OmniAccess Stellar AP

Deployment & Configuration & Troubleshooting Guide

Alcatel-Lucent Internetworking

26801 West Agoura Road, Calabasas, CA 91301

(818) 880-3500

Revision History

Ed.	Date	Description
1.0	Sep-2018	Document creation
2.0	Jan-2019	Update Software Upgrading for AP1201 and useful CLI Commands New creation for log collection and AP reboot log collection method
2.2	May-2019	Update useful CLI commands for chapter 6.1
2.3	Jun-2019	Update section 7.2.1 to 7.2.10 for troubleshooting guide
2.4	Jun-2019	Update section 7.2.11 to 7.2.20 for troubleshooting guide
2.5	Jul -2019	Update section 7.2.21 to 7.2.30 for troubleshooting guide Update section 5.5 to 5.27 for feature introduction
2.6	Jul -2019	Update section 7.2.31 to 7.2.33 for troubleshooting guide Update section 5.28 to 5.29 for feature introduction Optimize format and details
2.7	Jul-2019	Update section 7.2.11 for troubleshooting guide Update section 7.2.34 to 7.2.35 for troubleshooting guide
2.8	Sep-2019	Update session 7.2.36 to 7.2.43 for troubleshooting guide Update session 5.30 to 5.47 for feature introduction
2.9	Sep-2019	Update the format for 7.2.38/40 Update the title for 7.2.39 and 5.44 Update the topology for 5.30 to 5.47 Update the screenshots for 5.40 and 5.41
3.0	Mar-2020	Update section 5.48 to 5.52 Update section 7.2.48 to 7.2.51
3.1	Apr-2020	Update section 7.2.44 Optimize section 6
4.0.0.1	Oct-2020	Add section 7.2.25
4.0.1.1	Jan-2021	Add 4.0.1 and recommended configuration
4.0.2	March-2021	Add 4.0.2 WCF troubleshooting feature
4.0.3	Sept-2021	Add 4.0.3 Advanced Analytics troubleshooting feature, 160MHz config, AP1351 support
4.0.4	Feb-2022	Add 4.0.3 Added WCF enhancements, AP as 802.1x client, RAP DS-Lite support
4.0.5	Mar-2023	Add 5.57 to 5.65 Add 8.42 to 8.48

Contents

Table des matières

1 Introduction

1.1 Objective

The objective of this document is to give a brief introduction of Stellar series solution on the features, configurations and troubleshooting, in order to help and guide the TSS team to provide better service to the end customers.

1.2 Glossary

ACS	Auto Channel Selection
AP	Access Point
APC	Auto Power Control
BLE	Bluetooth Low Energy
CLI	Command Line Interface
DCM	Dynamic Client Management
DRM	Dynamic Radio Management
IG	Installation Guide
MIMO	Multiple-Input Multiple-Output
MU-MIMO	Multi-User Multiple-Input Multiple-Out
OVC	OmniVista Cirrus
OVE	OmniVista Enterprise
QSG	Quick Start Guide
WBM	Web Based Management
ZTP	Zero Touch Provision
SSID	Service Set Identifier
WLAN	Wireless Local Area Network
RSSI	Received Signal Strength Indicator
IGMP	Internet Group Management Protocol
EXPRESS	Basic management unit of Stellar AP
GI	Guard Interval
PSK	Pre-Shared Key
PMF	Protected Management Frames

2 Stellar Overview

2.1 Introduction

The high-performance OmniAccess Stellar Series featuring enhanced WLAN technology with RF Radio Dynamic Adjustment, distributed control Wi-Fi architecture, secure network admission control with unified access, built in application intelligence and analytics, making it ideal for enterprises of all sizes demanding a simple, secure and scalable wireless solution.

Deliver enterprise-grade Wi-Fi to high-density client environments in offices, hospitals, schools, retail stores and warehouses. Achieve our highest speeds and best performance for your network services and applications. Ensure your users have network access anywhere on your campus.

Main features are:

- Seamless roaming and Quality of Service for real-time applications
- VoWLAN support with QoS for each application (Voice, Video, Collaboration, etc..)
- Integrated simple guest management
- Built-in customizable captive portal
- Support of role-based management access (Admin, Viewer and Guest Manager)
- Enhanced RF technology - Radio Dynamic Adjustment with DFS/TPC to deliver reliable, high-performance WLAN access
- OmniVista 2500 managed deployment embeds a visionary controllerless architecture, providing user-friendly workflows for unified access plus an integrated unified policy authentication manager
- Zero-touch provisioning (ZTP)

2.2 Product Matrix

Product Line Matrix is accessible on MyPortal: link

2.3 Working Modes

Three working modes are supported by all Stellar APs:

- **Express mode** - Plug and Play: Secure Web managed (HTTPS) cluster deployment
  Stellar Series APs by default operates in cluster architecture to provide simplified plug-and-play deployment. The access point cluster is an autonomous system that consists of a group of OmniAccess Stellar APs and a virtual controller, which is a selected access point, for cluster management. One AP cluster supports up to 255 APs. The access point cluster architecture ensures simplified and quick deployment. Once the first AP is configured using the configuration wizard, the remaining APs in the network will come up automatically with an updated configuration. This ensures the whole network is up and functional within a few minutes. Stellar Series APs also supports secure zero-touch provisioning with Alcatel- Lucent OXO Connect R2, a mechanism by which all access points in a cluster will obtain bootstrap data securely from an on premise OXO Connect.
- **OVC mode** - Cloud enabled with OmniVista Cirrus
  Stellar Series APs can be managed by Alcatel-Lucent OmniVista® Cirrus cloud platform. OmniVista® Cirrus powers a secure, resilient and scalable cloud-based network management platform. It offers hassle free network deployment and easy service rollout with advanced analytics for smarter decision making. Offers IT friendly Unified Access with secure authentication and policy enforcement for users and devices.
- **OVE mode** - OmniVista 2500 managed deployment
  Stellar Series APs can be managed by Alcatel-Lucent OmniVista® 2500 on premise Network Management System. The access points are managed as one or more access point (AP) groups (a logical grouping of one or more access points). The OmniVista 2500 next generation management suite embeds a visionary controller-less architecture, providing user friendly workflows for unified access together with an integrated unified policy authenticati on manager (UPAM) which helps define authentication strategy and policy enforcement for employees, guest management and BYOD devices. Stellar Series APs has built-in DPI technology providing real-time Application Monitoring and enforcement. The network administrator can obtain a comprehensive view of applications running in the network and apply adequate control to optimize the performance of the network for business critical applications. OmniVista 2500 provides advanced options for RF management, WIDS/WIPS for intrusion detection and prevention, and a heat map for WLAN site planning.

3 Deployment

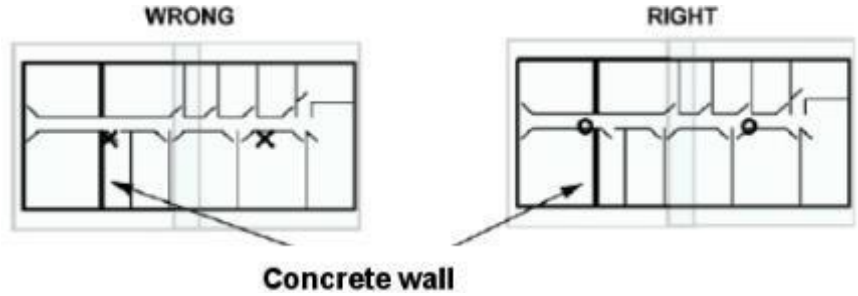
3.1 AP Placement & Guidelines

3.1.1 General Recommendations

- Position the APs above obstructions.
- Position the APs horizontally near the ceiling in the center of each coverage area, if possible. APs are designed to be installed horizontally; either standing up in a plenum or hanging from a ceiling, to create the largest coverage area per AP. Hanging the AP from the ceiling provides the best coverage.
- Position APs in locations where users are expected to be. For example, large rooms are typically a better location for APs than a hallway.
- Place APs no more than 40 meters apart from each other. Placing APs further apart almost always results in poor coverage.
- Do not mount APs outside buildings.
- Do not mount APs on building perimeter walls unless the operator wants to provide coverage outside the building.
- **Important**: Do not mount AP antennas within one meter (3 feet) of any metal obstructions. The radio frequency waves from the APs are blocked and/or reflected by metal objects, such as ducts, conduit, pipes, bookcases, elevator shafts, stairwells, and walls.

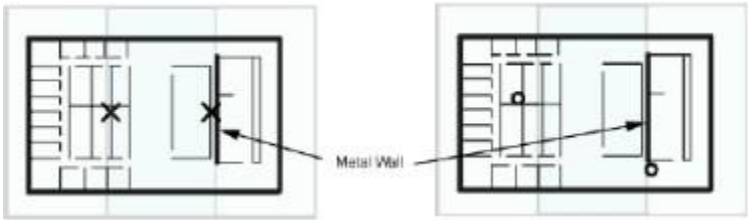
3.1.2 Three Sample Solutions to AP Placement Problems

In the first example, there is a large concrete wall in the middle of one coverage area.



The figure on the left shows a poor installation of two APs indicated with an X. The figure on the right shows a better solution. Both APs are mounted in hallways. The leftmost AP is moved to other side of wall to provide coverage on left side of the wall and the rightmost AP is moved slightly left to provide better coverage to overlap area.

In the second example, there is a large metal wall next to a planned location.



The figure on the left shows a poor installation of two APs indicated with an X. The figure on the right shows a better solution. The right most AP is moved to the hallway slightly to the right of one end of the metal wall. The left most AP is moved up and to the left to provide better coverage to overlap area.
In the third example, the AP needs to be mounted in a right angle corner of a hallway.

In the right angle corner of a hallway, mount the AP at a 45 degree angle to the two hallways as shown in the figure on the right. The Alcatel-Lucent AP internal antennas are not omnidirectional, and will cover a larger area if mounted this way.

3.1.3 Interferers

802.11b/g/n standards share the unlicensed Industrial, Scientific and Medical (ISM) band (2.4 GHz) with a number of other wireless technologies. Bluetooth devices and microwave ovens are the most common ones and can be found on a site where WLAN will be deployed. AP placement should be chosen in order to minimize interferences on the WLAN system’s performance. Interferences by WLAN on other technologies is not discussed, except cohabitation with DECT APs. For more information, see Cohabitation with DECT APs.

Cohabitation with Bluetooth Devices

Bluetooth technology is based on frequency hopping over 79 channels in the 2400 to 2483.5 MHz band.
There are 3 power classes

- Power class 1: max transmit power: +20 dBm (range 100 m)
  - Voice application: do not mount an Alcatel-Lucent AP within 10 meters of a power class 1 Bluetooth AP. The number of maximum simultaneous calls on WLAN AP can decrease significantly if a Bluetooth AP class 1 emits within 10 meters.
  - 802b/g/n data application: for maximum throughput, do not mount an Alcatel-Lucent AP within 10 meters of a power class 1 Bluetooth AP.
    802.11b/g/n data throughput is reduced when a user within 10 meters from a class 1 Bluetooth device in use. To ensure 80% of the maximum data throughput, users should be at least 10 meters away from a Bluetooth class 1 device.
- Power class 2: maximum transmit power: +4 dBm (range 10m)
  - Voice application: do not mount an Alcatel-Lucent AP within 1 meter of a power class 2 Bluetooth AP. WLAN handset users can experience cuts in the audio when placed less than 1 meter from a Bluetooth class 2 devices in use. Cuts are less than 1 second long and can appear in bursts. General audio quality is minimally impacted.
  - 802b/g Data application: for maximum throughput, do not mount an Alcatel-Lucent AP within 10 meters of a power class 2 Bluetooth AP.
  - 802.11b/g data throughput is reduced when a user is within 10 meters from a class 2 Bluetooth device in use. To ensure 80% of the maximum data throughput, users should be at least 3 meters away from a Bluetooth class 2 device.
- Power class 3: max transmit power: 0 dBm (range 10 cm)
  - Not tested, interferences should be minimal on WLAN.

Cohabitation with Microwave Ovens

Microwave ovens emit signals in the ISM band. Depending on how well the oven is shielded, emissions can disturb WLAN applications. To reduce interference from microwave ovens, check the label on the microwave which should provide the central operating frequency. Most microwave ovens operate at a central frequency of 2.45 GHz, Emissions occur in a large band, so typically disturb channels 6 to 11. In this case, an AP close to a microwave oven should be set to channel 1.

Cohabitation with other WLAN APs

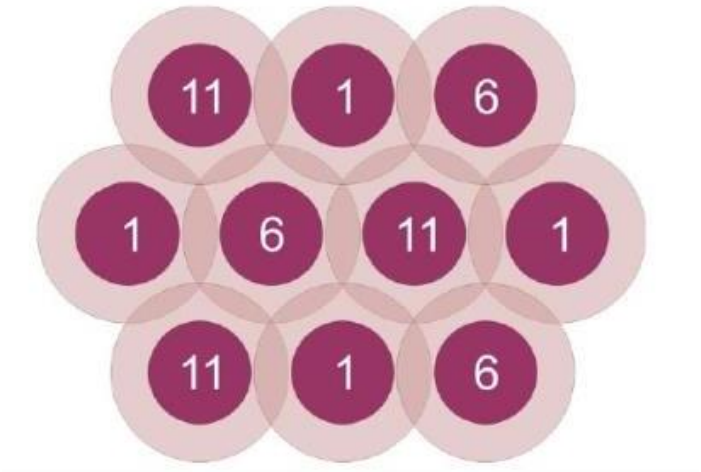
Adjacent APs need to use different radio channels to prevent interference between them. See Channel and Transmission power Considerations.

