Release Notes

OmniAccess Stellar AP

AWOS Release 4.0.5 – GA Release

These release notes accompany the OmniAccess Stellar Operating System (AWOS) Release 4.0.5 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, AP1261-RW-B, AP1201H, AP1201L, AP1201HL, AP1320 series, AP1360 series, AP1201BG, AP1301, AP1301H, AP1311, AP1331, AP1351, AP1451.

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
AP-Name Broadcast in Beacon Frame (Express&OVE&OVC)	All
CSA (802.11h) (Express&OVE&OVC)	All
[PERWIFI-147] SNMPv3 (Express&OVE&OVC)	All
Wi-Fi Enhanced Open (Express&OVE&OVC)	All
GRE tunnel resiliency (Stellar AP -- OmniSwitch) (OVE)	All
Multiple options in DHCP option 82 string (OVE&OVC)	All
Client isolation should additionally allow configuring an Allowlist of MAC address (OVE&OVC)	All
Ability to update certificate for Captive Portal on AP without upgrading them (Express)	All
AP1301H downlink TAG VLAN support (Trust tag & Bypass VLAN)	AP1301H
AP1201H RAP downlink port support applying ARP with VLANs	AP1201H

Fixed Problem Reports Between Build 4.0.5.23 and 4.0.4.7120

PR	Description
Case: N/A ALEISSUE-1057	**Summary:** For best security practice, the admin must change the default password at setup time. **Explanation:** AWOS-4.0.5 provides an optional choice for user to change default password of root and support at setup time under Express mode.
Case: N/A ALEISSUE-1219	**Summary:** AWOS 4.0.4 MR-2 Have a REST-API for downloading Stellar AP snapshot logs by HTTP instead of TFTP. **Explanation:**

	When AP is running Express mode, we can download snapshot logs by REST-API, more details on OmniAccess Stellar AP AWOS 4.0.5 – REST API Definition when running in Express mode
Case: 00609904 ALEISSUE-1261	**Summary:** Vulnerabilities CVE-2020-36254 and CVE-2019-12953 **Explanation**: Vulnerabilities reported on old version of SSH service module, on AWOS-4.0.5 SSH module is upgrade to new version. Click for additional information
Case: 00613146 ALEISSUE-1274	**Summary:** Issue with L2GRE tunnel. **Explanation**: TCPMSS of L2GRE tunnel is fixed with 1400, this could cause large size packets being dropped. On AWOS-4.0.5 TCPMSS of L2GRE tunnel changes according to MTU of L2GRE. Click for additional information
Case: 00619412 ALEISSUE-1281	**Summary:** OpenSSL Vulnerability CVE-2022-0778. **Explanation**: The issue is fixed by upgrading OpenSSL. Click for additional information
Case: 00604830 ALEISSUE-1337	**Summary:** Kafka uploader module doesn't reconnect properly to Kafka broker. **Explanation**: This is fixed by adding connection detect mechanism, if Kafka broker can't be connected for more than 600 seconds, AP will start to connect Kafka broker again. Click for additional information
Case: N/A ALEISSUE-1302	**Summary:** Stellar is announcing AKM suite 00-0f-ac-01 (WPA) and PMF set optional. None of which is allowed in WPA3-Enterprise mode. **Explanation**: AP works on WPA3-Enterprise transition mode but not WPA3-Enterprise only mode when we configure the encription mode as WPA3_AES (in OV mode) or WPA3-Enterprise(in express mode) ,this is why we see Stellar AP announcing AKM suite 00-0f-ac-01 (WPA) and PMF set optional. Starting AWOS 4.0.5 AP supports running WPA3-Enterprise only mode.
Case: 00622182 ALEISSUE-1318	**Summary:** "ApRadioUtilization" and "ApTxpower" information is not retrieved on 802.11ax models **Explanation**: The issue is fixed by using new command to collect channel utilization for 802.11ax devices.
Case: 00620147	**Summary:** WCF not working very frequently on Mobile devices using browser with secured DNS enabled

ALEISSUE-1327	**Explanation**: In AWOS 4.0.5 – WCF is enhanced to support: 1.Client using an IPv6 address 2.Portal authentication scenario：WCF module handles DNS packets before client performs a portal authentication. Click for additional information
Case: 00637466 ALEISSUE-1356	**Summary:** Silent device connected behind the AP1201H is not working **Explanation**: Bypass feature is fixed to support this scenario Click for additional information
Case: 00640251 ALEISSUE-1360	**Summary:** Mac auth with ClearPass Server, no response from IP gateway, when user leaves the AP and returns back. **Explanation**: The issue is fixed by after roaming, client's ARP information and corresponding policy list are both updated. 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
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. Will be fixed on AWOS 4.0.6.
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 on AWOS 4.0.6.
WCF	WCF feature is not supported when WLAN Client is running behind an HTTP Proxy.	There is no known workaround at this time.

