Release Notes - Rev. A

OmniAccess Stellar AP

AWOS Release 4.0.3 – GA 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.

Table of Contents

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, AP1201H, AP1201L, AP1201HL, AP1320 series, AP1360 series, AP1201BG, AP1301, AP1311, AP1351

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 these release notes:

Feature	Platform Support
Wi-Fi QoE & Analytics (OVE/OVC)	Except AP1101, AP1201H, AP1201HL, AP1201L
AP Support Roaming RSSI Threshold for non-802.11K/V Clients (Express & OVE/OVC)	All
AP Support U-APSD Configuration (Express & OVE/OVC)	All
160MHz channel width support in RF Profile (Express & OVE/OVC)	AP1320 series, AP1360 series, AP1351

Notes:

- OmniAccess Stellar AP reserves two SSIDs (One on 2.4G band, and one on 5G band). They perform background scanning for WIPs/WIDs services to alert and take preventive actions on any security threat. It is secure and NO clients can connect to these SSIDs.

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 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 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 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-1039	**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: 00565590 ALEISSUE-1123	**Summary:** OmniAccess Stellar Clients getting disconnected due to CRC errors in Eth0 of Stellar AP1311. **Explanation:** This issue is related to driver that is updated from release AWOS 4.0.3. Click for additional information
Case: N/A ALEISSUE-909	**Summary:** OmniAccess Stellar WISPr-Session-Terminate-Time support for External Captive Portal. **Explanation:** This field provides times when the user should be disconnected from External Captive Portal.
Case: 00516835 ALEISSUE-913	**Summary:** OmniAccess Stellar Wifi6 APs Multicast/Unicast packets are dropped. **Explanation:** This issue is related to 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
Case: N/A ALEISSUE-909	**Summary:** WISPr-Session-Terminate-Time supporting for external portal use case. **Explanation:** Add new parameter support with external portal, which is when the user should be disconnected; in "YYYY-MM-DDThh:mm:ssTZD" form, where Y - year; M - month; D - day; T - separator symbol (must be written between date and time); h - hour (in 24 hour format); m - minute; s - second; TZD - time zone in one of these forms: "+hh:mm", "+hhmm", "-hh:mm", "-hhmm".
Case: N/A ALEISSUE-1123	**Summary:** Latency and CRC error noticed on AP1311 eth0 Port. **Explanation:** The issue is observed on AWOS 4.0.2 builds on AP1311, there is CRC error and Latency on eth0 port, it is optimized on AWOS 4.0.3 with low level chipset driver.

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-973	Guest users cannot authenticate over Captive Portal when a Proxy Server is enabled.	In current 403 build, HTTP Captive Portal redirection over

	Click for additional information	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.
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.
AP1220 reboot due to out of memory	When unicast traffic is large, AP may cause OOM, due to a sharp drop in available memory, especially for AP with less than 40m of available memory.	Reduce unicast traffic scenarios.
Device type and operate system	The Samsung client terminal device type and system reported by AP are incorrect. Notice: Occasional problem.	Use the client to access the web page for a period of time, and then refresh the display on OV.
LED state abnormal	After AP boot up, the blue light is on after the network is connected, and when network is unreachable due to LACP, the red light begins to flash. After waiting for the network to be connected, the blue light is detected again. Notice: Occasional problem.	Because of the LACP function, this is the normal design logic, and the state of the lamp will be optimized later.

