1999-0524 detected on AP-1322. Explanation: Fix related vulnerabilities. Click for additional information
ALEISSUE-1923/ ALEISSUE-1962 Case number: 00766306	Summary: AP reboot caused by exception : BUG: soft lockup / Exception stack(0xc9a89cb8 to 0xc9a89d00). Explanation: Disable the CPU core binding feature of the WAM module for the problematic APs to ensure the WAM can utilize all available CPUs. Click for additional information
ALEISSUE-2027 Case number: 00786703	Summary: Clients not able to join Wi-Fi network WPA3 PSK. Explanation: Actively locates and installs the corresponding PMK cache for the client during the four-way handshake negotiation. Click for additional information
ALEISSUE-2031 Case number: 00789108	Summary: Clients receiving duplicate open SSIDs. Explanation: Optimize the check script of the WAM module to ensure it actively restores normal operation upon detecting any WAM anomalies. Click for additional information
ALEISSUE-2053 Case number: 00792644	Summary: RAPs (managed OVNG) not sending authentication request to clear pass server. Explanation: Add support for the OVNG mode in the scripts related to the RAP external server. Click for additional information
ALEISSUE-2056 Case number: 00793872	Summary: OAW-Stellar Access point: Captive portal user not getting the valid certificate even after upgrading the AP. Explanation: Fix the full FQDN not working in Walled Garden. Click for additional information
ALEISSUE-2058 Case number: 00791888	Summary: PMK Hospital-Clients not having internet access. Explanation:

	Continuously monitor the status of the Netfilter queue and actively restore it if a stuck condition is detected. Click for additional information
ALEISSUE-2063 Case number: 00794213	Summary: RAP 1301H / 1201H EAP-TLS no longer works after upgrading to 5.0.1 Explanation: Enabling the Local Breakout feature automatically activates the Layer 3 forwarding functionality. Click for additional information
ALEISSUE-2082 Case number: 00795113	Summary: Client traffic to a whitelist MAC with isolation enabled stops suddenly. Explanation: Enhance the ARP configuration loading process by adding the parsing and loading of the white MAC configuration after the Policy restarts. Click for additional information
ALEISSUE-2083 Case number: 00797475	Summary: SR#00797475: Lev03_Northern America_56: OMNIACCESS Stellar WLAN: SSH sessions to Stellar Aps using putty no longer works. Explanation: Resolve compatibility issues between the new version of putty and the current version of dropbear. Click for additional information
ALEISSUE-2096 Case number: 00799807	Summary: AP1301H send IPv6 packets before LLDP that causes UNP issue. Explanation: Optimize the initiation timing of IPv6 to ensure it activates after the LLDP service has commenced operation. Click for additional information
ALEISSUE-2098 Case number: 00799317	Summary: AP blinking Red LED after upgrade to 5.0.1.27. Explanation: Optimize the detection and determination of power modes to prevent rendering the AP unavailable due to incorrect judgments. Click for additional information
ALEISSUE-2100 Case number: 00799820	Summary: OV Cirrus: AP reboot randomly and not connecting to OVC. Explanation: Disable the client abnormal connection detection script by default; enable it via AP configuration update tool (Extended Configuration Channel). Click for additional information

Fixed Problem Reports Between Build 5.0.1.27 and 5.0.1.1066

PR	Description
ALEISSUE-1959 Case number: 00772579	Summary: Les Tournels severals remote AP are down with reason 15, until reboot of Root AP, RSSI is 28. Explanation: Add workaround for 11AX devices to ensure that AP can be restored to normal in case of interface abnormalities. Click for additional information
ALEISSUE-1969 Case number: 00772486	Summary: Hidden SSID feature not working when Out-of-band Discovery feature of 6G is enabled. Explanation: Do not respond to probe request frames for hidden WLANs in this situation to prevent clients from seeing hidden WLANs. Click for additional information
ALEISSUE-1985 Case number: 00770117	Summary: AP-1321 with Static IP onboard on OVC with a delay more than 30 minutes after reboot. Explanation: AP will actively detect the results of callhome and re execute callhome in case of failure, when it detects that the WAN port has been set to a static IP. Click for additional information
ALEISSUE-1986 Case number: 00774425	Summary: Day light saving not getting updated automatically for summertime. Explanation: Adapt to the correct daylight-saving time. Click for additional information
ALEISSUE-1996 Case number: 00780850	Summary: Brazilian Flag Displayed for Portuguese language on Stellar Express Captive Portal. Explanation: Display the Portugal flag on Stellar Express Captive Portal when selecting Portuguese language. Click for additional information
ALEISSUE-1999 Case number: 00773929	Summary: Long roaming time when 802.11r is Enabled for clients with Static IP. Explanation: Advance the calculation time point of PMK for 11r to ensure that the terminal devices for 11r will now receive regular synchronization messages. Click for additional information
ALEISSUE-2013 Case number: 00792008	Summary: Syslog Log message for failed SSH/Web GUI access. Explanation: Add error message for SSH/Web GUI access failure.