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).	There is no known workaround at this time.
DSCP	DSCP downlink direction does not take effect on 5GHz of AP1451.	Will be fixed on AWOS 4.0.6
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-1308	Interface vlan configuration lost when WLAN access timer is configured.	Will be fixed on AWOS 4.0.6
ALEISSUE-1367	Unable to push network in local breakout if it includes OV2500 IP address.	Will be fixed on AWOS 4.0.5 MR1
ALEISSUE-1375	AP's 1311 are generating ACI (Adjacent Channel Interference) when selecting wrong channels in the 2.4Ghz frequency.	Will be fixed on AWOS 4.0.5 MR1
DHCP Server	DHCP Server is not available on AP1231 model.	Will be fixed on AWOS 4.0.5 MR1
RAP	Clients may not be access to network when switching desired AP from Group of RAP to a regular AP Group on 11AX platform devices.	Will be fixed on AWOS 4.0.5 MR1

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
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. 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 /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/AP1451, 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.

ALEISSUE-1358	ALL	Double authentication is supported only when the returned role is the same for each authentication.
ALEISSUE-1343	AP1201H(L)	VLAN 4090-4094 is not allowed configured.
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 Whitelist	All	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.

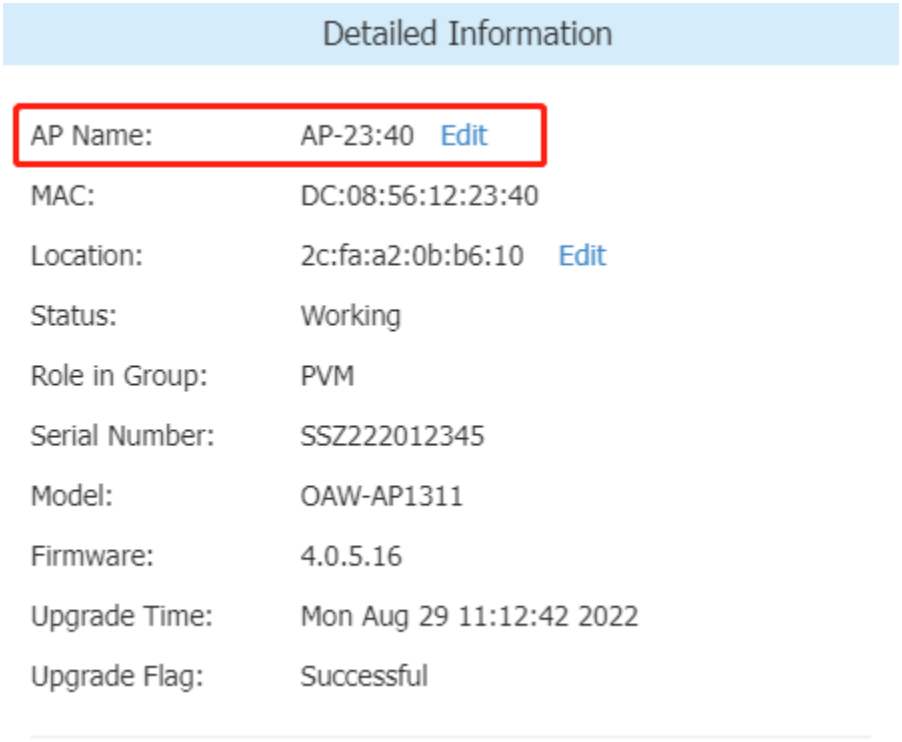
New Software Feature Descriptions

AP-Name Broadcast in Beacon Frame

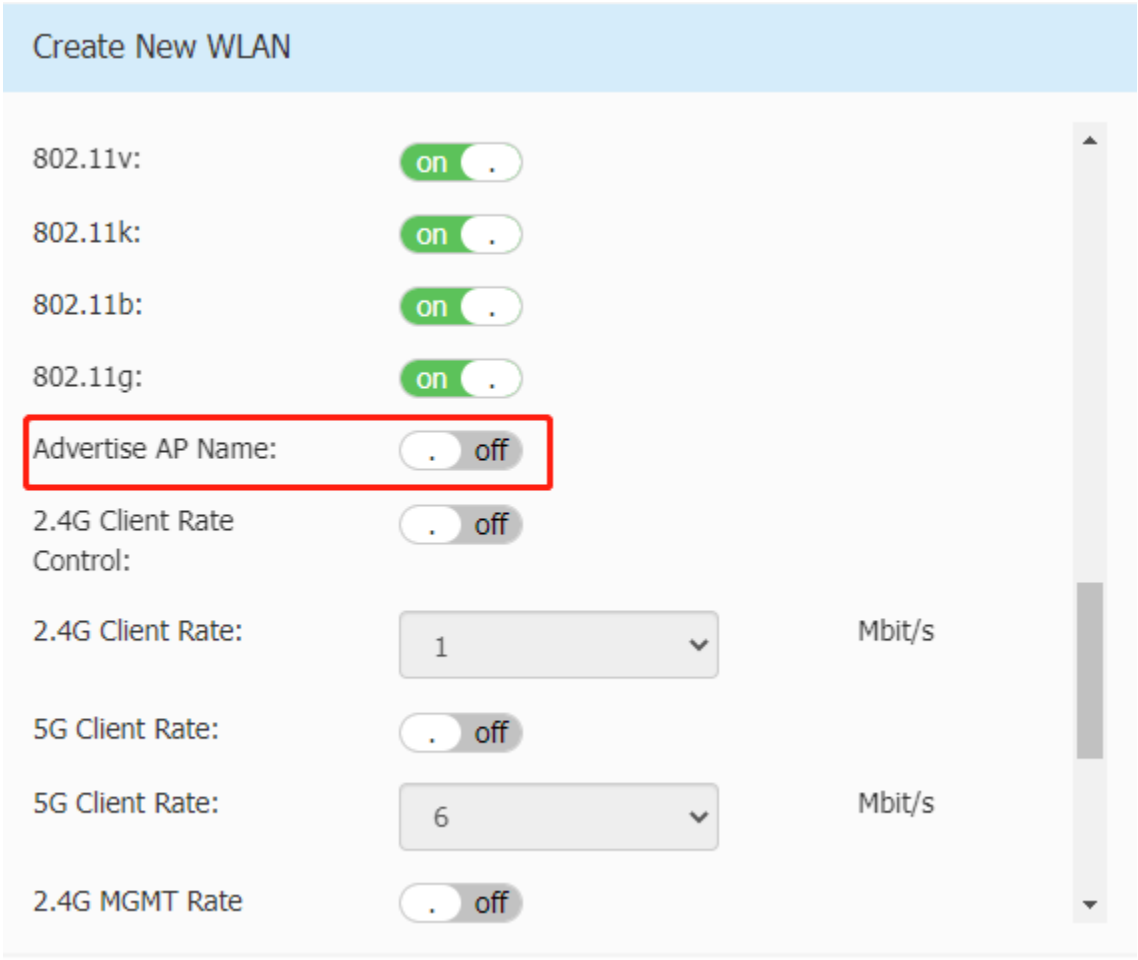
Most of the major vendors (Cisco, Aruba, Extreme and even Lancom etc.) support AP-name broadcast feature as part of the beacon frame. With this the deployment and maintenance become easier. Without this the APs are displayed using MAC address.

Per AP-Group we need a configuration option “Advertise AP Name”, which is disabled by default.
When enabled, the AP Name will be advertised as part of the standard 802.11 beacon frame using vendor specific tag.