LDAP	Configure on-premise LDAP with special characters for AP, clients to connect to the WLAN, page to prompt authentication failure.	1. Rebind the issued configuration globally. This problem can be solved. 2. Special characters cause, if there are no special characters, there is no problem
Portal authentication	When "/ # /\ / &" exists in the user parameters value of the AD server, and the client connects to WLAN, to launch the portal page, the login jump exception occurs.	Special characters cause, if there are no special characters, there is no problem
Portal authentication	When the authentication source is ldap/ad.portal authentication, AP will send a lot of mac authentication, and portal authentication will not be able to jump to the authentication success page for a long time.	There is no known workaround at this time.
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.
Apple device connection issue on 1320/1360 series	When the VLANID in SSID is modified, all clients will be kicked off, but Apple device may not send DHCP request when reconnecting with this SSID, that will cause to keep using old IP address and unable to connect to the network.	Disconnect and re-join this network with the Apple device.
AP1201H is in downlink bridge mode, and the client cannot get IP when it is associated with tag WLAN.	AP1201H is downlink bridge mode. When the client is associated with tag WLAN, it cannot get IP, that is, AP1201H and other models of AP. Tag bridge mode is not supported.	AP1201H has low performance and is not recommended as a bridge AP.
Short GI	The configuration on the web side of Short-GI does not seem to take effect. In the case of more WLAN, it only takes effect on some WLAN.	There is no known workaround at this time.
Express Login	[Cluster/AP] Downgrade version 4.0.3.x to version 4.0.0.x Actual result: log in to the cluster page after the upgrade is completed, and the password is changed to admin.	Login with default password and reconfigure it.
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	When you manually configure a V6 address of the same network segment on the client as the

	wireless network card of win 7 11n set to single-stack V6, check the network on-off condition of the V6 address.	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.
ARP Proxy	ARP Proxy does not work on 11AX products.	Will be fixed in AWOS 4.0.3 MR1
ALEISSUE-1127	Randomly ACL are no longer working connected users lost connection to services.	Will be fixed in AWOS 4.0.3 MR1
IP info update	AP is configured with DHCP method to obtain IP address, and when IP address changed due to lease time expired, sometimes it does not update on OV AP info list.	The current workaround is reboot AP.
Load Configuration	It takes long time for AP to register on OV when AP is configured with management VLAN and reboot. This happens only on APs which support LACP.	There is no known workaround at this time.
OS upgrade	Occasionally in cluster mode, when upgrade APs through wireless connection with low-end APs such as AP1201H, randomly some APs upgrade failed due to limited resources.	The current workaround is connect with high-end APs or upgrade one more time.
802.11r Roaming	Below scenarios client may fail when roams with 802.11R 1. Load balance takes effect when client roams from one AP to the other. 2. Failed to send MDIE when client roams.	For scenario 2, it will be fixed on AWOS 4.0.3 MR1.
Mesh	Occasionally in mesh network, the leaf node AP connects with more than one other APs.	The issue can disappear when reboot this AP, It will be fixed on AWOS 4.0.3 MR1.
DNS resolution	The issue happens in a fairly low frequency that client DNS request can't response.	The current work around is restart wcf service.
Configuration Restore	In one AP cluster, if PVC's AP model is same with other APs in this cluster, restore all configuration may fail.	There is no known workaround at this time.
Extend config channel	Private config by extend config channel can be overwritten on RF config.	It will be fixed on AWOS 4.0.3 MR1.
RAP	Client sometimes obtains IP address from local DHCP server, which it should obtain IP address from remote site.	It can be solved by client disconnect and connect to the

		SSID. It will be fixed on AWOS 4.0.3 MR1.
LAN configuration	LAN configuration on AP1311 does not take effect in Express mode due to GUI send wrong ports to AP.	It will be fixed on AWOS 4.0.3 MR1.
Dedicated Scanning	When enabling dedicated scanning on an AP1311, after a reboot WLANs will not be created if connected with ETH0. This happens only on an AP1311 when connected to ETH0 port.	The current workaround is to switch the Ethernet connection to ETH1 from ETH0 or disable dedicated scanning. It will be fixed in AWOS 4.0.3 MR1.

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.