	Click for additional information
ALEISSUE-2025 Case number: 00785422	Summary: Stellar External captive portal no longer working after upgrade to 5.0.1. Explanation: Reopen port 8080 but close fastcgi to prevent customers from accessing the APUI page. Click for additional information
ALEISSUE-2045 Case number: 00791556	Summary: EIRP on AP1511 is well above the legal limit for FCC. Explanation: Fix has been included to follow the regulatory standards.

Fixed Problem Reports Between Build 4.0.7MR6 and 5.0.1.27

PR	Description
ALEISSUE-1773 Case number: 00729492	Summary: The WIPS functionality is not performing as expected with the Stellar AP. Explanation: 1. Change the WIPS suppression message interval to 1 second 2. Simulate bidirectional sending of disassociation request messages Click for additional information
ALEISSUE-1798 Case number: 00658943	Summary: AP1101 rebooted due to kernel panic Kernel panic - not syncing: Fatal exception in interrupt. Explanation: Chipset vendor provides two patches for wireless driver to solve this problem. Click for additional information
ALEISSUE-1854 Case number: 00744752	Summary: Certificate-based authentication (EAP-TLS) fails. Explanation: Modify gso-size to ensure that UDP packets can be properly fragmented and forwarded through the GRE tunnel. Click for additional information
ALEISSUE-1956 Case number: 00770918	Summary: Stellar AP1361: eth1 and SFP interface not visible on GUI. Explanation: Add eth1 and eth2 interface to the default configuration for AP1361. Click for additional information
ALEISSUE-1954 Case number: 00770720	Summary: Request for Remediation of Reported Vulnerabilities (Stellar AP) TCP ports 8883 and 1884. Explanation: Fix related vulnerabilities.

	Click for additional information
ALEISSUE-1964 Case number: 00773223	Summary: Stellar AP1321-1301: After rebooting, the Ap restart in loop Explanation: Remove redundant and non-valuable power supply from lldp module. 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
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.
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 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.
AP1411 Radio Configuration	After switching the radio, the previously unused band is set to a disabled state (Express).	Manually enable the band in AP RF.
SNMPv3	Some special characters can cause SNMP communication issues. The special characters include the following: \$, ", ()	Don't using these special characters.
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.
Mesh	1.If AP working on DFS channel, the client/mesh client can't connect to AP. 2.Create new WLAN on band different from Mesh, will cause reconnect on mesh network.	1.Change the channel to non-DFS channel. 2.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.
Dynamic VLAN	1. When dynamic VLAN is assigned for client, ACL and Client isolation for wired user will not take effect. 2. When client roaming with dynamic VLAN, client IP may not be displayed on UI.	Will be supported in future release.

	3. Kick off iPhone client, and then connect to WLAN with dynamic VLAN, it can't obtain IP address sometimes, it can be recovered by forgetting the network and connect again. No issue on other type of client.	
Enhanced Open	Modify Enhanced Open WLAN to Open, Client can't obtain IP address, this issue happens only on AP1101.	Disable/Enable WLAN. Will be fixed in future release.
Static WEP	Wireless client can still connect to WLAN when configured index value different from the WLAN's index.	Will be fixed in future release.
Wired Client	For devices which supports downlink port, there are issues below: 1. Wired Client will go offline and online when modify Wireless WLAN or Downlink port config. 2. Plug and unplug Wired Client to OAW-AP1301H and move it to other ports of Switches in the same LAN, then plug it back to OAW-AP1301H, will cause FDB learn error in rare cases. Disable and enable the corresponding port can recover.	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 AP1511/AP1521.	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.
Trush 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.
Connectivity	Customers will observe data stall while moving far away from the AP while the station (mainly iPhone 16 series) connecting 5G radio of BE devices.	Will be fixed in future release.
Policy	The WiFi7 device can't configure Layer4 service group.	Will be fixed in future release.
RAP	The WiFi7 device not support RAP.	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.
Romaing	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.
LACP	When the switch is configured for single-port LACP, the aggregation fails probabilistically.	Disable the LACP feature on Switch side.
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.