Cohabitation with DECT APs

Place WLAN APs at least 3.5 meters from DECT APs in order not to disturb DECT communications.

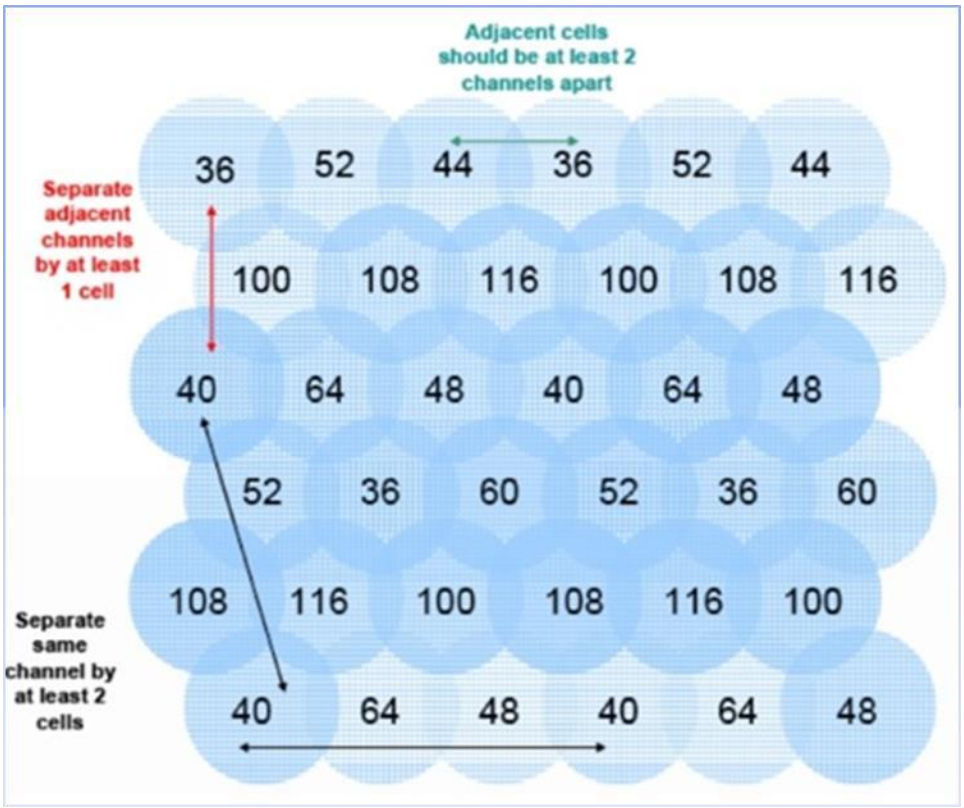
3.1.4 Channel and Transmission power Considerations

Adjacent APs need to use different radio channels to prevent interference between them. The 802.11b/g/n standard provides for three non-interfering channels: channels 1, 6, and 11. APs within range of each other should always be set to non-interfering channels to maximize the capacity and performance of the wireless infrastructure, as shown in the diagram below.



If adjacent APs are set to the same channel, or use channels with overlapping frequency bands, the resulting interference will cause a significant reduction in the network performance and throughput, and will degrade overall voice quality.

In an 802.11a/n deployment, all 23 channels are considered non-overlapping, since there is 20 MHz ofseparation between the center frequencies of each channel. However, since there is some frequency overlap on adjacent 802.11a channel sidebands, there should always be at least one cell separating adjacent channels and two cells separating the same channel, as shown in the diagram below.



For voice only applications: do not use the same channel for APs placed less than 3.5 meters from each other. This distance assumes that the AP's transmit power is 100 mW, For an interfering AP emitting at a different power level, the rule is, the interferer has to be at such a distance that it should not been seen by the system at more than －40 dBm.

For voice and data applications in 802.11b/g band: do not use the same channel for APs placed less than 12 meters from each other. This distance assumes that the AP's transmit power is 100 mW, For an interfering AP emitting at a different power level, the rule is, the interferer has to be at such a distance that it should not been seen by the system at more than －47 dBm.

The transmission power of APs can be increased or decreased to provide more or less AP coverage area. Generally, the transmission power setting should be the same for all APs in a facility. This minimizes the chance of higher-power APs interfering with nearby lower-power APs and provides consistent coverage.

It is recommended to set AP power output to 100 mW. If this cannot be accommodated, use a 50 mW setting or a minimum of 30 mW. With lower power output settings, special attention must be made to AP placement to ensure there are no frequency reuse issues. Regardless of the selected power level settings, all APs and handsets must be configured with the same settings to avoid channel conflicts and unwanted cross-channel interference.

In mixed 802.11b/g environments, set the power of the 802.11b and 802.11g radios to the same setting, if they are separately configurable. For example, set both radio to 30mW to ensure identical coverage on both radios.

For mixed 802.11a/b/g environments, where the AP uses all three radios types, AP placement should first be determined by modeling for the characteristics of 802.11a, since this environment will typically have the shortest range. Then, the transmission power of the 802.11b and 802.11g radios should be adjusted to provide the required coverage levels for those networks, within the already established AP locations.

Where possible, all APs should be set to the same transmission power level within a given radio type. For example, set all 802.11a radios to 50 mW and set all 802.11b and 802.11g radios to 30 mW. It crucial to then set the transmission power of the handset to match the transmission power of the APs. This will ensure a symmetrical communication link. Mismatched transmission power outputs will result in reduced range, poor handoff, one-way audio and other QoS issues.

3.2 Express mode

Stellar APs, by default, are running in "**Express mode**". To configure the AP out-of-box, connect the AP to the network and powered by POE or power adapter, and ensure the AP could retrieve an IP address from the network.

When the LED on AP would be in "Green Blinking" state, a SSID named with "**AP-xx:xx**" (xx:xx is the last 4 characters of the AP MAC address) will be able to detected and connected. After associated with this WLAN SSID, the AP Web Based Management page would be able to reached via below default URL: http://mywifi.al-enterprise.com:8080/. After login with the default account (user: **Administrator** / Password: **admin**), the "***configuration wizard***" would be displayed on WBM configuration, user may follow the wizard to configure the AP.

For more details, please refer to the QSG document of each AP model.

In case of some abnormal situation, below methods could help to make the AP back to "factory settings":

- Long pressing the "reset" button
- Command "*firstboot*" + "*reboot*" input via Console or SSH connection
- Click "*Clear All Configuration*" from "*WBM -> AP Configuration*"

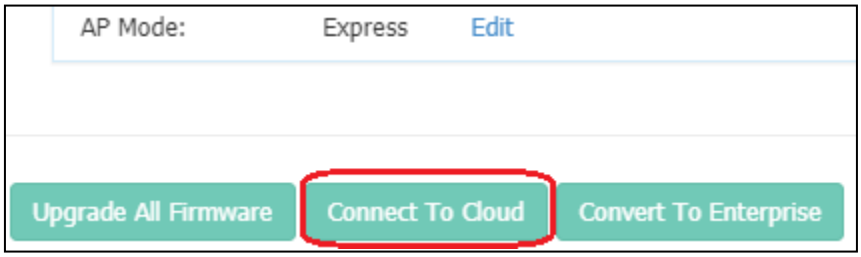
3.3 OV Cloud Mode

Stellar APs could be centralized managed by OmniVista Cirrus. A default OVC Server URL is built-in AP software. The AP will be switched to OVC mode automatically when below two conditions are met:

- AP network is able to reach the built-in OVC Server URL
- The AP hardware information has been correctly configured in OVC Server.

AP in "Express mode" could be switched to OVC mode through Web Based Management as below:

- Login AP WBM, go to "AP Configuration", and click "Connect To Cloud" button.



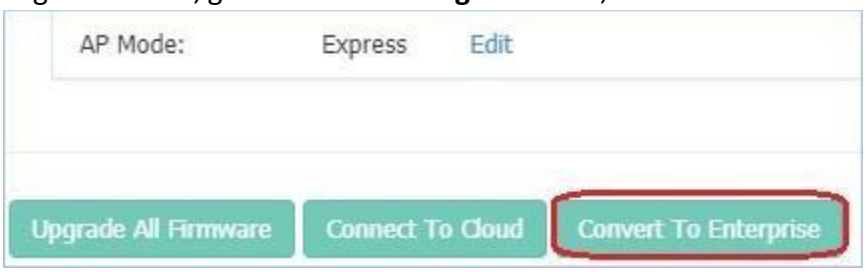
- Specify the OVC Management Server address, and press "Save" button.

For more details, please refer to the related guides or documents of OmniVista Cirrus.

3.4 OV Enterprise mode

Stellar APs could also be centralized managed by OmniVista Enterprise. Below two methods could be used to switch the AP to OVE mode:

- AP receives option 43 or option 138 from the DHCP server specifying the OmniVista IP, the AP will boot up and connect to OmniVista 2500 for management.
- AP in "Express mode" could be switched to OVE mode through Web Based Management as below:
  - Login AP WBM, goes to "**AP Configuration**", and click "**Convert To Enterprise**" button.



  - Specify the OVE Server IP address, and press "**Convert**"

For more details, please refer to the related guides or documents of OmniVista Enterprise.

4 Software Upgrading

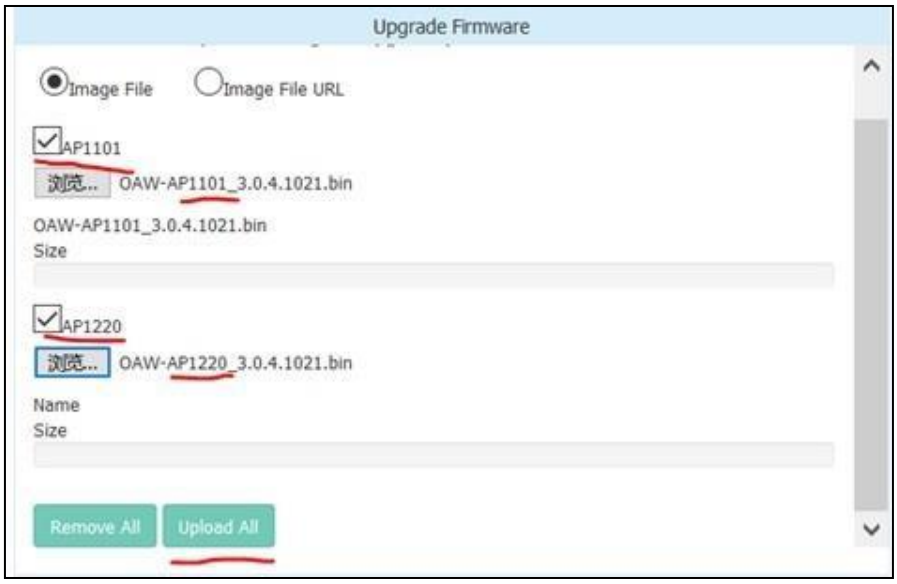
4.1 Upgrading in Express mode

Working in “ Express mode ” , the AP software upgrading could be managed from the Web Based Management. The software upgrading could be managed either in the whole cluster or per single AP. While to avoid any incompatibility issue, strongly recommend to keep all the APs within the whole cluster in the same software versions.

Procedures of AP upgrading in the whole cluster

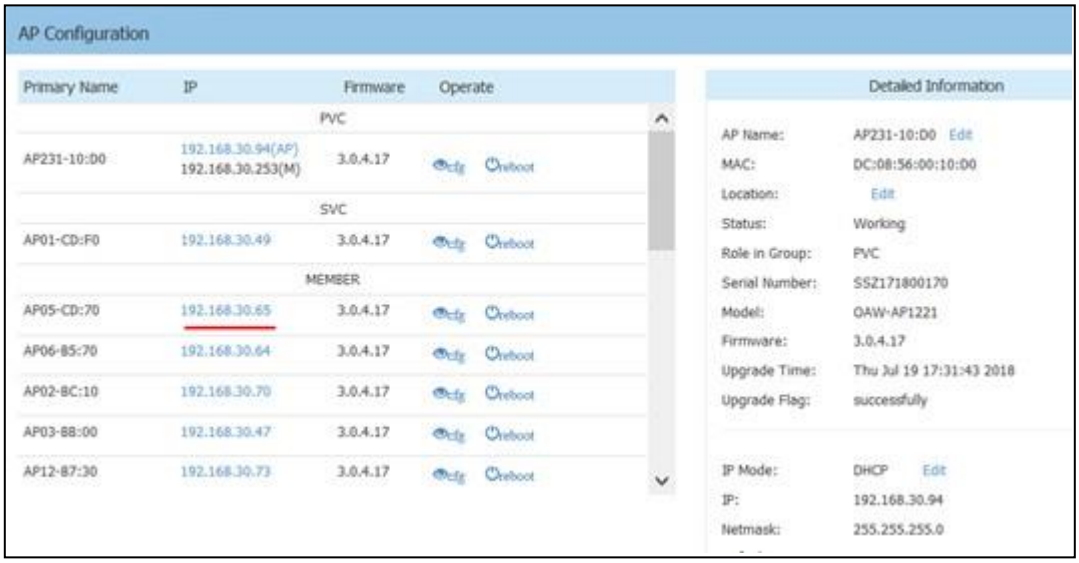
- Login AP WBM, go to “**AP Configuration**”, and click “**Upgrade All Firmware**” button.
- Click the AP modes need to be upgraded, and select the AP firmware accordingly. Then press “**Upload All**”.

  Importance: Don't turn off the power during the upgrade process.



Procedures of Single AP Software Upgrading:

- Login AP Cluster WBM, go to “**AP Configuration**” and Select the IP address of AP which need to be upgraded.