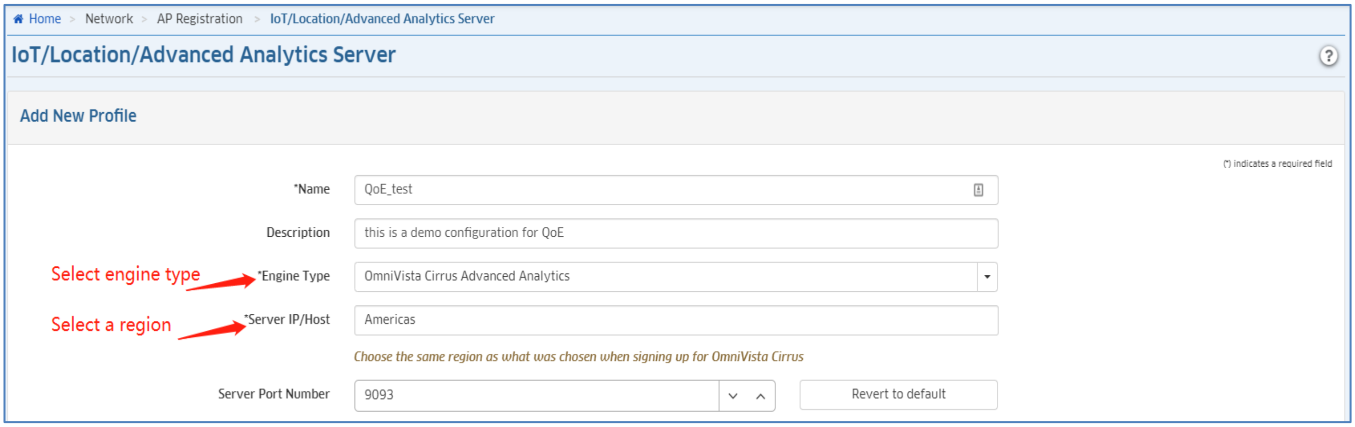
Show device name	All	When some clients connect to wlan, there is no option12 field in the dhcp message, so its hostname cannot be displayed.
DPI	AP1311/AP1301	DPI is not supported on AP1301 & AP1311 products in this release.
Management VLAN Static IP LACP	AP1351	When configure LACP + Management VLAN + 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.
Limited maximum client connection	AP1351	On AP1351 5G-low radio in this release it supports maximum 128 clients connection, it will support maximum 512 clients connection in 4.0.4 release.
High efficiency	AP1351	In Express mode, 5G radio of AP1351 always works in High efficiency mode, there is lack of button to disable it.
ARP Proxy	AP1220 series	APs may reboot due to huge amount of ARP request messages; it is suggested to enable ARP Proxy by default.

New Software Feature Descriptions

Wi-Fi QoE & Analytics

Wi-Fi networks need to be monitored for infrastructure capacity and its usage, associating client types and monitor regularly for interference and rogue. AP is responsible for collecting and reporting events to OVNG, OVNG is responsible for display those data in a user-friend manner, OVE/C is responsible for QoE configuration.