1. Go to AP Configuration -> Detailed Information, and find AP Name below, you can change name desired.



2. Go to WLAN -> Create New WLAN, Switch “Advertise AP Name” button to enable this function.

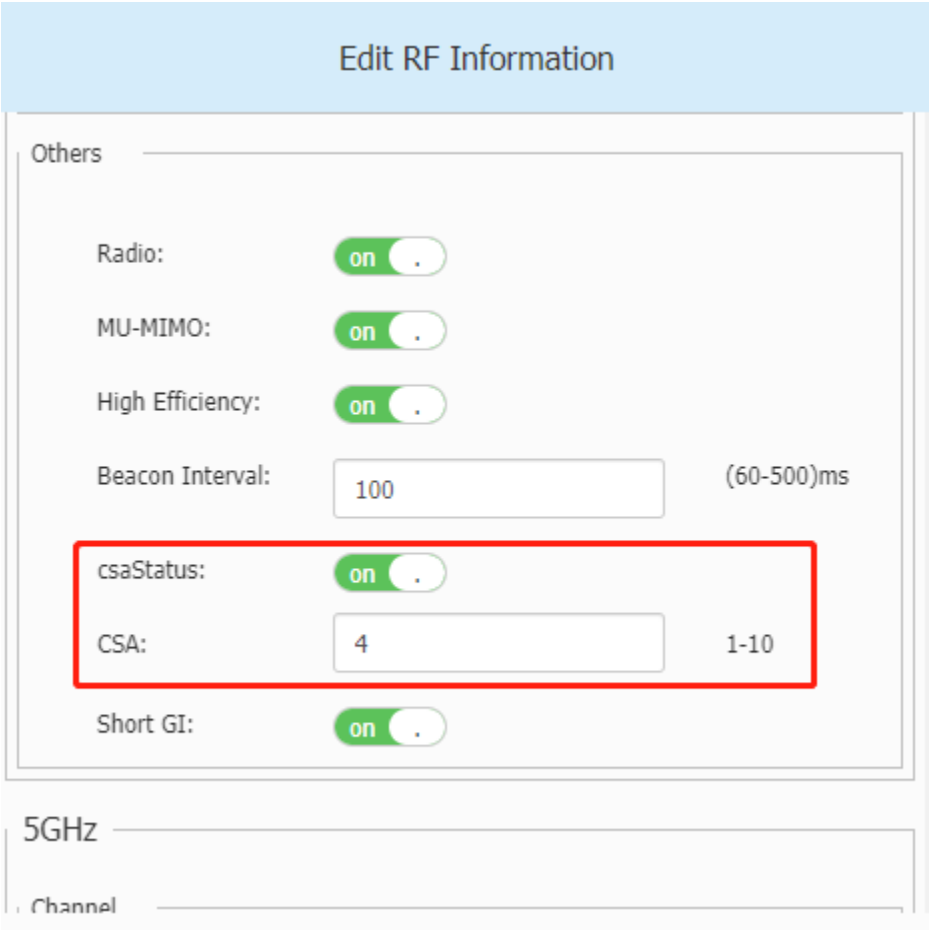


CSA (802.11h)

Channel Switch Announcement (CSA), as defined by IEEE 802.11h, enables an AP to announce that it is switching to a new channel before it begins transmitting on that channel. This allows the clients, who support CSA, to transition to the new channel with very minimal downtime.

- CSA “ON/OFF” (default ON)
- CSA-Count “range 1-10” (default 4)