- A new WBM page (apui) will be opened. Click "**Image File**" from "System" and select the AP software according to the AP model. Press "**Upload**" button to start the upgrading.
  Importance: Don't turn off the power during the upgrade process.

4.2 Upgrading in OV Cloud mode

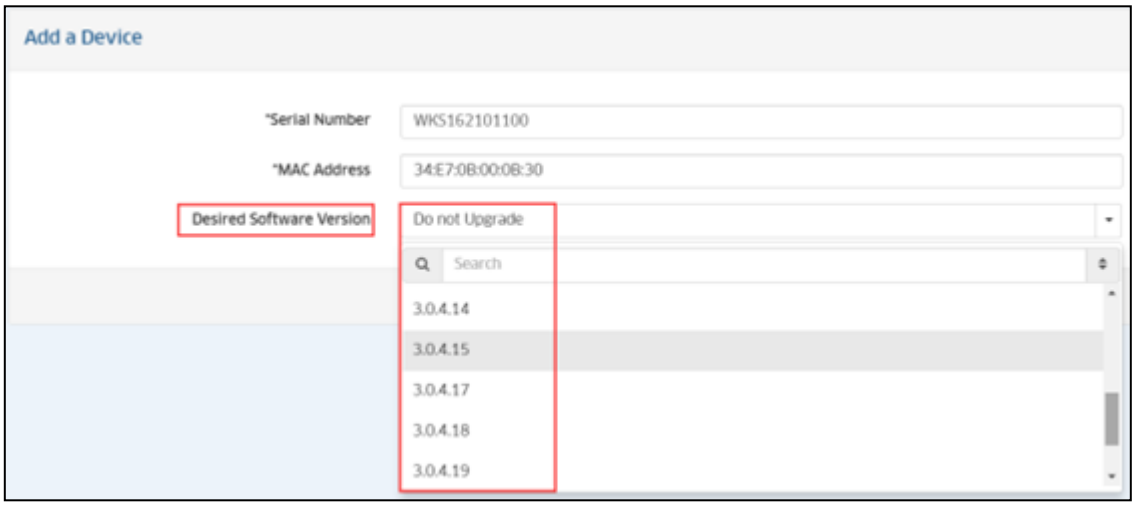
When working in OVC (OmniVista Cloud) mode, the AP software could be centralized managed through OVC management server. Single or all APs could be upgraded as requested.

✐ **Note**: *From AWOS-3.0.4.x and later releases, the AP upgrading will be started in 30 minutes. Regarding the previous releases (AWOS-3.0.3.x), "manual restart" of the AP would be required to trigger the upgrading.*

Procedures of the upgrading in OVC mode:

Upgrade when registering a new AP to OV Cloud

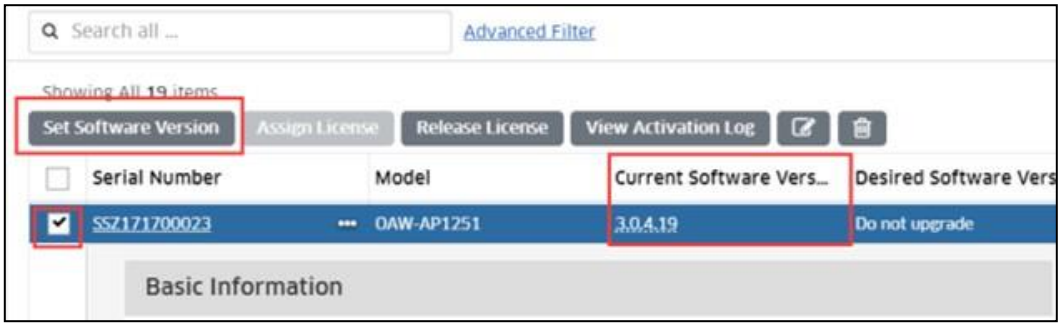
- Log in OV cloud, enter the **Network** -> **inventory** -> **device Catalog** page, click the "**+**" button, enter the MAC and SN, and select the software version that wants to be updated in the "**Desired Software Version**", then click create.



- AP will be registered to OV cloud after upgrading to the selected version.

Upgrade for one registered AP

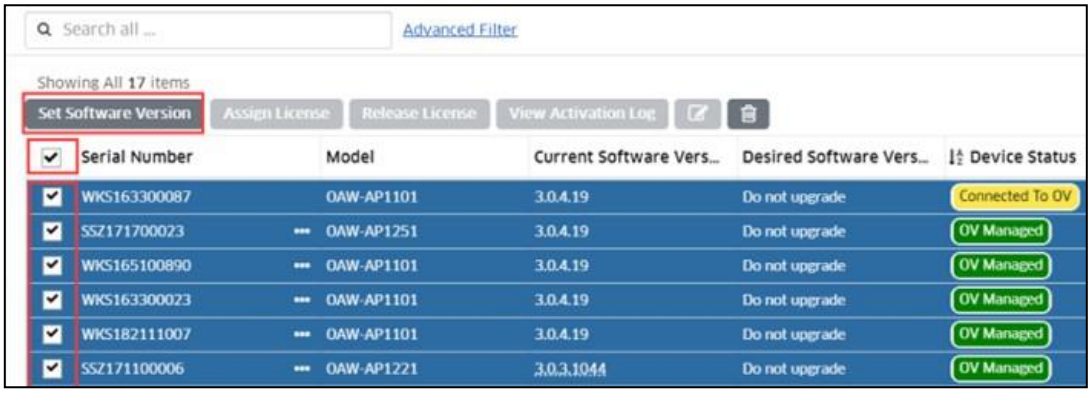
- Go to the **Network** -> **inventory** -> **device Catalog** page, select the AP need to be upgraded, and click the "**Set Software Version**" button.



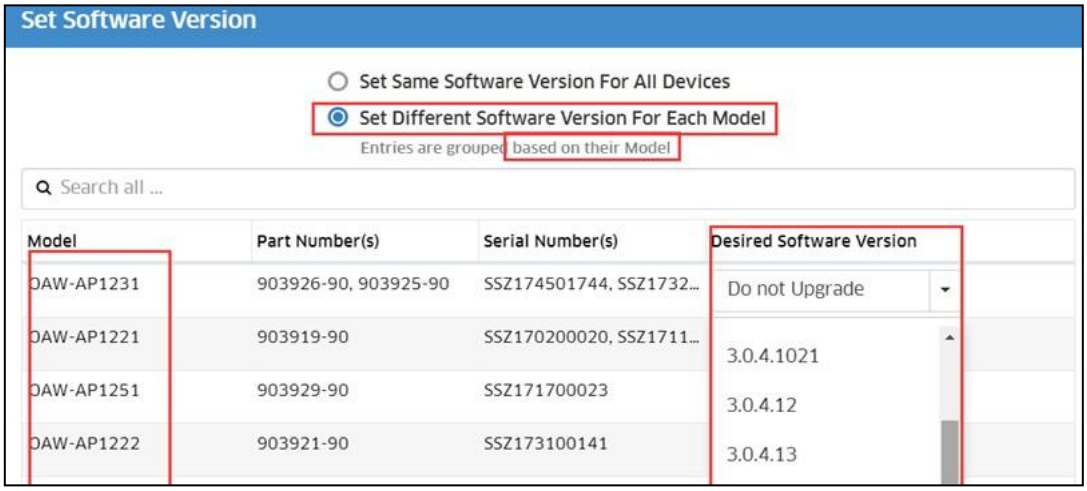
- Select the version you want to upgrade in "**Desired Software Version**" and click **apply**.
  The AP will start to upgrade when the next callhome is sent.

Upgrade for multiple registered AP

- Go to the **Network** -> **inventory** -> **device Catalog** page, select multiple (or all) AP need to be upgraded, and click the "**Set Software Version**" button



- Select the "**Set Different Software Version For Each Model**" option, select the version to be upgraded in the "**Desired Software Version**" drop-down box, and click apply.



- The APs will start to upgrade when the next call-home was sent.

4.3 Upgrading in OV Enterprise mode

When working in OVE (OmniVista Enterprise) mode, the AP software could be centralized managed through OVE management server. Single or all APs could be upgraded as requested.

✐ **Note:** *Reboot of the AP is mandatory during the AP upgrading, so no WLAN service at that moment.*

Procedures of the upgrading in OVE mode:

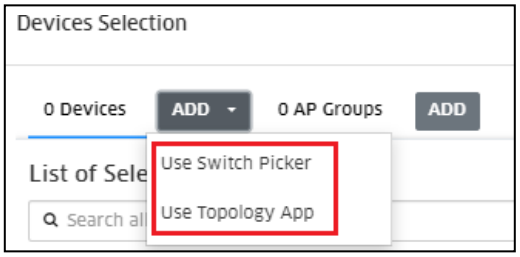
AP Software versions uploading:

- Log in OV Enterprise, enter the **Configuration--Resource Manager--Upgrade Image** page and click **import** to upload the AP software version to be upgraded.

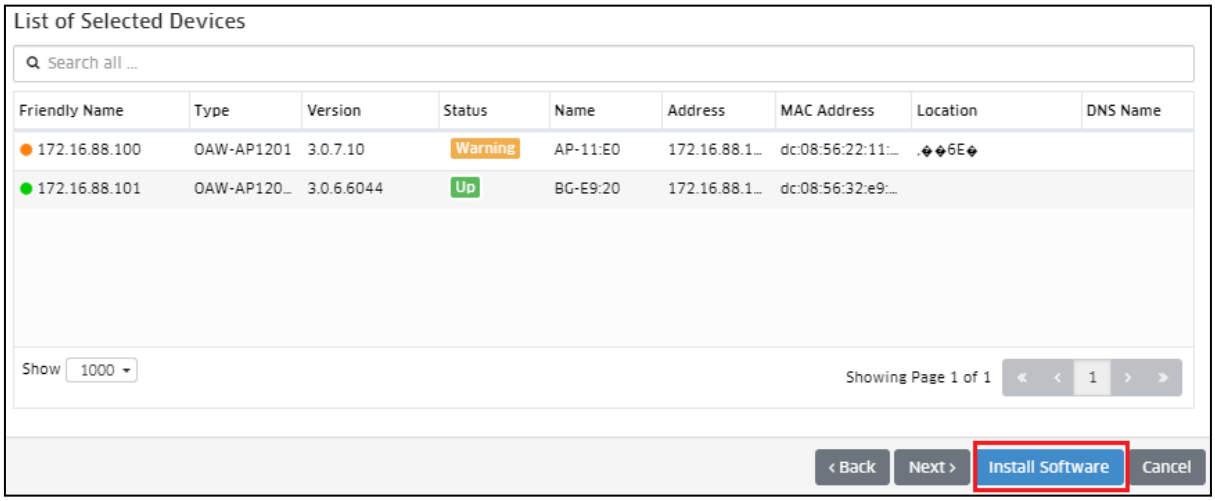
- After uploading the AP software version, please select the file and click the **install** button, and then go to **devices selection** step.

Upgrade per AP/APs

- Click the "**next**" to open the **device selection** window. Click the **ADD** button of device and use "**Use Picker**" or "**Use Topology App**" to select the AP to be upgraded.



- In the "**Use Switch Picker**" page, select the AP, and click the **add** button to add to the selected window, then click **OK**
- In the "**Use Topology App**" page, select the AP need to be upgraded and click **OK.**



Upgrade per AP Group

- In the **device selection** window, click the **ADD** button of AP Groups, go to the group selection window.
- Select AP Groups, and click the **Add** button, and click OK.
- After selecting the AP, click the "**Next**" to enter the Software Installation page.
- Click the "**install software**" button to enter the upgrade page.

✐ **Note**: *To avoid incompatibility issues, suggest keeping the same AP software version in the AP group. So, it's better to use "AP Group" when upgrading the APs.*

4.4 Upgrading through Bootloader

In some specific cases, the AP may be not in a normal operation state, which cannot be succeeded upgraded though any of the working modes. It will need to upgrade the AP through Bootloader.

4.4.1 Entering Bootloader

To enter the bootloader, it will need to connect the console port and open the console session. During the AP initialization, pressing any key when below words showing on the screen of console:

```
Hit any key to stop autoboot:  2
```

4.4.2 AP1101

Procedure of the upgrading AP1101 through bootloader:

✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:
- OAW-AP1101-UBOOT_KERNEL_**4.0.x.x**.bin
- OAW-AP1101-UBOOT_ROOTFS_**4.0.x.x**.bin

✓ To enter the bootloader during AP initialization, which is described in 4.4.1.

✓ Network configuration (IP Address, TFTP Server Address…)

Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

```
# set ipaddr 172.16.18.11
# set serverip 172.16.18.129
```

✓ AP upgrading through bootloader

```
# set bootcmd bootm 0x9f050000
# mw 0x18060008 0x0
# set lk-aos "tftp 0x80060000 OAW-AP1101-UBOOT_KERNEL_4.0.x.x.bin && erase 0x9f050000
+0x180000 &&cp.b 0x80060000 0x9f050000 0x180000"
# set lf-aos "tftp 0x80060000 OAW-AP1101-UBOOT_ROOTFS_4.0.x.x.bin && erase 0x9f1d0000
+0xc20000 &&cp.b 0x80060000 0x9f1d0000 0xc20000"
# run lk-aos && run lf-aos && reset
```

4.4.3 AP1220 Series

Procedure of the upgrading AP1220 Series through bootloader:

✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:

- OAW-AP1220-UBOOT_FIRMWARE_**4.0.x.x**.bin

✓ To enter the bootloader during AP initialization, which is described in 4.4.1.