1. Go to OVE/C Home>Network>AP Registration>IoT/Location/Advanced Analytics Server



Home > Network > AP Registration > IoT/Location/Advanced Analytics Server

IoT/Location/Advanced Analytics Server

Add New Profile

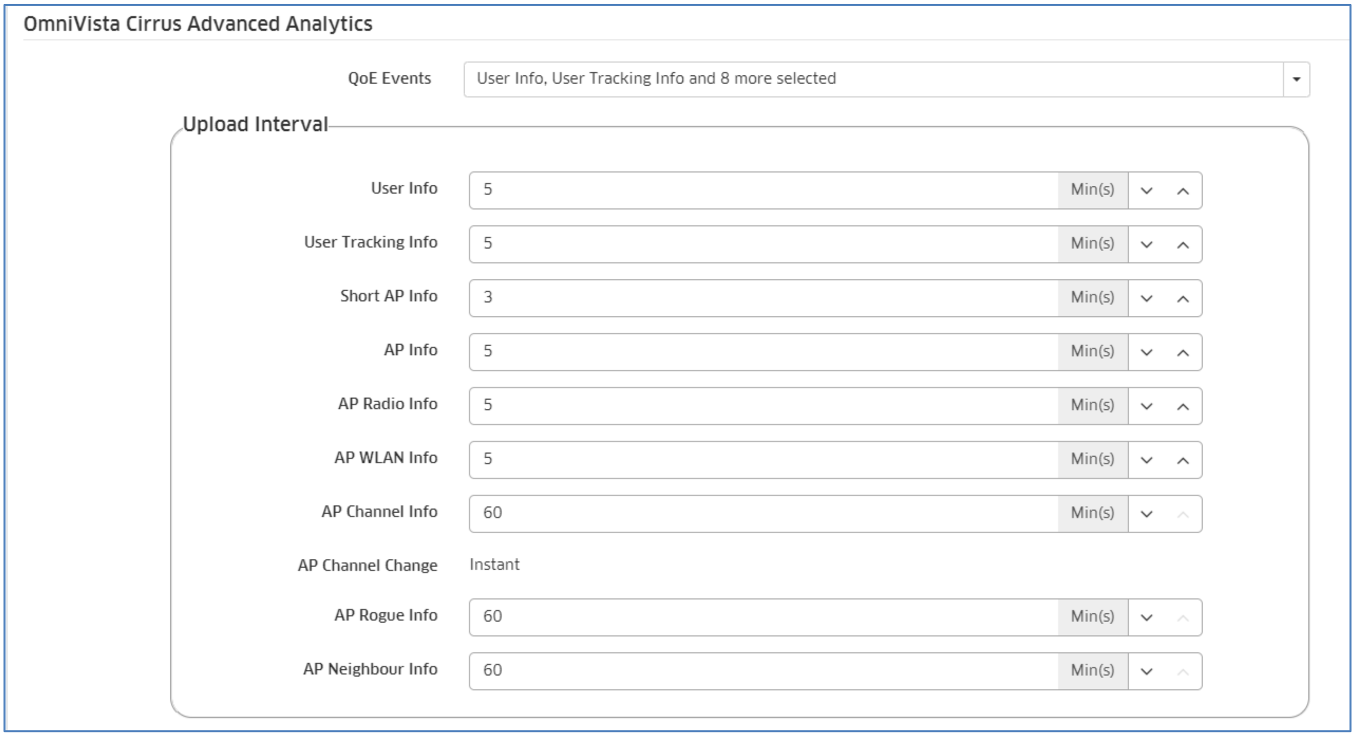
(*) indicates a required field

*Name	QoE_test
Description	this is a demo configuration for QoE
*Engine Type	OmniVista Cirrus Advanced Analytics
*Server IP/Host	Americas
	Choose the same region as what was chosen when signing up for OmniVista Cirrus
Server Port Number	9093

Select engine type

Select a region

2. Following upload interval can be configured, or you can leave with it by default



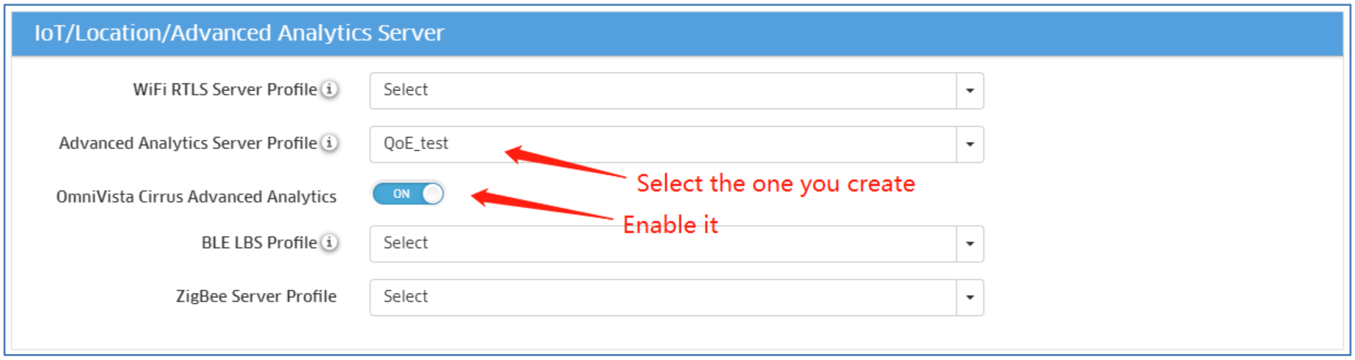
OmniVista Cirrus Advanced Analytics

QoE Events: User Info, User Tracking Info and 8 more selected

Upload Interval

User Info	5 Min(s)
User Tracking Info	5 Min(s)
Short AP Info	3 Min(s)
AP Info	5 Min(s)
AP Radio Info	5 Min(s)
AP WLAN Info	5 Min(s)
AP Channel Info	60 Min(s)
AP Channel Change	Instant
AP Rogue Info	60 Min(s)
AP Neighbour Info	60 Min(s)