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.
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	1. AP1201HL switches to a Group with downlink configuration, wired client cannot access it. 2. AP1201HL enables trust tag and option 82, wired client may not obtain IP address.
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	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.
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 / 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.
Link aggregation	AP1351	There is very low probability on AP1351 that ethernet PHY fail to receive messages in the scenario of link aggregation.
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 / 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".

Enhanced Open WLAN	All	Mobile devices with Apple iOS do not support OWE, Mobile devices with Android 10 or later support OWE, Computers with Windows 10 version 2004 or later and a wireless adapter that supports OWE.
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 mode, 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 If a cluster has any of the following models, limit remains at 7 user SSIDs. • 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 connects 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.
Mesh	All	When AP create a new WLAN on MESH AP, the mesh connection will be interrupted briefly.
802.1x	All	AP doesn't support CoA messages in case of 802.1x authentication.
Wi-Fi 7 MLO	AP1511/A P1521	Clients that support Wi-Fi 7 MLO features may not be able to access the MLO 6G radio configured on AP1511/AP1521 due to compatibility issues.
Wi-Fi 7 MLO	AP1511/A P1521	WPA3 encryption is required for WLAN configured with MLO.
Wi-Fi 7 MLO	AP1511/A P1521	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/iBeaconRawData 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.
MESH	ALL	The cluster setup failed due to isolation settings between client APs under root in MESH scenario.
CLUSTER	ALL	The device with 5.0.1.x build cannot join the cluster which PVC is device with build before 5.0.1
WCF	ALL	UCC service exception or delayed WCF response can prevent clients from accessing web pages due to DNS resolution failure.

6G Discovery	WIFI 6E/WIFI 7 AP	Some client not support In-Band discovery, if AP only has 6G WLAN, we recommend configure the 6G channel to a PSC(Preferred Scanning Channel) channel, the PSC channel list includes: 5, 21, 37, 53, 69, 85, 101, 117, 133, 149, 165, 181, 197, 213 and 229.
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	WiFi7 AP	When the "WPA3 backward" function is enabled for WLAN, the 11r roaming of clients may fail if they use different types of encryption.
AP Bridge	ALL	Before configuring to AP Bridge mode, need to clear the "save to running" configuration.
Power consumption	WiFi6/WiFi7 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.

New Software Feature Descriptions

Ethernet-over-USB

Recognize the USB interface as an Ethernet port, creating the needed interfaces and allowing to communicate with the AP internal switch.

Have a software switch to enable/disable USB-over-Ethernet from OmniVista Cirrus 10 and Express mode.

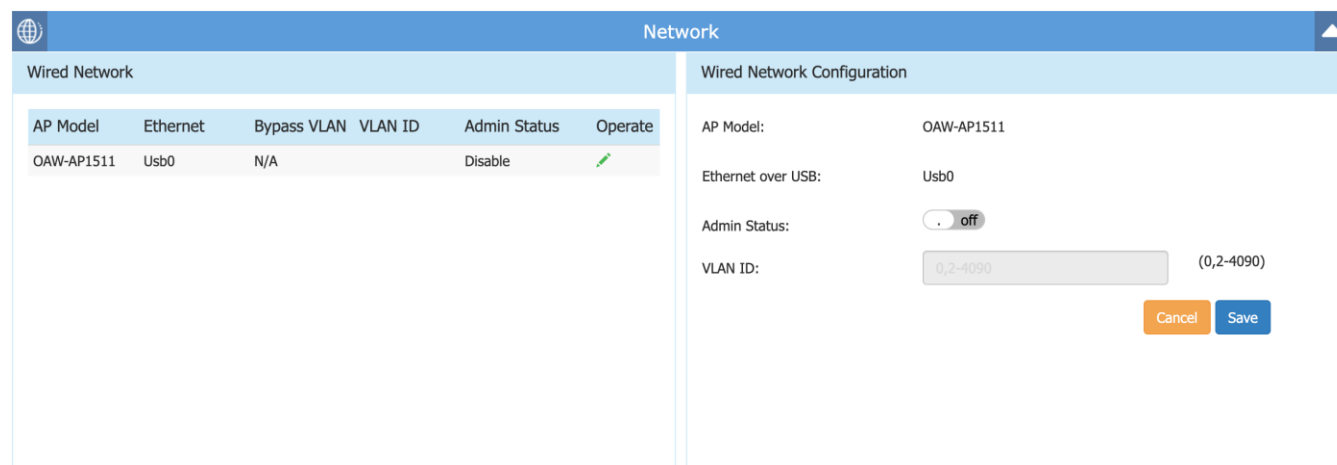
Allow to apply an ARP to the new Ethernet port, including:

VLAN tag, so the traffic from the USB dongle can exit the AP Ethernet port with a tagged VLAN.

ACL/QoS Policy, so the traffic from the USB dongle can be filtered and avoid security issues.

Below is the configuration display:

Express



AP Model	Ethernet	Bypass VLAN	VLAN ID	Admin Status	Operate
OAW-AP1511	Usb0	N/A		Disable	

Wired Network Configuration

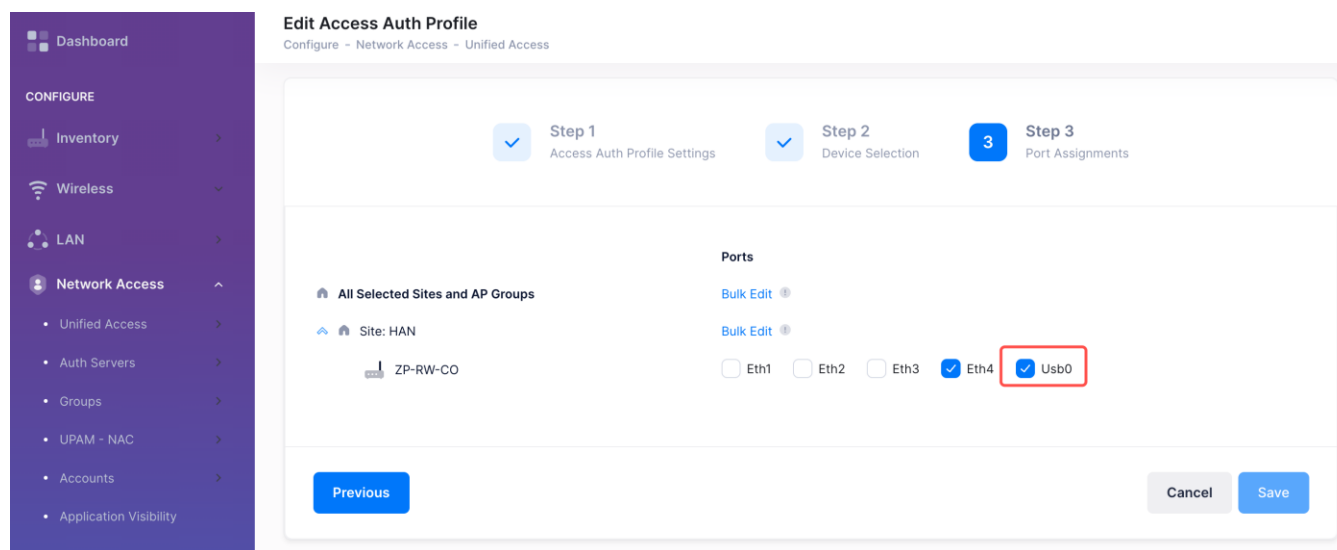
AP Model: OAW-AP1511

Ethernet over USB: Usb0

Admin Status: ☐ off

VLAN ID: (0,2-4090)

OmniVista Cirrus 10



Edit Access Auth Profile
Configure - Network Access - Unified Access

Step 1: Access Auth Profile Settings | Step 2: Device Selection | **Step 3: Port Assignments**