✓ Network configuration (IP Address, TFTP Server Address…)

Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

```
# set ipaddr 172.16.18.11
# set serverip 172.16.18.129
# save
```

✓ AP upgrading through bootloader

```
# tftpboot 0x84000000 OAW-AP1220-UBOOT_FIRMWARE_4.0.x.x.bin
# nand erase 0x0 0x10000000 && nand write 0x84000000 0x0 $filesize
# nand read 0x85000000 0x0 $filesize
# md5sum 0x85000000 $filesize
# reset
```

✓ After AP reboot, entering below commands to make dual system working.

```
# fm_switch
# reboot
```

4.4.4 AP1230 Series

There’re two Ethernet ports on AP1230 Series, one is Gigabit Ethernet port, another one is 2.5 Gigabit Ethernet port. We **MUST** use the **Gigabit Ethernet** port for both upgrading AP through bootloader and upgrading UBoot version.

Procedure of the upgrading AP1230 through bootloader:

✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:

- OAW-AP1230-UBOOT_FIRMWARE_**4.0.x.x**.bin

✓ To enter the bootloader during AP initialization, which is described in 4.4.1.

✓ Network configuration (IP Address, TFTP Server Address…)

Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

```
# set ipaddr 172.16.18.11
# set serverip 172.16.18.129
# save
```

- ✓ AP upgrading through bootloader

```
# tftpboot 0x42000000 OAW-AP1230-UBOOT_FIRMWARE_4.0.x.x.bin
# nand erase 0x0 0x10000000 && nand write 0x42000000 0x0 $filesize && nand read 0x42000000 0x3000000 $filesize
# nand read 0x43000000 0x0 $filesize && md5sum 0x43000000 $filesize
# nand read 0x44000000 0x3000000 $filesize && md5sum 0x44000000 $filesize
# reset
```

- ✓ After AP reboot, entering below commands to make dual system working.

```
# fm_switch
# reboot
```

4.4.5 AP1251

Procedure of the upgrading AP1250 Series through bootloader:

- ✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:
  - OAW-AP1250-UBOOT_FIRMWARE_**4.0.x.x**.bin
- ✓ To enter the bootloader during AP initialization, which is described in 4.4.1.
- ✓ Network configuration (IP Address, TFTP Server Address…)

  Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

```
# set ipaddr 172.16.18.11
# set serverip 172.16.18.129
# save
```

- ✓ AP upgrading through bootloader

```
# tftpboot 0x84000000 OAW-AP1250-UBOOT_FIRMWARE_4.0.x.x.bin
# nand erase 0x0 0x10000000 && nand write 0x84000000 0x0 $filesize && nand read 0x84000000 0x03000000 $filesize
# nand read 0x85000000 0x0 $filesize && md5sum 0x85000000 $filesize
# nand read 0x83000000 0x03000000 $filesize && md5sum 0x83000000 $filesize
# reset
```

- ✓ After AP reboot, entering below commands to make dual system working.

```
# fm_switch
# reboot
```

4.4.6 AP1201

Procedure of the upgrading AP1201 Series through bootloader:

- ✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:
  - OAW-AP1201-UBOOT_FIRMWARE_3.0.x.x.bin
- ✓ Network configuration (IP Address, TFTP Server Address…)

  Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

```
# set ipaddr 172.16.18.11
# set serverip 172.16.18.129
```

- ✓ AP upgrading through bootloader

```
# tftpboot 0x84000000 OAW-AP1201-UBOOT_FIRMWARE_3.0.x.x.bin
# nand erase 0x0 0x8000000 && nand write 0x84000000 0x0 $filesize && nand write 0x84000000 0x03000000 $filesize
# nand read 0x85000000 0x0 $filesize && md5sum 0x85000000 $filesize
Second check Md5 Command:
# nand read 0x83000000 0x03000000 $filesize && md5sum 0x83000000 $filesize
```

```
# reset
```

4.4.7 AP1320 Series

Procedure of the upgrading AP1320 Series through bootloader:

✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:
- OAW-AP1320-UBOOT_FIRMWARE_4.0.x.xx.bin

✓ To enter the bootloader during AP initialization, which is described in 4.4.1.

✓ Network configuration (IP Address, TFTP Server Address…)

Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

```
# set ipaddr 172.16.18.11
# set serverip 172.16.18.129
# save
```

✓ AP upgrading through bootloader

```
# tftpboot 0x44000000 OAW-AP1320-UBOOT_FIRMWARE_4.0.x.xx.bin
# nand erase 0x0 0x3000000 && nand write 0x44000000 0x0 $filesize && nand erase
0x3800000 0x3000000 && nand write 0x44000000 0x3800000 $filesize
# reset
```

4.4.8 AP1311

Procedure of the upgrading AP1311 through bootloader:

✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:
- OAW-AP1311-UBOOT_FIRMWARE_4.0.x.xx.bin

✓ To enter the bootloader during AP initialization, which is described in 4.4.1.

✓ Network configuration (IP Address, TFTP Server Address…)

Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

```
# set ipaddr 172.16.18.11
# set serverip 172.16.18.129
# save
```

✓ AP upgrading through bootloader

```
# tftpboot 0x42000000 OAW-AP1311-UBOOT_FIRMWARE_4.0.x.xx.bin
# nand erase.chip && nand write 0x42000000 0x0 $filesize && nand write 0x42000000
0x3200000 $filesize
# nand read 0x42000000 0x0 $filesize && md5sum 0x42000000 $filesize
# nand read 0x42000000 0x3200000 $filesize && md5sum 0x42000000 $filesize
# reset
```

4.4.9 AP1301

Procedure of the upgrading AP1301 through bootloader:

✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:
- OAW-AP1301-UBOOT_FIRMWARE_4.0.x.xx.bin

✓ To enter the bootloader during AP initialization, which is described in 4.4.1.

✓ Network configuration (IP Address, TFTP Server Address…)

Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

```
# set ipaddr 172.16.18.11
# set serverip 172.16.18.129
# save
```

✓ AP upgrading through bootloader

```
# tftpboot 0x42000000 OAW-AP1301-UBOOT_FIRMWARE_4.0.x.xx.bin
# nand erase.chip && nand write 0x42000000 0x0 $filesize && nand write 0x42000000 0x3200000 $filesize
# nand read 0x42000000 0x0 $filesize && md5sum 0x42000000 $filesize
# nand read 0x42000000 0x3200000 $filesize && md5sum 0x42000000 $filesize
# reset
```

4.4.10 AP1360 Series

Procedure of the upgrading AP1360 Series through bootloader:

✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:

- OAW-AP1360_FULL_4.0.x.x.bin

✓ To enter the bootloader during AP initialization, which is described in 4.4.1.

✓ Network configuration (IP Address, TFTP Server Address…)

Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

```
# set ipaddr 172.16.18.11
# set serverip 172.16.18.129
# save
```

✓ AP upgrading through bootloader

```
# tftpboot 0x41000000 OAW-AP1360_FULL_4.0.x.x.bin
# sf probe;sf read 0x41380000 0x380000 0x40000 && sf erase 0 0x800000;sf write 0x41000000 0 0x800000;
# nand device 0 && nand erase.chip && nand write 0x41800000 0x0 0x7000000
# reset
```

4.4.11 AP1351

Procedure of the upgrading AP1351 Series through bootloader:

✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:

- OAW-AP1351-UBOOT_FIRMWARE_4.0.x.x.bin

✓ Network configuration (IP Address, TFTP Server Address…)

Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

```
# set ipaddr 172.16.18.11
# set serverip 172.16.18.129
```

✓ AP upgrading through bootloader

```
# tftpboot 0x84000000 OAW-AP1351-UBOOT_FIRMWARE_4.0.x.x.bin
# setenv machid 8010012 && sf probe && imgaddr=0x44000000 && source $imgaddr:script
# mmc read 0x44000000 0x00000022 a000 && md5sum 0x44000000 0x1400000
# mmc read 0x44000000 0x0000a022 a000 && md5sum 0x44000000 0x1400000
# mmc read 0x44000000 0x00014022 a000 && md5sum 0x44000000 0x1400000 (only check 20M)
# mmc read 0x44000000 0x0004a022 a000 && md5sum 0x44000000 0x1400000 (only check 20M)
# reset
```

4.5 Upgrading UBoot

Normally, it's **NOT** necessary to upgrade UBoot software of APs. While in some very special cases, the new UBoot software version maybe needed to solve some issues.

This chapter describes the procedure of the UBoot upgrading for different AP models.

4.5.1 AP1101

Procedure of UBoot upgrading:

- ✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:
  - hos-r21-boot.bin
- ✓ To enter the bootloader during AP initialization, which is described in 4.4.1.
- ✓ Network configuration (IP Address, TFTP Server Address…)

  Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

```
ath> set ipaddr 172.16.18.11
ath> set serverip 172.16.18.129
```

- ✓ UBoot Upgrading

```
ath> run lu
```

4.5.2 AP1220 Series

Procedure of UBoot upgrading:

- ✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:
  - OAW-AP1220-uboot_1.x.bin
- ✓ To enter the bootloader during AP initialization, which is described in 4.4.1.
- ✓ Network configuration (IP Address, TFTP Server Address…)

  Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

```
# set ipaddr 172.16.18.11
# set serverip 172.16.18.129
```

- ✓ UBoot Upgrading

```
# tftpboot 0x84000000 OAW-AP1220-uboot_1.x.bin
# imgaddr=0x84000000 && source $imgaddr:script && reset
```

4.5.3 AP1230 Series

Procedure of UBoot upgrading:

- ✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:
  - OAW-AP1230-uboot_1.x.bin
- ✓ To enter the bootloader during AP initialization, which is described in 4.4.1.
- ✓ Network configuration (IP Address, TFTP Server Address…)

  Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

```
# set ipaddr 172.16.18.11
# set serverip 172.16.18.129
# save
```

- ✓ UBoot Upgrading

```
# tftpboot 0x42000000 OAW-AP1230-uboot_1.x.bin
# imgaddr=0x42000000&&sf probe&&source $imgaddr:script
```

```
# reset
```

4.5.4 AP1251

Procedure of UBoot upgrading:

- ✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:
  - OAW-AP1250-uboot_1.x.bin
- ✓ To enter the bootloader during AP initialization, which is described in 4.4.1.
- ✓ Network configuration (IP Address, TFTP Server Address…)

  Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

```
# set ipaddr 172.16.18.11
# set serverip 172.16.18.129
# save
```

- ✓ UBoot Upgrading

```
# tftpboot 0x84000000 OAW-AP1250-uboot_1.x.bin
# imgaddr=0x84000000 source $imgaddr:script && reset
```

4.5.5 AP1201

Procedure of UBoot upgrading:

- ✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:
  - OAW-AP1201-uboot_1.x.bin
- ✓ To enter the bootloader during AP initialization, which is described in 4.4.1.

  Example: IP address=172.16.18.11; TFTP Server Address=172.16.18.129

```
# set ipaddr 172.16.18.11
# set serverip 172.16.18.129
```

- ✓ UBoot Upgrading

```
# tftpboot 0x84000000 OAW-AP1201-uboot_1.0.bin
# imgaddr=0x84000000 source $imgaddr:script
# reset
```

4.5.6 AP1320 Series

Procedure of UBoot upgrading:

- ✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:
  - ap321_uboot_v1.x.img
- ✓ To enter the bootloader during AP initialization, which is described in 4.4.1.

  Example: IP address=172.16.18.11; TFTP Server Address=172.16.18.129

```
# set ipaddr 172.16.18.11
# set serverip 172.16.18.129
```

- ✓ UBoot Upgrading

```
# tftpboot 0x44000000 ap321_uboot_v1.x.img
# set machid 8010009
# sf probe
# imgaddr=0x44000000 && source $imgaddr:script
# reset
```

4.5.7 AP1311

Procedure of UBoot upgrading:

- ✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:
  - ap311_uboot_v1.x.img
- ✓ To enter the bootloader during AP initialization, which is described in 4.4.1.
  Example: IP address=172.16.18.11; TFTP Server Address=172.16.18.129
  ```
  # set ipaddr 172.16.18.11
  # set serverip 172.16.18.129
  ```
- ✓ UBoot Upgrading
  ```
  # tftpboot 0x42000000 ap311_uboot_v1.x.img
  # sf probe && imgaddr=0x42000000 && source $imgaddr:script
  # reset
  ```

4.5.8 AP1301

Procedure of UBoot upgrading:

- ✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:
  - ap301_uboot_v1.x.img
- ✓ To enter the bootloader during AP initialization, which is described in 4.4.1.
  Example: IP address=172.16.18.11; TFTP Server Address=172.16.18.129
  ```
  # set ipaddr 172.16.18.11
  # set serverip 172.16.18.129
  ```
- ✓ UBoot Upgrading
  ```
  # tftpboot 0x42000000 ap301_uboot_v1.x.img
  # sf probe && imgaddr=0x42000000 && source $imgaddr:script
  # reset
  ```

4.5.9 AP1360 Series

Procedure of UBoot upgrading:

- ✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:
  - Ap231_uboot_v1.x.img
- ✓ To enter the bootloader during AP initialization, which is described in 4.4.1.
  Example: IP address=172.16.18.11; TFTP Server Address=172.16.18.129
  ```
  # set ipaddr 172.16.18.11
  # set serverip 172.16.18.129
  ```
- ✓ UBoot Upgrading
  ```
  # tftpboot 0x84000000 AP231-uboot_1.x.bin
  # imgaddr=0x84000000 source $imgaddr:script
  # reset
  ```

4.5.10 AP1351

Procedure of UBoot upgrading:

- ✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:
  - ap351-uboot_v1.x.img
- ✓ To enter the bootloader during AP initialization, which is described in 4.4.1.
  Example: IP address=172.16.18.11; TFTP Server Address=172.16.18.129