3. Go to Home>Network>AP Registration>AP Group, pick one group and edit below, and then apply:



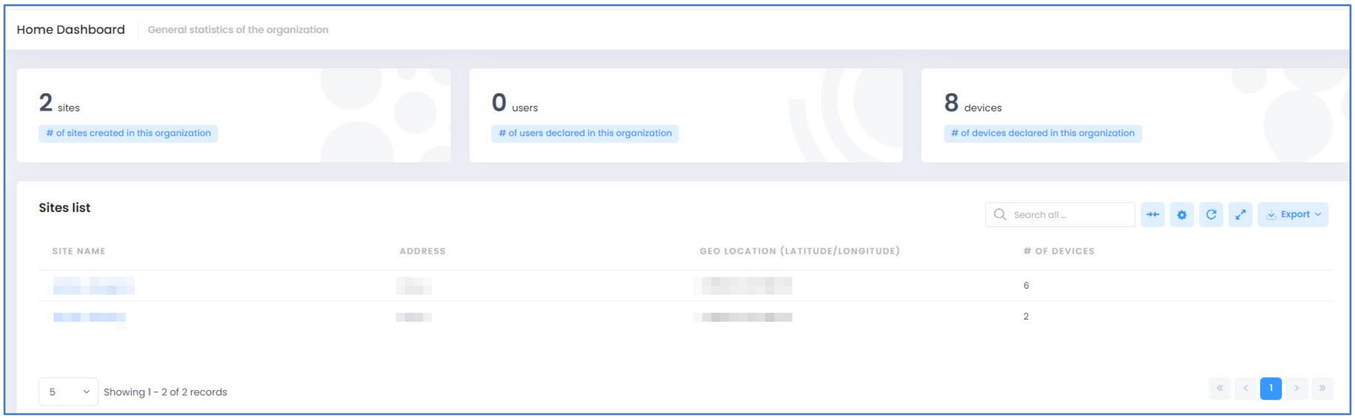
IoT/Location/Advanced Analytics Server

WiFi RTLS Server Profile ⓘ	Select
Advanced Analytics Server Profile ⓘ	QoE_test
OmniVista Cirrus Advanced Analytics	ON
BLE LBS Profile ⓘ	Select
ZigBee Server Profile	Select

Select the one you create

Enable it

4. Go to OVNG website https://preview.manage.ovcirrus.com/ (note: this link is preview ENV, for demonstrate only), the screenshot below shows dashboard of OVNG.



Home Dashboard | General statistics of the organization

2 sites — # of sites created in this organization

0 users — # of users declared in this organization

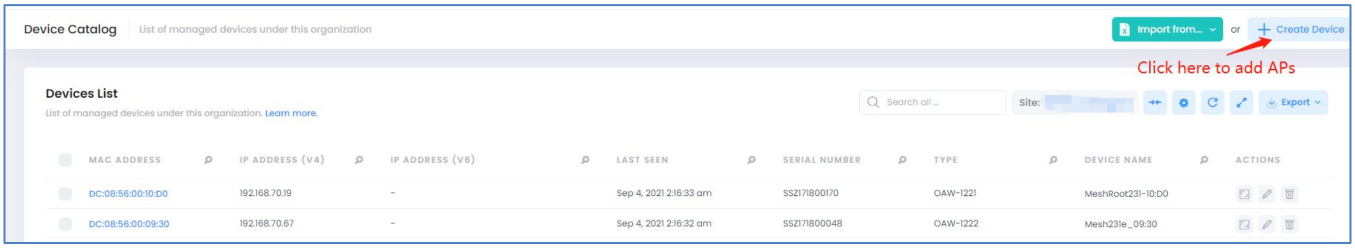
8 devices — # of devices declared in this organization

Sites list

SITE NAME	ADDRESS	GEO LOCATION (LATITUDE/LONGITUDE)	# OF DEVICES
[redacted]	[redacted]	[redacted]	6
[redacted]	[redacted]	[redacted]	2

5 Showing 1 - 2 of 2 records

5. Go to OVNG CONFIGURE -> Network-Wide -> Inventory -> Device Catalog, Add APs which are applied QoE configuration in OVE AP Group.