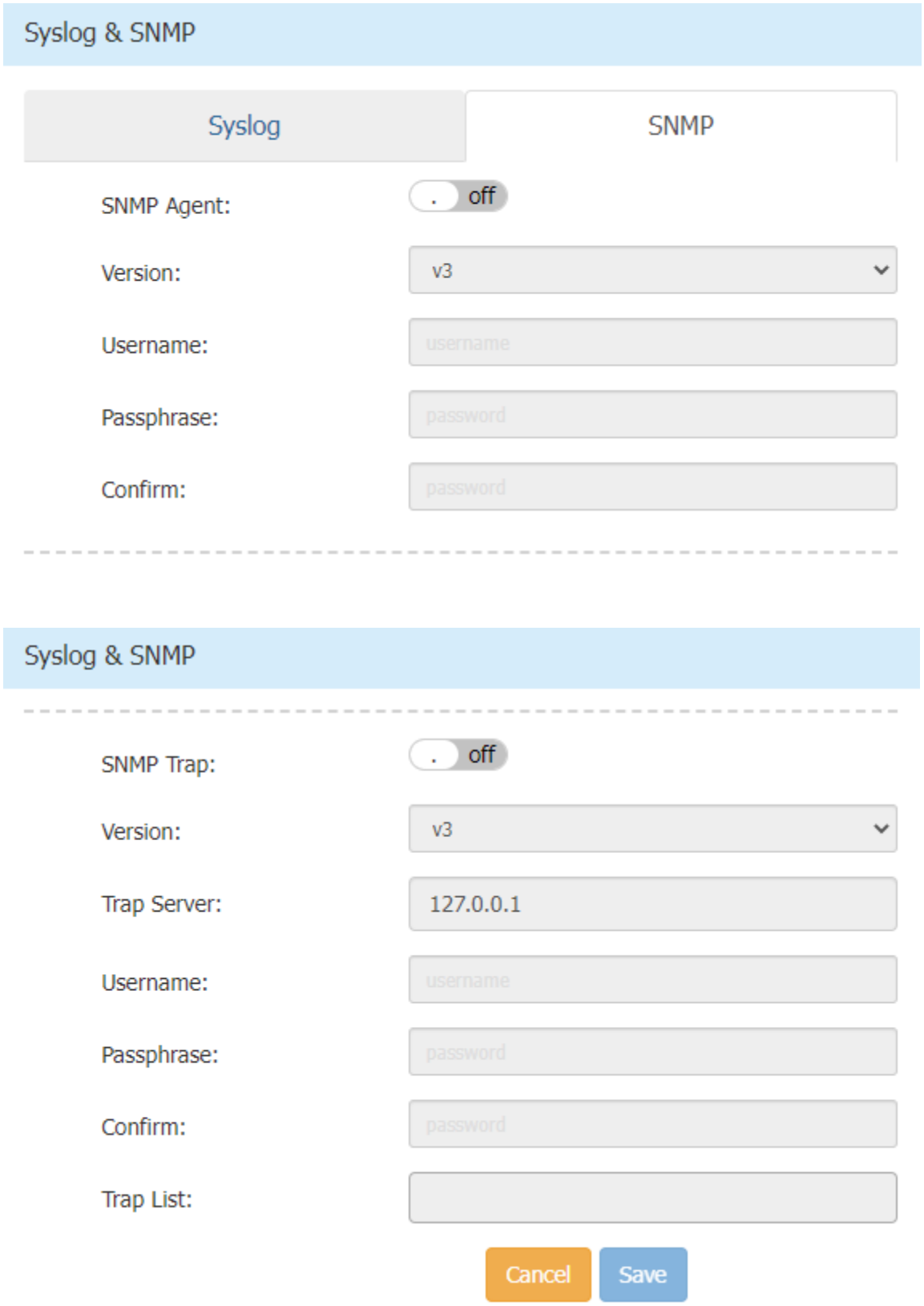
Go to Wireless->RF-> Edit RF Information, it can be configured on each radio.



[PERWIFI-147] SNMPv3

Within AP Group definition, when enabling SNMP service, add selection option for version v2c or v3, default to v3 for new installations, trap definition service must also add selection option for version v2c or v3, default to v3 for new installations.

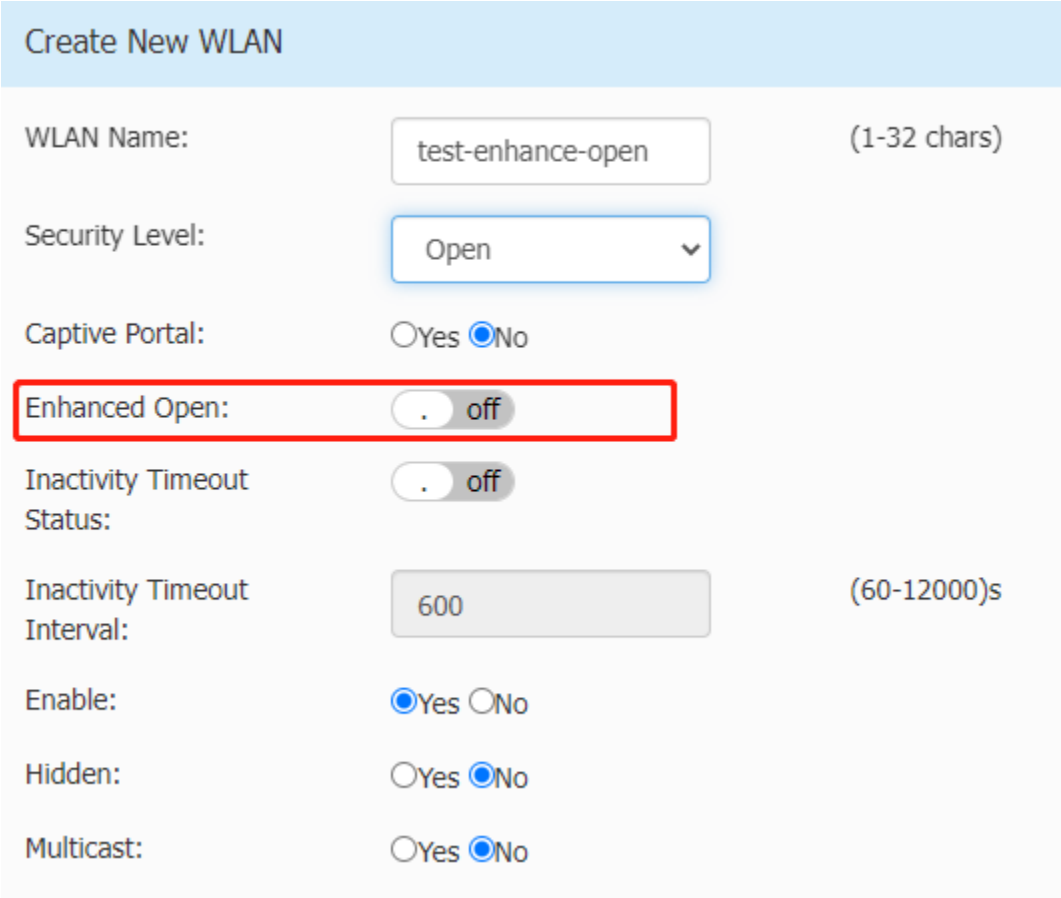
Go to System->Syslog & SNMP for configuration below.