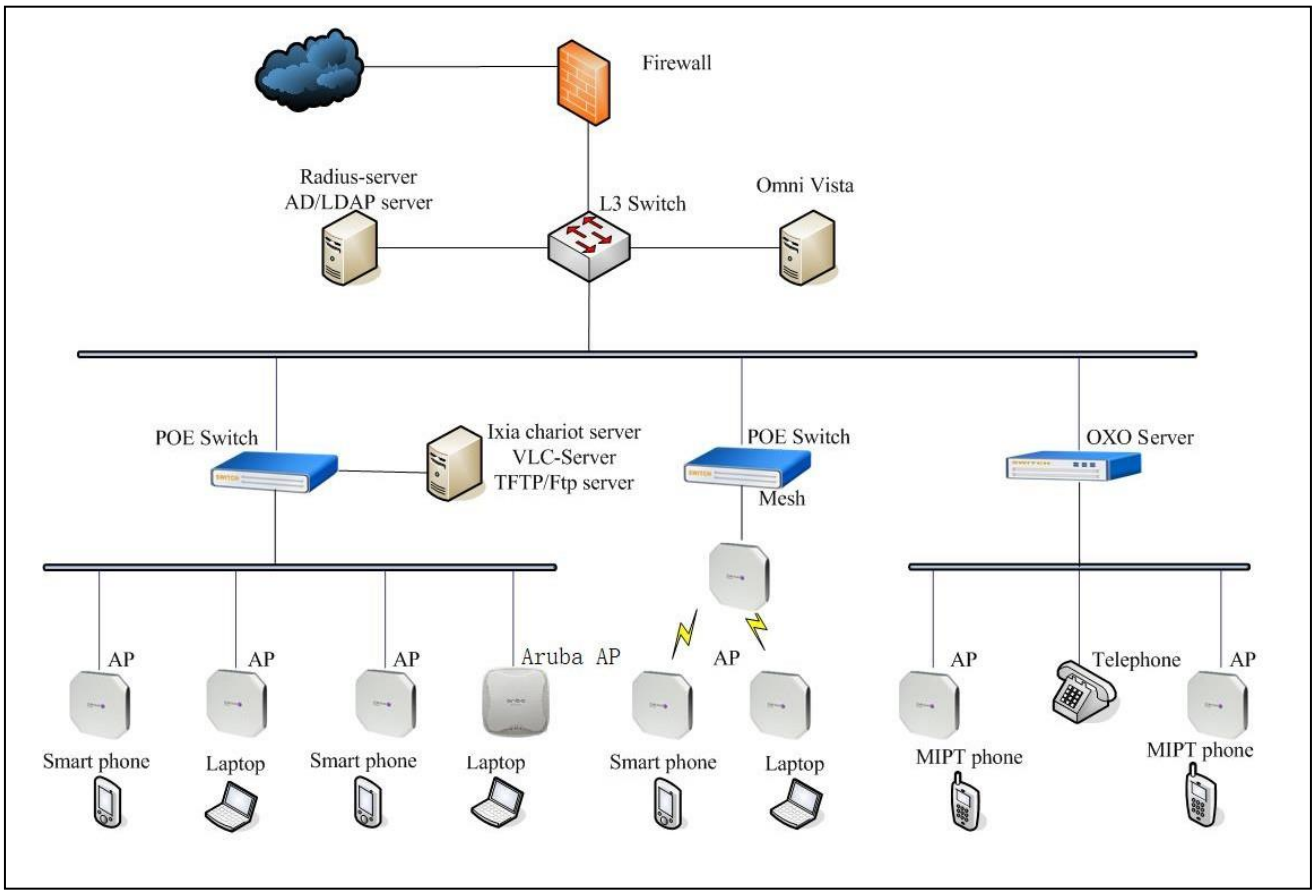
```
# set ipaddr 172.16.18.11
# set serverip 172.16.18.129
```

- ✓ UBoot Upgrading

```
# tftpboot 0x84000000 ap351-uboot_v1.x.img
# setenv machid 8010012 && sf probe && imgaddr=0x44000000 && source $imgaddr:script
# reset
```

5 Features and Configurations

5.1 Topology for reference



5.2 ACS & DRM

5.2.1 Feature description

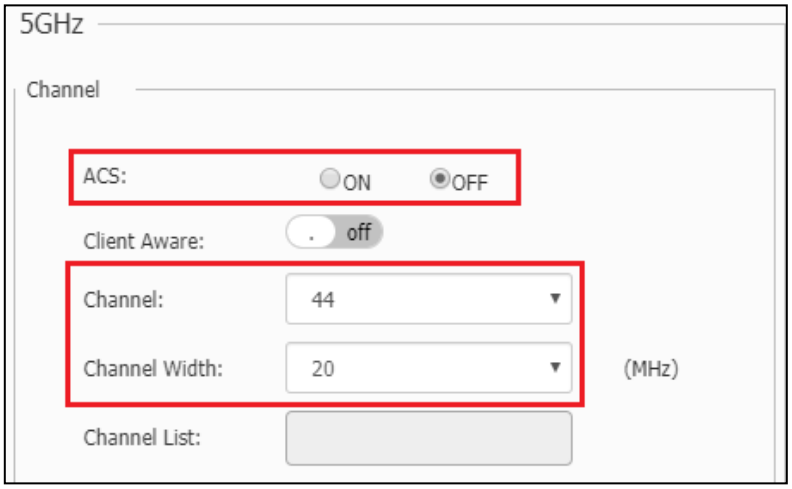
Adjacent APs need to use different radio channels to prevent interference between them. APs within range of each other should always be set to non-interfering channels to maximize the capacity and performance of the wireless infrastructure. Please check chapter 3.1.3 for more detail.

To avoid mutual interference with adjacent APs, ACS (auto channel selection) could be used to make the AP to check and select a best channel under the radio environment automatically. The algorithm will help the AP to find the channel with best radio performance.

And if working on 5G radio, the DRM could be used to define a “Channel List” to make the AP to select the channels from the list.

5.2.2 Configuration and Recommendation

Login the WEB UI and go to “**Wireless**” sub-menu.
Go to “**RF**” configuration, and select the AP to be configured.
The **ACS** could be turn **ON/OFF** separately on 2.4GHz or 5GHz.
On 5GHz radio, the DRM could be configured.



5.3 APC

5.3.1 Feature description

In order to have a better radio coverage, and less mutual interference between the adjacent APs, APC (Auto Power Control) could be used to make the AP to scan the other APs transmission power, and then to calculate and control its owner RF transmission power.

5.3.2 Configuration and Recommendation

APC configuration is similar to ACS, which has been described in 5.1.2.

APC could be turned ON/OFF separately on 2.4GHz or 5GHz

5.4 Load Balancing

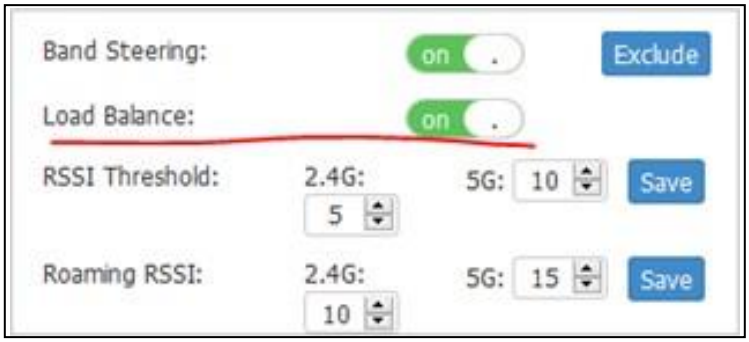
5.4.1 Feature description

Load balancing is used to make the wireless clients could be associated to the AP with good performance, by checking the number clients associated, and uplink RSSI info synchronized between the neighbor APs.

It’s balancing the clients working on the same radio band.

5.4.2 Configuration and Recommendation

The “load balancing” could be activated from “**WEB UI** -> **Wireless**” page as below:



5.5 Band Steering

5.5.1 Feature description

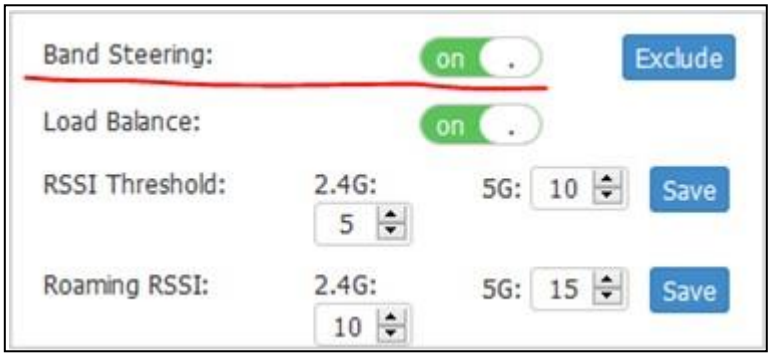
Dual-band devices could be associated with the AP either in 2.4GHz or 5GHz. “Band Steering” feature is able to help this kind of devices to be associated on a better radio band, which is based on:

- RSSI in 5GHz radio.
- RF utilization of the channel of each radio band.
- Number of stations on the radio
- The difference of the stations on the two radio bands.

The band steering feature is handled during “Pre-association” phase.

5.5.2 Configuration and Recommendation

The “Band Steering” could be activated from “**WEB UI** -> **Wireless**” page as below:



5.6 Mesh Network

5.6.1 Feature description

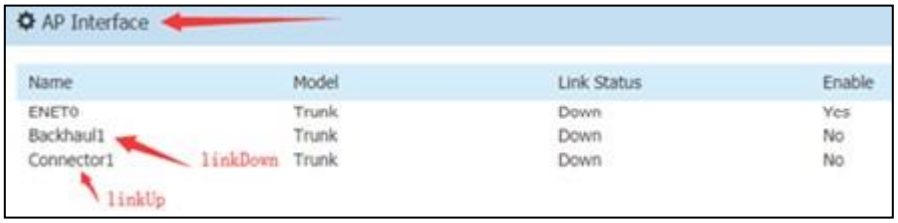
Mesh is a mode for connecting AP s over the air. In previous versions of Neptune and Uranus, different APs were supported to form mesh. Bridge can be regarded as a special mesh network (also through wireless connection, but not Release the wireless signal, just for better data transmission).

The new function in the Saturn project is display of the topology which only supported by OVE&OVC (just for mesh AP). User can see the root icon, mesh link, and AP basic information in the topology. In the bridge AP page, SSH, AP WEB, and WEB certificate are added to facilitate the management of the bridge AP.

5.6.2 Configuration and Recommendation

No matter which mode the AP worked, we should go to the AP UI firstly.

In AP WEB, Network -> AP Interface



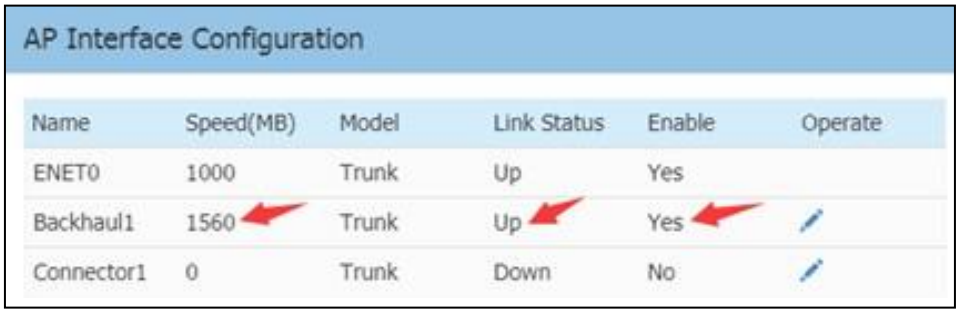
You will see two identical MESH configuration buttons and click on any one.