Device Catalog | List of managed devices under this organization

Click here to add APs

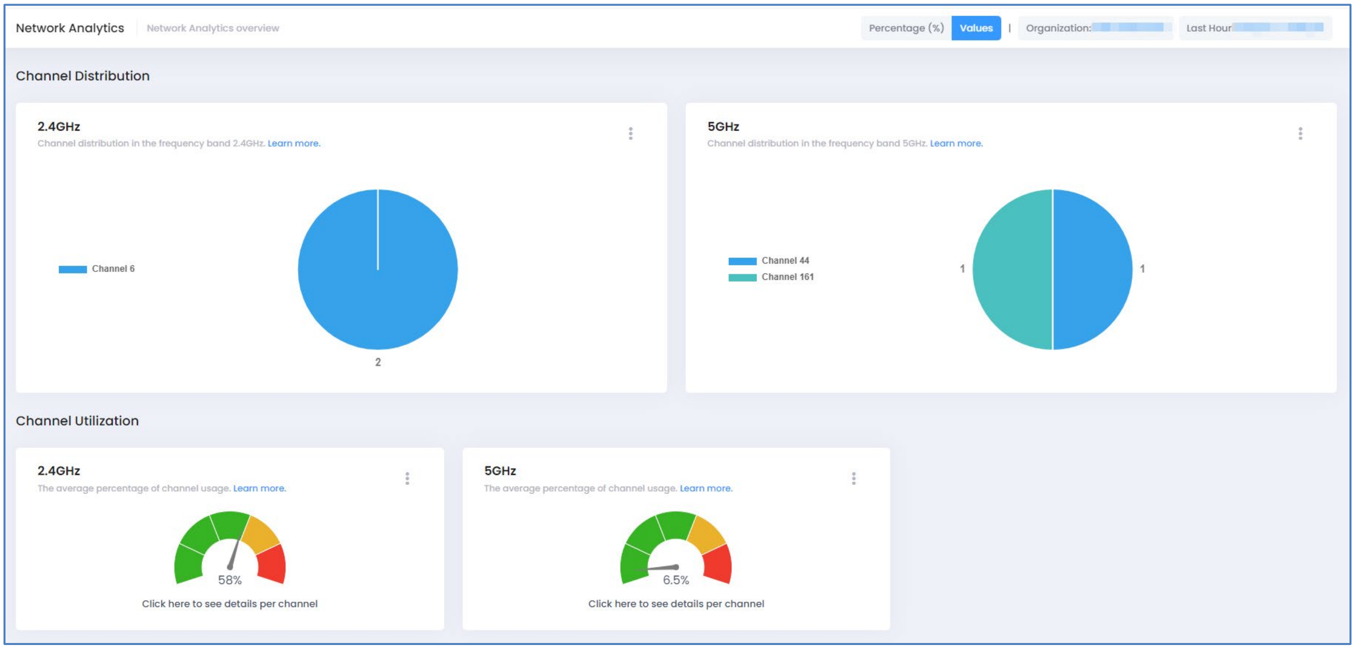
Devices List

List of managed devices under this organization. Learn more.

Site: [redacted]

MAC ADDRESS	IP ADDRESS (V4)	IP ADDRESS (V6)	LAST SEEN	SERIAL NUMBER	TYPE	DEVICE NAME	ACTIONS
DC:08:56:00:10:D0	192.168.70.19	-	Sep 4, 2021 2:16:33 am	SSZ171800170	OAW-1221	MeshRoot231-10:D0	
DC:08:56:00:09:30	192.168.70.67	-	Sep 4, 2021 2:16:32 am	SSZ171800048	OAW-1222	Mesh231e_09:30	

6. Go to OVNG MONITOR -> Network-Wide -> Analytics to check QoE status of APs, here is an example below displays network analytics.