Wi-Fi Enhanced Open

Administrators can now provision an OPEN SSID that is secure. The main Usecase is in public spaces which provide open non-protected access (particularly to Guests), can now provide encryption and privacy using OmniAccess Stellar.

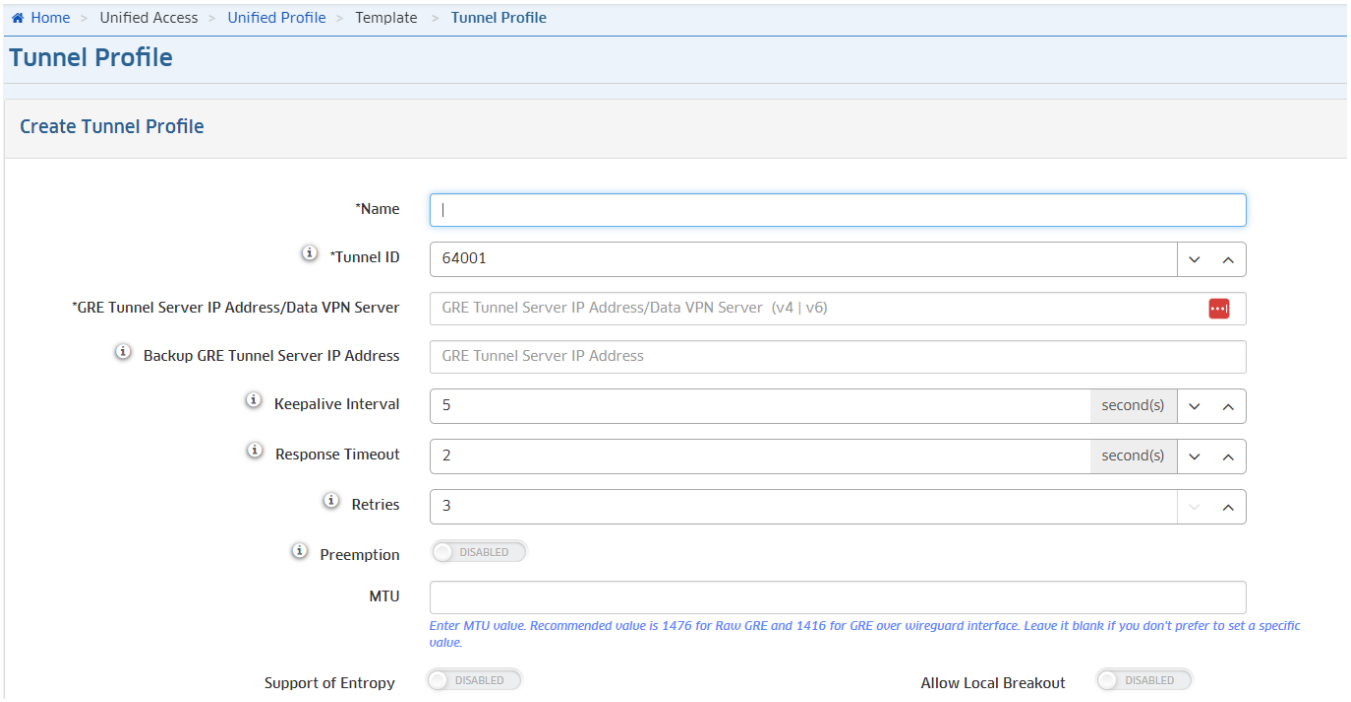
Go to WLAN -> Create New WLAN, Select Security Level with “Open”, then Enhanced Open button can be shown, by default it is disabled, switch the button to enable.