The MESH configuration page is as follows

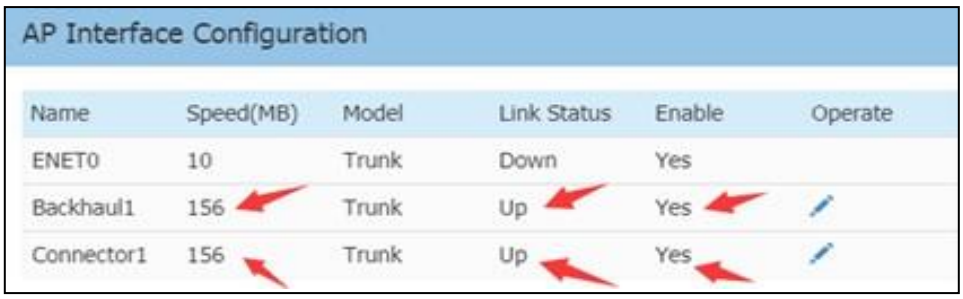
Note:

In the mesh or bridge network user must keep the mesh SSID ,Band and Passphrase is the same between all the APs
In the mesh or bridge network there must have at least one root node

If it is a root node, only the Backhaul interface is enabled. It is normal if the speed is not zero after about one minute. If it is a non-root node, both the Backhaul and Connector interfaces are enabled. And if the MESH network is established, the speed of Connector interface will be not zero

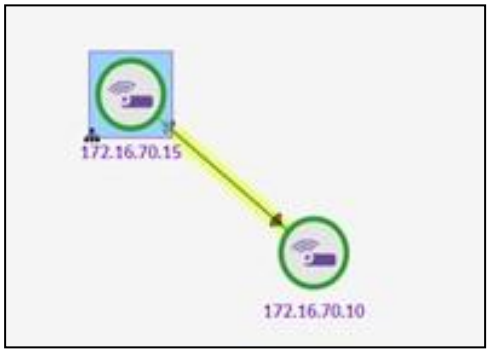


ROOT AP



NON-ROOT AP

If the MESH network is established, and the AP mode is OV (OVE & OVC), you can see the topology page as follows.
Network --> TOPOLOGY --> AP GROUP
The root AP will have a root icon, and the upper node from the AP will use a wirelessly connected symbol. Select link->mesh link will only display mesh link



If the bridge network is established, and the AP mode is OV (OVE or OVC), you can see the bridge AP page as follows
Network →AP Registration →Access Points → Bridge AP
If the bridge AP is up, in the default configuration, you can edit the SSH, AP WEB, WEB Certification, the default is off.
You can also choose one AP or more APs to edit. (Click the edit button). And you can choose AP to Apply Default Configuration

5.6.3 Restrictions for Mesh network

- The mesh AP directly connects up to 8 slave APs, and the chain is up to 4 hops and the max AP number is up to 16 APs in a mesh network.
- The WLAN limits is 5 with single frequency on mesh AP. If AP works in bridge mode, it will not broadcast wireless signals.
- Users can only change the channel of root AP
- In the topology page, if mesh APs in a group, you can see the topology, in different groups, there will be an external flag seeing the topology in the physical topology.
- Bridge AP doesn't need a license in OVE, but license is required in OVC

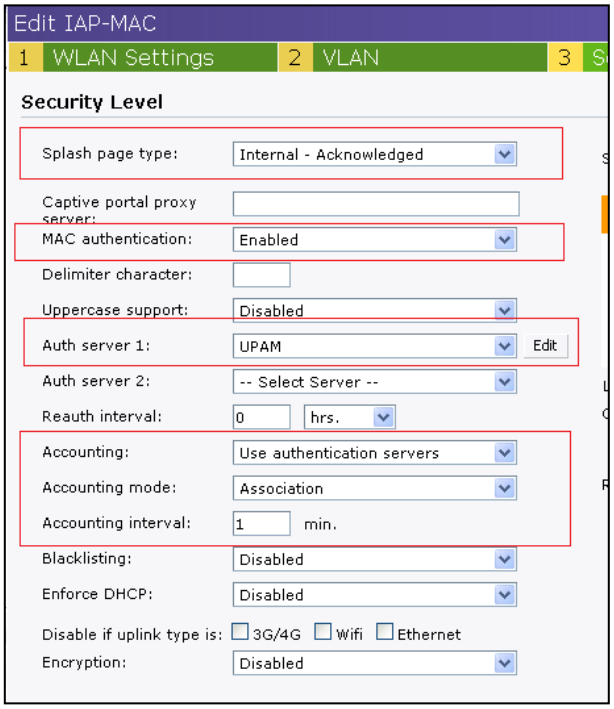
5.7 Aruba AP integration with UPAM

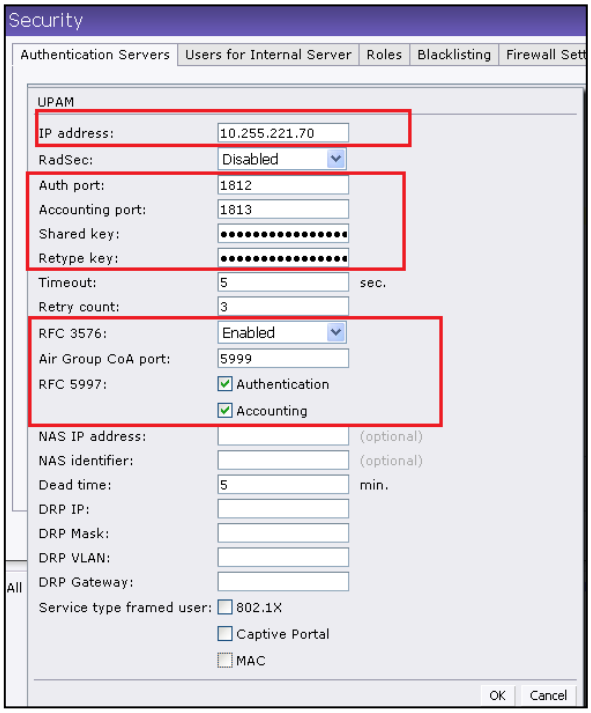
5.7.1 Feature description

UPAM can be as external authentication radius server for Aruba AP, supporting Aruba APs (Instant + Controller mode)

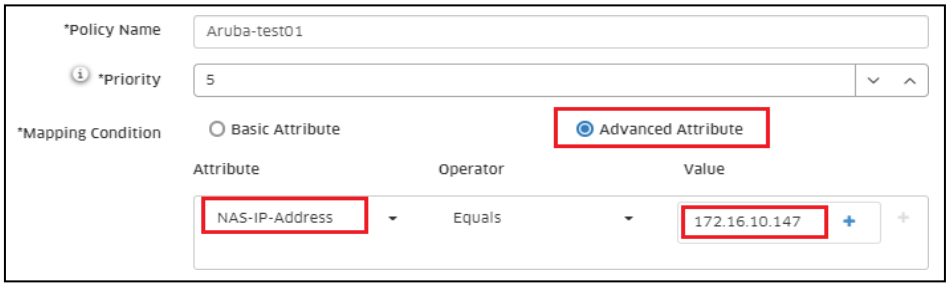
5.7.2 Configuration and Recommendation

This topic will introduce Pure MAC authentication, Pure 802.1x authentication, MAC + Portal (BYOD/GUEST) authentication with Aruba AP, which work mode is instant.
Test Aruba AP: APIN0334 (version 6.5.3.2)
Pure MAC authentication
Configurations on Aruba AP:





UPAM aspect configurations:

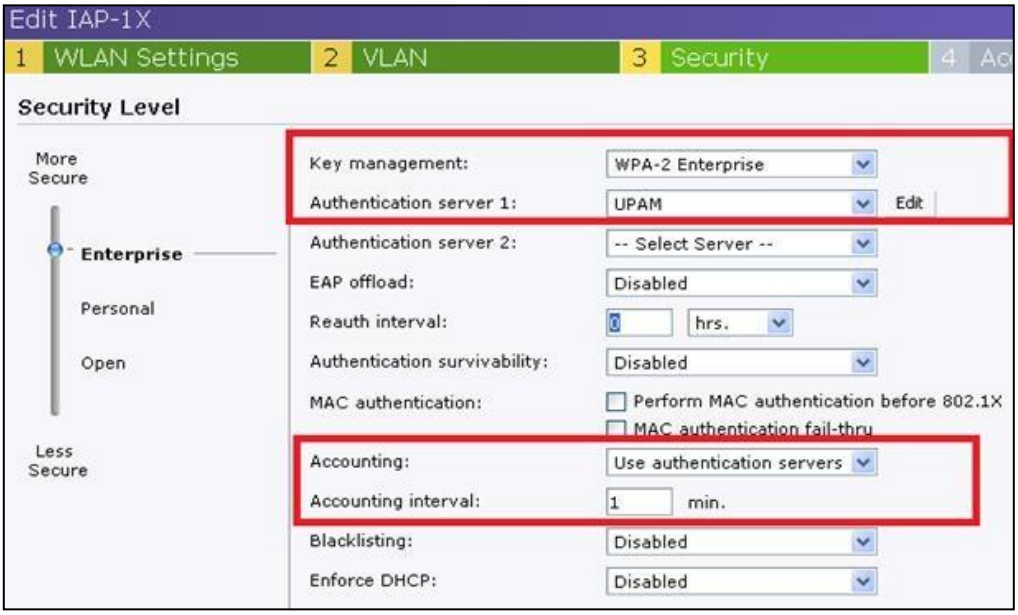


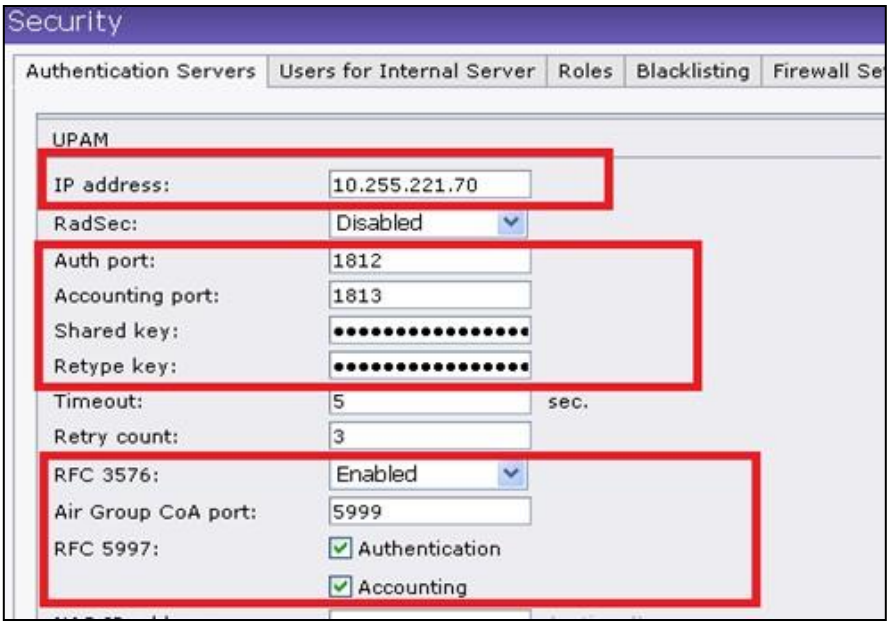
Note:

- *If you want to have an authentication for Aruba or other vendors, you should select Mapping Condition to Advanced Attribute.*
- *Basic Attribute is just for Stellar AP.*
- *Please select the right attribute which match the one sent by Aruba AP*
- *Do not forget to add company property account.*

Pure 802.1x authentication

Configurations on Aruba AP:



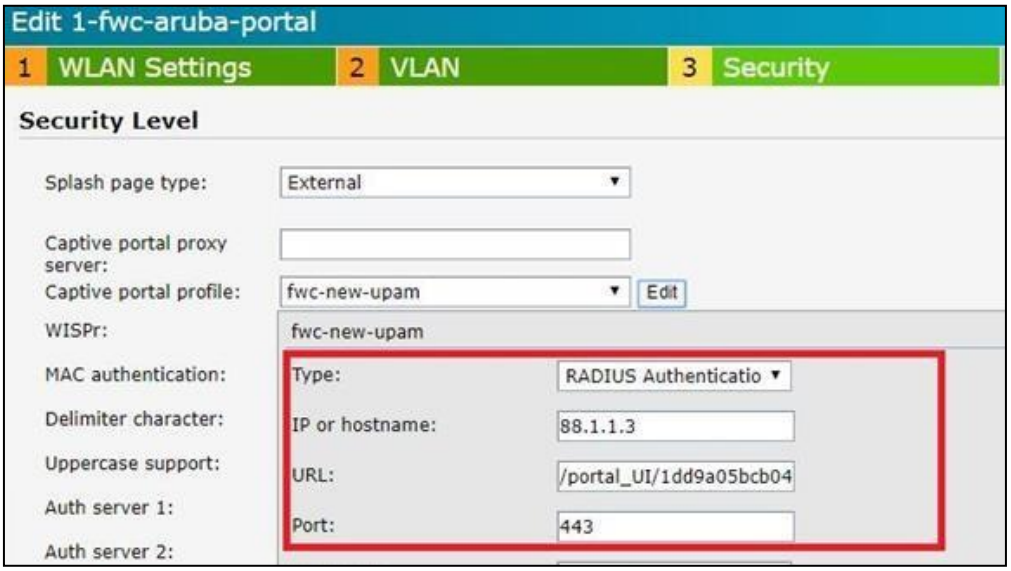


Configurations on UPAM are the same as above about MAC authentication and also need to add Employee account.