Network Analytics | Network Analytics overview

Percentage (%) | Values | Organization: [redacted] | Last Hour [redacted]

Channel Distribution

2.4GHz

Channel distribution in the frequency band 2.4GHz. Learn more.

5GHz

Channel distribution in the frequency band 5GHz. Learn more.

Channel Utilization

2.4GHz

The average percentage of channel usage. Learn more.

Click here to see details per channel

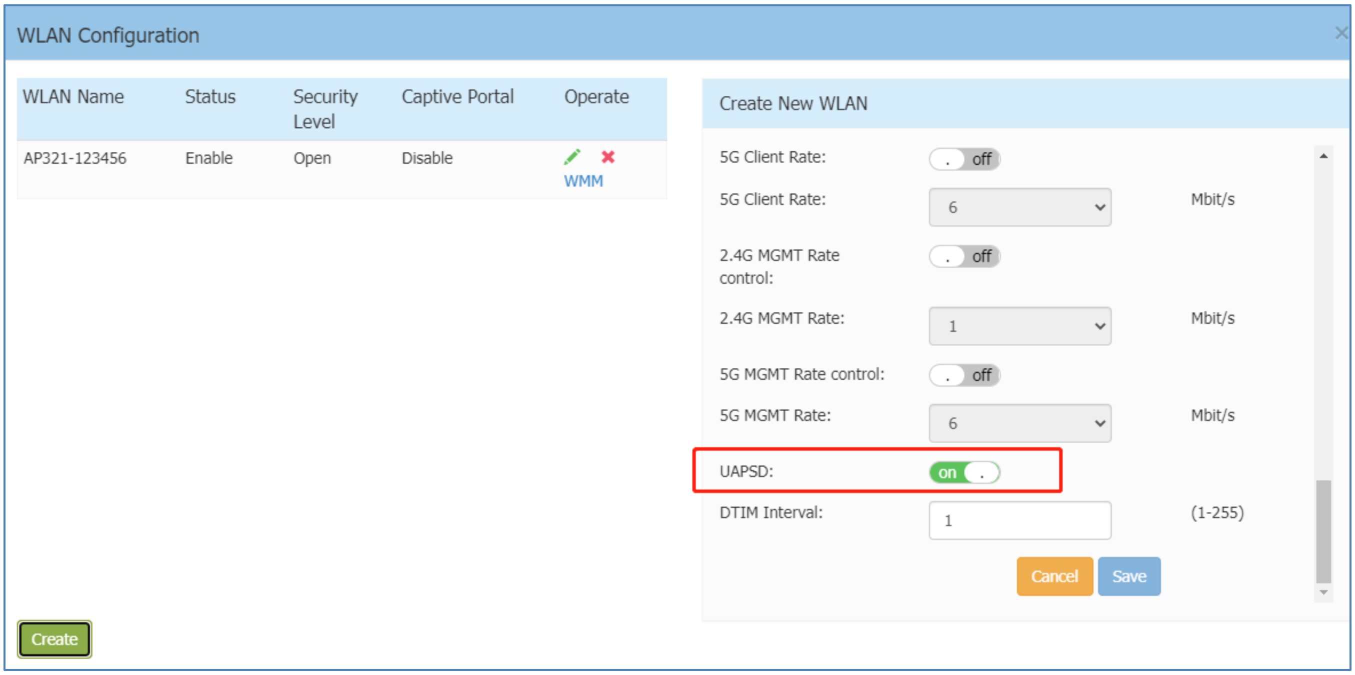
5GHz

The average percentage of channel usage. Learn more.

Click here to see details per channel

AP Support U-APSD Configuration

U-APSD configuration is added on WLAN configuration, please refer to the screenshot below:



WLAN Configuration

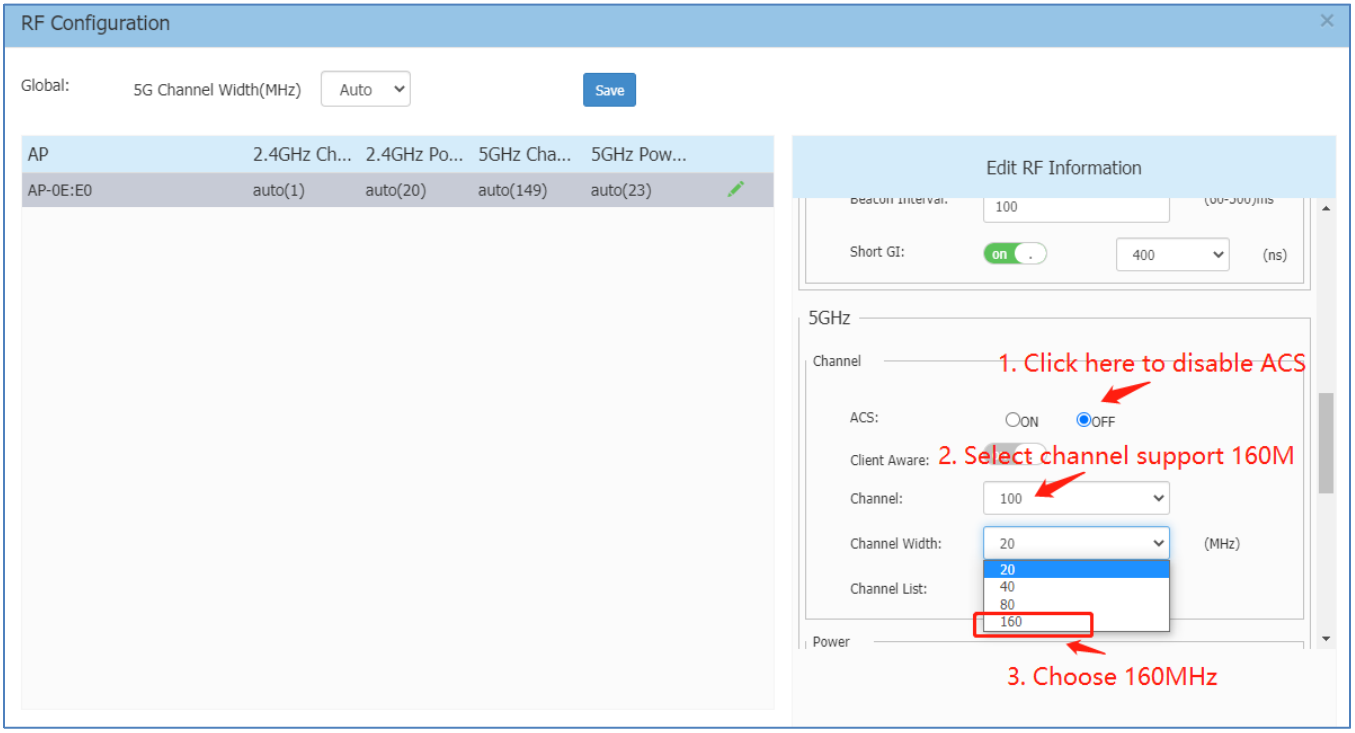
WLAN Name	Status	Security Level	Captive Portal	Operate
AP321-123456	Enable	Open	Disable	WMM

Create New WLAN

5G Client Rate:	off	
5G Client Rate:	6	Mbit/s
2.4G MGMT Rate control:	off	
2.4G MGMT Rate:	1	Mbit/s
5G MGMT Rate control:	off	
5G MGMT Rate:	6	Mbit/s
UAPSD:	on	
DTIM Interval:	1	(1-255)

160MHz channel width support in RF Profile

Go to Wireless -> RF Configuration, then disable ACS and select channel which support 160MHz, and then roll down channel list and choose 160MHz, after that, you can save the configuration.



RF Configuration

Global: 5G Channel Width(MHz) Auto

AP	2.4GHz Ch...	2.4GHz Po...	5GHz Cha...	5GHz Pow...
AP-0E:E0	auto(1)	auto(20)	auto(149)	auto(23)

Edit RF Information

Beacon Interval: 100 (60-300)ms

Short GI: on 400 (ns)

5GHz

Channel

ACS: ○ON ●OFF

Client Aware:

Channel: 100

Channel Width: 20 (MHz)

Channel List:

Power

1. Click here to disable ACS

2. Select channel support 160M

3. Choose 160MHz

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.