GRE tunnel resiliency (Stellar AP - OmniSwitch)

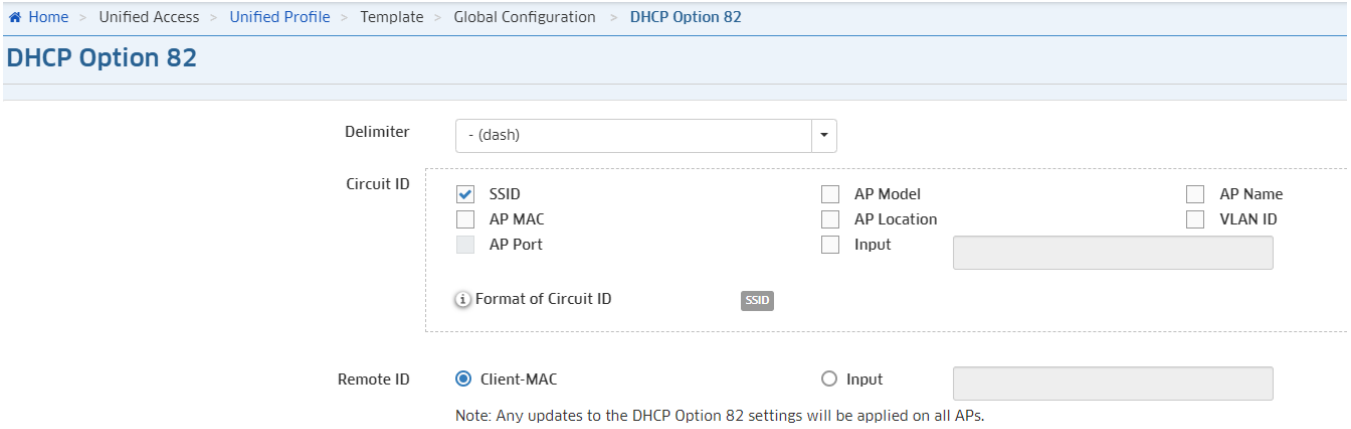
To provide GRE resilience for AP's to terminate on a primary and secondary IP address on different 6860 switches in two diverse DC's giving GRE resilience if a DC is lost.

It is supported only in OVE mode, go to OV->Home->Unified Access->Unified Profile->Template->Tunnel Profile to create corresponding Tunnel Profile, for details of use, please refer to user guide of OVE.



Multiple options in DHCP option 82 string

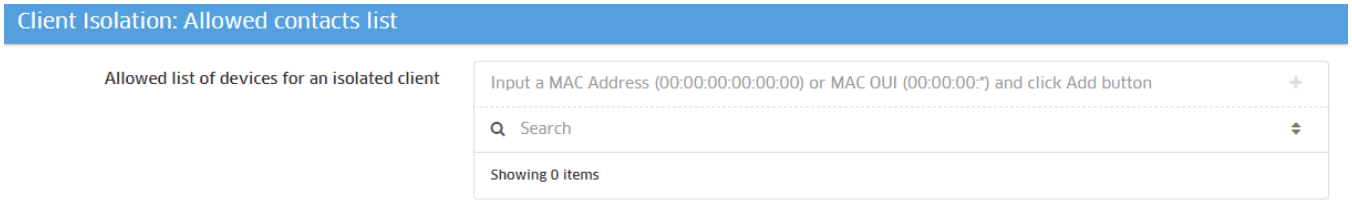
DHCP option 82 setting available through Unified Access/ Global settings is limited to selection of only single parameter or the admin can configure a custom text string. In the release of 4.0.5, AP allows the admin to specify the custom string as $$vlan-$ssid-$apmac under OVE & OVC, for details of use, please refer to user guide of OVE & OVC.