MAC + Portal authentication

Configurations on Aruba AP:

A、Security Level Configurations

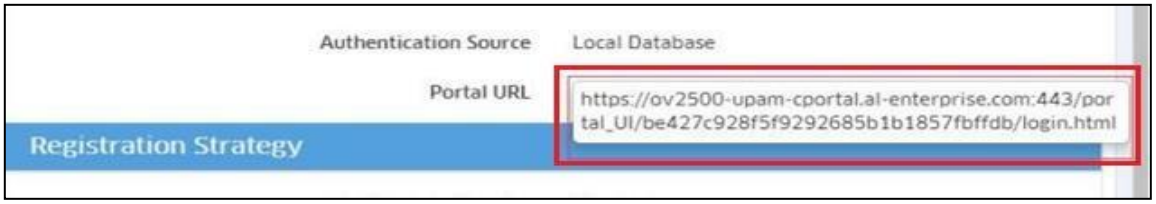


B、Captive Portal profile Configurations

Note:

Please ensure the URL is consistent with UPAM GUEST/BYOD access strategy, you can get it as below steps:

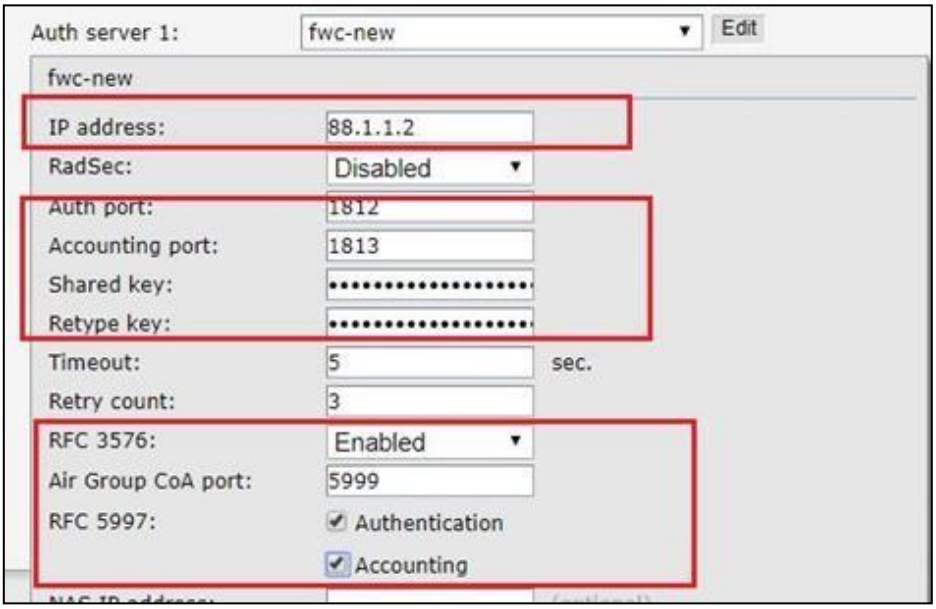
Go to "UPAM" → " BYOD ACCESS" → " BYOD Access Strategy" and select the related strategy,



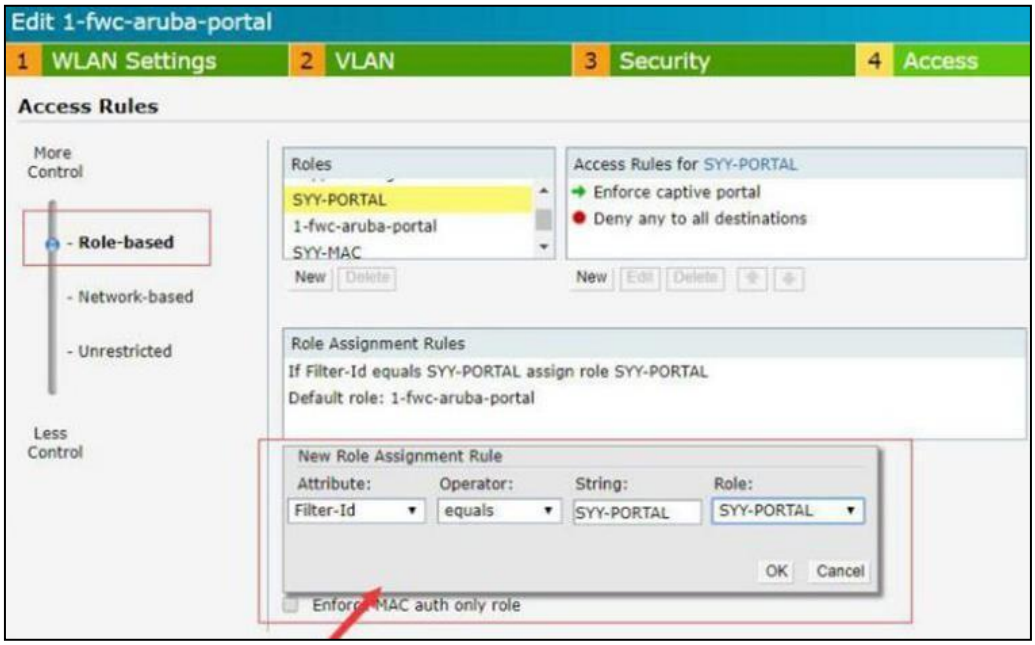
For example:

https://ov2500-upam-cportal.al-enterprise.com:443/portal_UI/be427c928f5f9292685b1b1857fbffdb/login.html

Just input the content in red font, and please note that every BYOD or GUEST access strategy own unique URL.



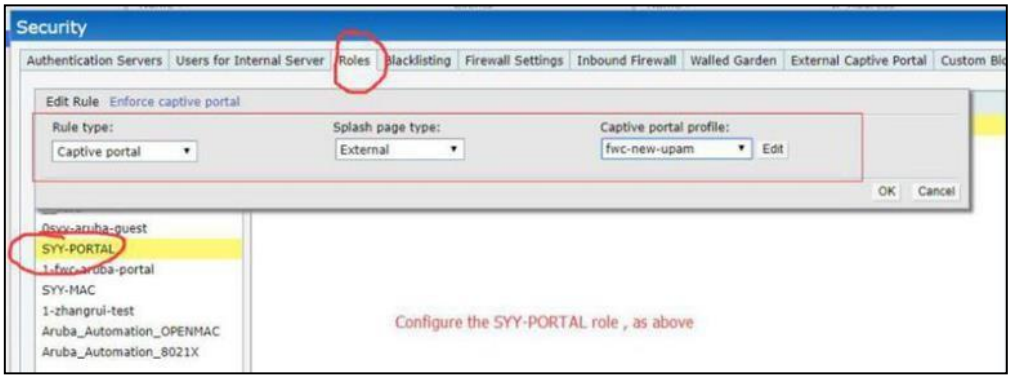
C、Auth Server Configurations(Base on Security Level)



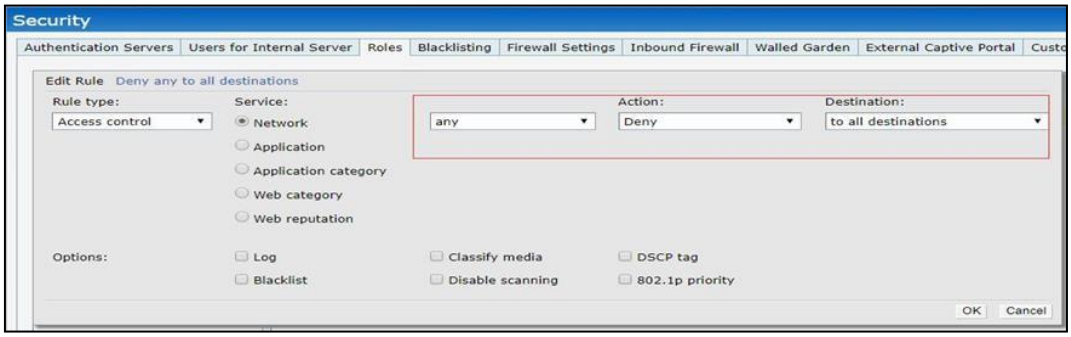
D、Access Rules setting

Note:

Creat a new role assignment, just like above, there is a role named ‘SYY-PORTAL’, and also you need to configure the role to UPAM and let UPAM assign the role to Aruba AP.



E、Roles setting



F、Roles setting

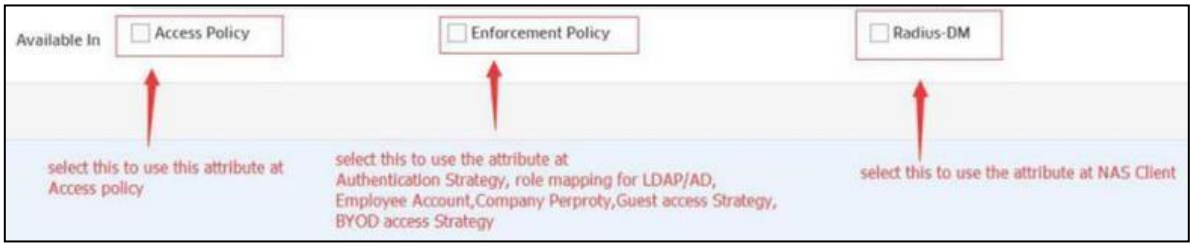
Configurations on UPAM are the same as above about MAC authenticationNote

:

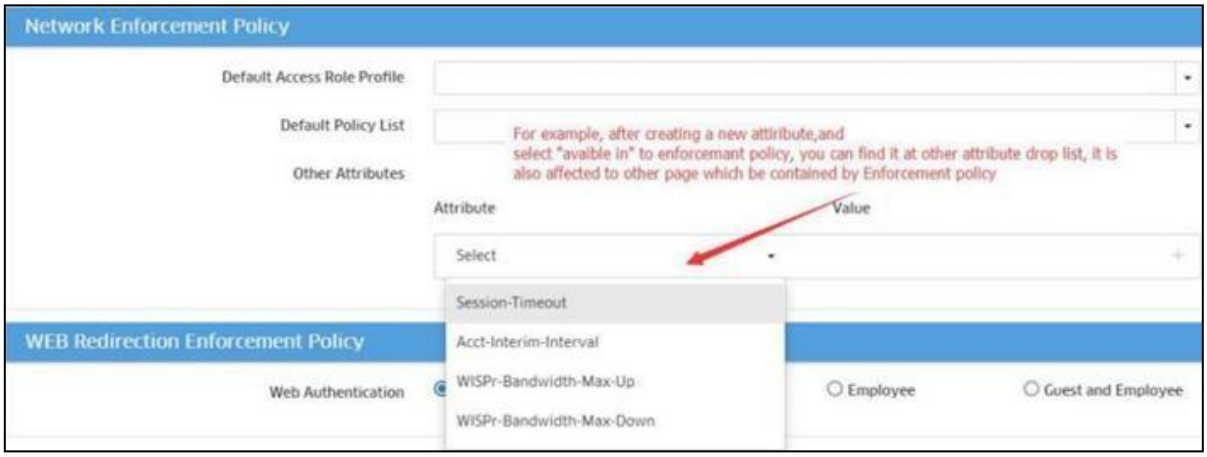
Default ARP in Authentication strategy and Fixed ARP in GUEST access strategy need also correspondent with Aruba AP.

5.7.3 Extra enhancement

UPAM can also have a flexible structure to every vendor besides Aruba and Alcatel AP. There is another new configurati on page to be shown below(*UPAM>Settings>Radius Attribute Dictionary*). Other Vendor's AP need be verified if needed.



Follow configurations on UPAM>Authentication>Authentication Strategy:



Radius Attribute Dictionary can customize attribute, when you complete to create, do not forget to click “sync to RADIUS” or else it will not work.

For Alcatel or Aruba AP, actually you do not need to create a new attribute; there are many of default attributes to be created beforehand.

5.8 Data Quota

5.8.1 Feature description

Today with Guest Access Strategy we can define session timeout. Once the session duration is completed, the user is kicked off and is required to re-authenticate. The user can connect back until account validity period is valid.

However, the admin can further control when to allow the clients back again into the network with or without re-authentication or are forced to watch a promotional video or is redirected to take a survey.

Data Quota is only supported on OVE & OVC mode. When client connects to the WLAN which type is Guest Network (Open & Captive Portal), it will start calculated data consumed. When client visits the website in walled garden lists, it will consume the data quota too.

In Guest Access Strategy, part of post portal authentication after Session Timeout interval provide an option to specify “Data usage quota” in MB, optional “Quota reached redirection URL”.

5.8.2 Configuration and Recommendation

When create a new SSID, many configuration should be changed.

Global Configuration

Batch Creation->Configure the Batch Creation Account in the global configuration.

The unit of data quota on Global Configuration page is MB.

When an account is created, the data quota in the account defaults to the data quota configured in Global Configure/Service Level.

Guest Access Strategy Configuration

In the Guest Access Strategy page, configure “Data Quota Status”, "Quota Exhausted URL" at the post portal authentication Enforcement module. When create a new SSID, new Guest Access Strategy will be created by default.

The default value of “Data Quota Status” is “Disabled”.

The Quota Exhausted URL is a string which prefix is “http://” or “https://”. It can be set null. If not be configured, when the data quota of user consumed over, will redirect to login page. If configured by operator, will redirect to the configured Quota Exhausted URL page.

If the data Quota reaches zero, the failure information will be directly returned, prompting to log in with another account or contacting the administrator to increase the traffic limit.

- Access Role Profile Configuration

In Home ->Unified Access ->Unified Profile ->Device Config ->Access Role Profile. Fill in a URL that must be added to the whitelist and redirected to the URL when the account usage reaches the limitation.

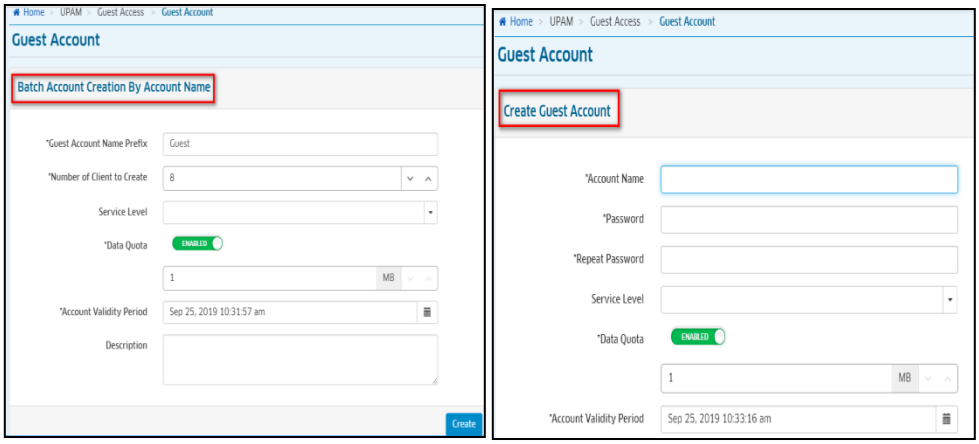
- Guest Account Configuration

The Guest account will add the data quota attribute.

When adding an account, the corresponding data quota will be obtained according to the Global Configure corresponding to the visitor account.

After the addition is successful, the administrator can also modify the data quota of the account.

Batch creation/Self-Registration Account /One



Admin can see the remainder data quota of the account in account detail page. Extend new data quota you want.

- Guest Device Configuration

The guest account authentication process changes, check whether the device has a remember record

If the device does not have remembered record, push the corresponding portal page.

If the device has remembered record, check the data Quota of the account according to the account information in the remember device.