Ports

☐ Eth1 ☐ Eth2 ☐ Eth3 ☒ Eth4 ☒ Usb0

MACsec

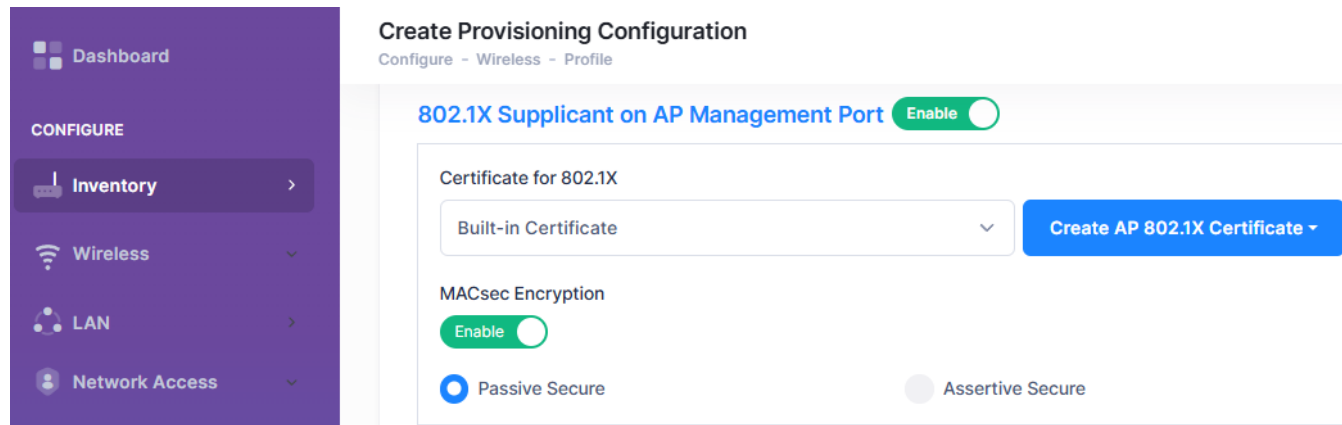
AWOS support MACsec (802.1AE-2018 and 802.1X-2020 for Key management and the establishment of secure associations).

Support for AP1320 Series and AP1360 Series.

Passive Secure: Default selection. MACsec negotiation on Switch decides, else remains open.

Assertive Secure: MACsec encrypted, else remains block.

Below is the configuration display:



Power consumption

AWOS support Power Profiles where the Administrator can adjust the power consumption of the APs:

Allow the AP radio MIMO to move from 4x4:4 -> 3x3:3 -> 2x2:2 -> 1x1:1 for power saving

Allow the AP to disable the USB Host interface

Allow the AP to reduce the wired port speed from 5Gbps -> 2.5Gbps -> 1Gbps

Disable IoT(BLE/Zigbee) Radio

Disable Scanning Radio

Disable one or several Radios in multi-radio APs (for instance, turning off 2,4GHz and 6GHz and keeping 5Ghz active)

The EthernetEEE function is enabled by default and cannot be configured.

Power control for Power Profiles: The administrator can define different timeframes in the week and assign a Power Profile to each time frame.

OWD

Below is the configuration display:

Power Profile						
Power Profile						
Name	Chainmask	Radio OFF	Wired Speed	Operate		
Power-test	2*2	2.4GHz	5Gbps	 		

Power Control						
Power Control						
Name	Calendar	Start Ti...	End Time	Power Profile	Status	Operate
Power-ctr...	Wed,Thu	00:00	24:00	Power-test	enable	 

Power Profile

Name:

Power-test

Chainmask:

2x2:2

Radio OFF:

☒ 2.4GHz

☐ 5GHz

☐ 6GHz

☐ Scanning

Wired Speed:

5Gbps

USB:

off

BLE:

off

Cancel

Save

Power Control

Status:

on

Name:

Power-ctrl-test

Calendar:

☐ Mon

☐ Tue

☒ Wed

☒ Thu

☐ Fri

☐ Sat

☐ Sun

Start Time:

00:00

End Time:

24:00

Power Profile:

Power-test

Cancel

Save

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: ale.welcomecenter@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 2024 ALE International, ALE USA Inc. All rights reserved in all countries.