Client isolation should additionally allow configuring an Allowlist of MAC address

In the release of 4.0.5, user can add Allowlist of MAC address for Client isolation function in OVE & OVC mode.

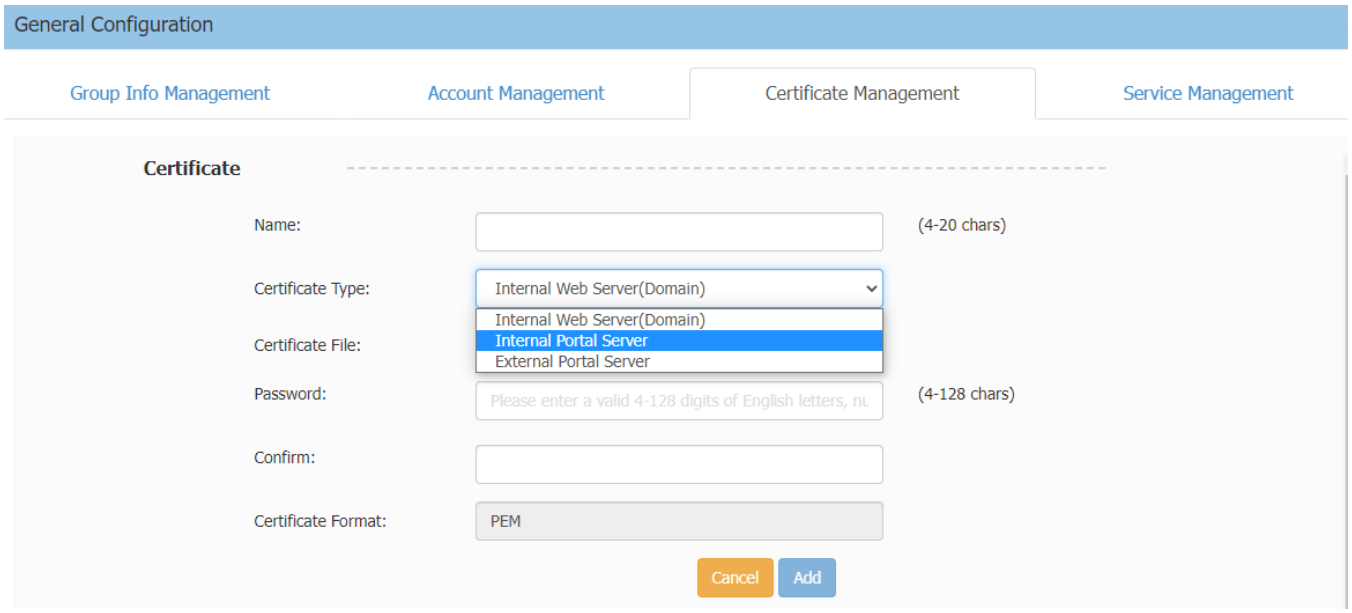
Go to OV->Home->Unified Access->Unified Profile->Template->Access Role Profile->Client Isolation to add Allowed list.



Ability to update certificate for Captive Portal on AP without upgrading them

We know that we need to renew certificates periodically as the certs are valid only for 390+ days and we also know that SOME customers will run into the scenario where they are using AP version X and their CP certificate suddenly expires. The customers will not accept to upgrade their AP just to get the new CP certificate. In the release of 4.0.5, AP provides a facility to update the certificates within the same AP.

Go to System->General Configuration->Certificate Management, Select Internal Portal Server and import correct format of certificate to AP.



AP1301H downlink TAG vlan support (Trust tag & Bypass vlan)

In the release of 4.0.5, AP provides Trust tag & Bypass vlan for AP1301H, function is the same as AP1201H.

Go to Network->Wired Network->Wired Network Configuration, Bypass Mode and Trust tag can be configured inside it.

Wired Network

AP Model	Ethernet	Bypass Mode	VLAN ID	Admin Status	Operate
OAW-AP1301H	LAN4	Disable	444	Enable	
	LAN3	Enable	5	Enable	
	LAN2	Disable	45	Enable	
	LAN1	Disable		Disable	

Wired Network Configuration

Admin Status: on

Bypass Mode: off

VLAN ID: 444 (0,2-4090)

Upstream: 0 (0-1024000)kbps

Downstream: 0 (0-1024000)kbps

Trust Tag: Use ',' interval value (2-4090)

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.