If the data Quota doesn’t reach zero, the authentication is passed.

If the data Quota reaches zero,

If the Quota Exhausted URL is configured in the guest Access Strategy, the URL is pushed
If the Quota Exhausted URL is not configured, the portal URL is pushed.
If want to change account, check if device is remembered. If remembered, delete this device.

5.9 Display RF/Static AP Neighbor ship in OV Heat-map

5.9.1 Feature description

In AWOS 3.0.4 and OVC 2.0 and later build, it supports to statically add AP neighbor and display the list of neighbors (discovered over air + static).

It should display the AP neighbors in heat-map when a given AP is selected, highlight the corresponding neighboring APs.

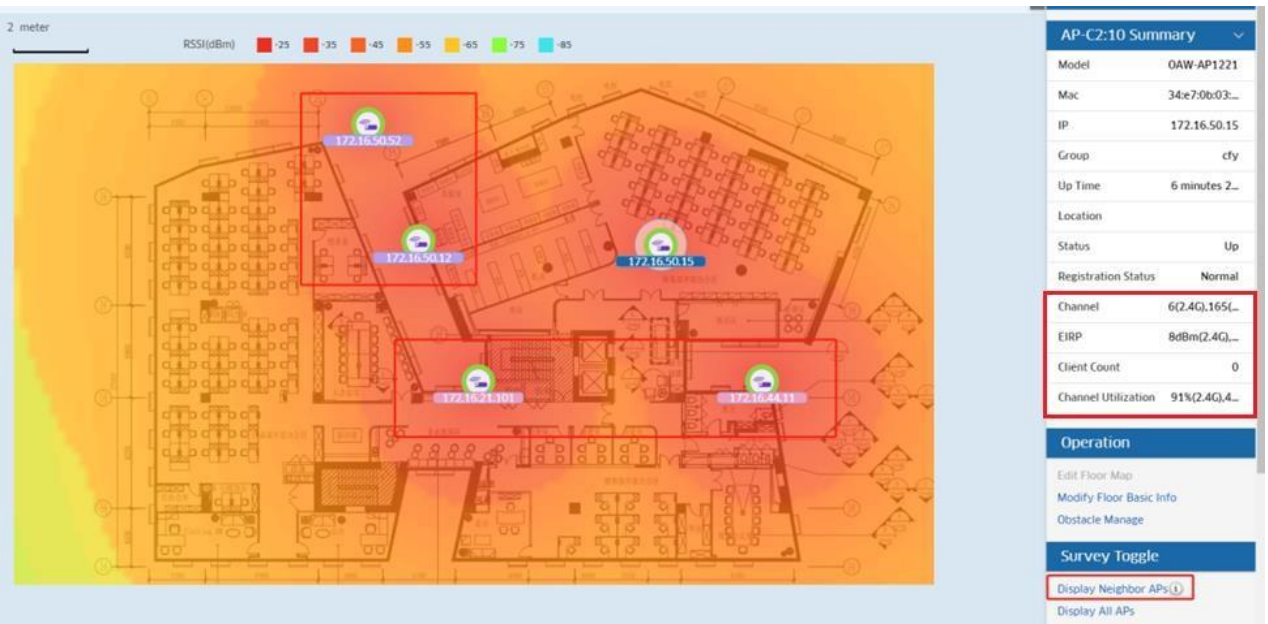
Use different color to show static Vs over the air discovered neighbor.

For each AP selected also show number of clients associated, channel in use (2.4GHz/5GHz), corresponding utilization, RSSI and Radio Tx Power (2.4GHz/5GHz) (inclusive of antenna gain).

5.9.2 Configuration and Recommendation

Display Neighbor APs

Home->WLAN->Heat Map->Display Neighbor APs, the APs with pink and purple background color are the AP’s neighbor APs which with blue background color.



Then click ‘Display All APs’ to display all the APs in heat-map.

- Display RF in heat-map

Click one AP in heat-map, the RF information will display on right. It will show Channel/EIRP/Client count/Channel Utilization of AP.

5.9.3 Notes and restrictions

There must have SSID in AP to display heat-map and display RF in heat-map.

An icon with purple text background color represents static neighbor AP, and a pink color represents an automatically discovery neighbor AP.

The text background color is purple when an AP is both static neighbor AP and automatically discovery neighbor AP.

Clients count includes wireless and wired clients on AP.

5.10 Wireless user, allow easy onboarding of headless Wi-Fi device

5.10.1 Feature description

When we use BYOD-certified WLAN, because of the need to pass Portal authentication, it is difficult to use this WLAN for devices that cannot open web pages for authentication, such as game consoles and wireless printers.

Now designed such a function, after BYOD authentication can open a configuration page to configure the remembered device, if the Mac address of the configured device corresponds to the actual device address, then this device does not need to open the portal page again, but This WLAN can be used directly.

5.10.2 Configuration and Recommendation

Just add the required device to the BYOD self-service page, no additional configuration required.

BYOD self service Configuration

After finished BYOD authentication, click the “Add Remember Device” to jump to the BYOD self-service page and configure the corresponding device information.

Devices added in this way use the account used to log in to the BYOD self-service page.

5.11 IPV6

5.11.1 Feature description

IPv6 protocol enables next generation large-scale IP networks by supporting addresses that are 128 bits long. This allows 2*128 possible addresses (compared to 2*32 possible IPv4 addresses).

It supports IPv6 client authentication, management & policy control, Authentication (MAC based, Captive Portal, 802.1x).

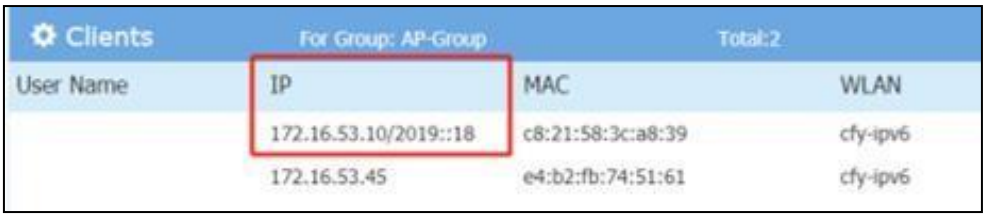
IPv6 client information management – AP UI components where we display Client IP information needs to support IPv6 and the display should be in standard IPv6 (Locator, WLAN Client list, UPAM user and device DB, logging).

In the 306 program ,the IPv6 feature only supports the client management. The AP only pass through the packages about IPv6.

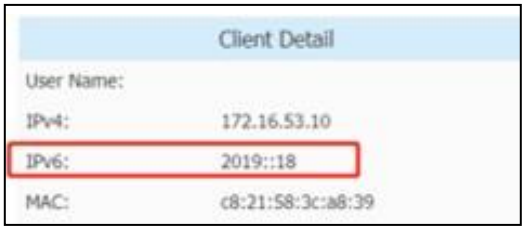
5.11.2 Configuration and Recommendation

Clients IP

1. Cluster main web->Clients, It display clients’ IPV6 address.



2. Cluster main web->Clients->Clients Information, It display clients’ IPV6 address.



3. Cluster main web->AP->AP Configuration->AP UI, It display client’s IPV6 address.

Walled Garden

Cluster main web->Access->Black List& White List->Walled Garden, you can configure IPV6 address for it.

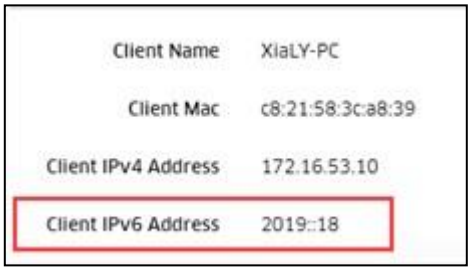
ACL

Cluster main web->Access->ACL->ACL Configuration->Add/Edit ACL, you can configure IPV6 address for source IP and destination IP.

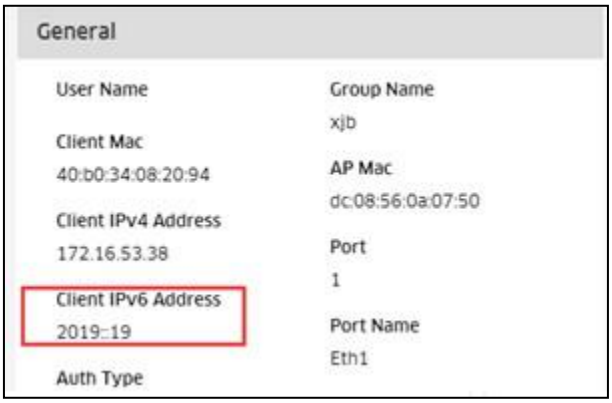
OVC & OVE

It needs set up the DHCPv6 server in the L3 switch and the DNS v6 server. Then make sure the environment is normal. On the OV page, you need only specify the VLAN-ID of the DHCPv6 server.

Go to “Home - WLAN - Client-Client List -Wireless Client List”. It will display the wireless client IPv6 address



Go to “Home - WLAN - Client-Client List -Wired Client List”:



IPV6 are also supported on the below configuration filed:

- Locator configuration
- Policy/ACL configuration
- White-List configuration

5.11.3 Notes & restrictions

Starting IP and ending IP in walled garden must be same IP type.

Source IP and destination IP in ACL must be same IP type.

5.12 UPAM Guest Strategy Enhancements

5.12.1 Feature description

Now we need to have more requirements for Guest authentication, including bulk creation of users, global configuration, service level and extend account functions. Now we have integrated these requirements to provide this function.

5.12.2 Configuration and Recommendation

After creating a new SSID (open guest mode), we can configure these items.

- Guest Global Configuration

  We can configure the following functions on the Global Configuration page.

  - ✓ Create a switch for the guest user in batches.
  - ✓ Guest account global configuration of account validity period and device expiration date.
  - ✓ Data Quota global configuration.
  - ✓ Service level switch and configuration item.
- Batch Creation Configuration

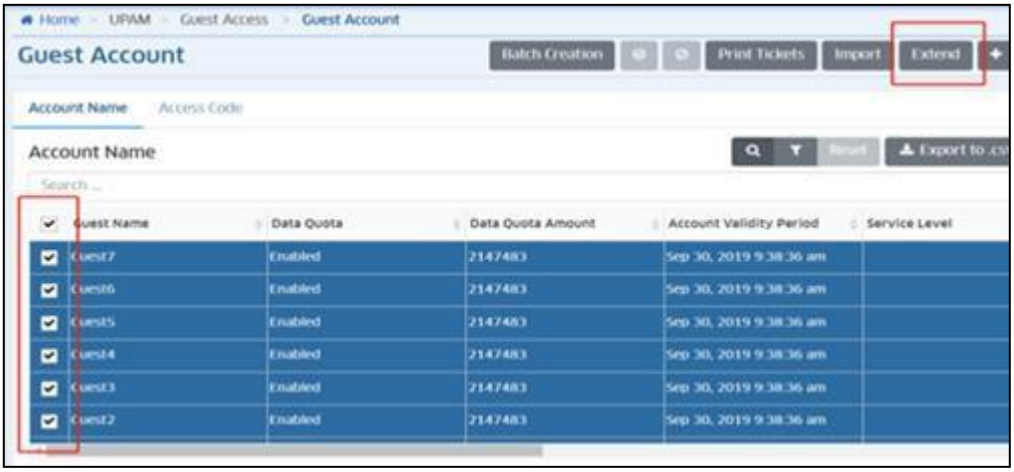
Need to open the switch in the global configuration page, the default prefix configured in the global configuration will be displayed on the page.

- Open the Batch Creation Account in the global configuration.

The Batch Account Creation by Account Name page allows you to create a guest account in batches and select a service level.

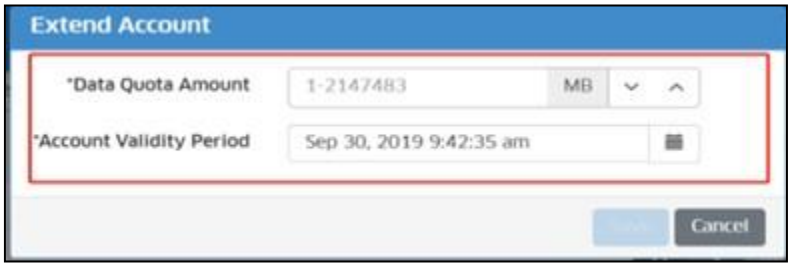
- Extend Configuration

First we need to create an account first, create it in batches or create it separately. Then select the account that needs to be extended, click the extend button at the top right.



Extend Configuration-1

- This will allow you to configure the new account expiration date and the Data Quota value.



Extend Configuration-2

5.13 WPA3

5.13.1 Feature description

WPA3 is a new type of encryption technology. WPA3 Encryption Type is available in both personal and enterprise Security Levels.

5.13.2 Configuration and Recommendation

- Cluster mode

There are 3 scenarios in cluster mode to create WLAN of wpa3 type.

A. Created in the setup wizard:

The factory AP enters the setup wizard page, according to the wizard, you can create wlan3 type WLAN. Such as creating wpa3-personal:

B. Created in the main page:

Go to the main page and click the "New" button to create

- ✓ wpa3-personal
- ✓ Both(wpa2&wpa3)
- ✓ wpa3-enterprise(CNSA disable)

- ✓ wpa3-enterprise(CNSA enable)

C. Created in the WLAN list:

Click WLAN to enter the WLAN configuration page, and you can create a wpa3 type WLAN.

Such as creating wpa3-personal:

- OV mode

There are 2 scenarios in OVE&OVC mode to create wlan of wpa3 type.

1. Created in the SSIDs page:
   - ✓ Go to the "Home-->WLAN-->SSIDs" page.
   - ✓ Go to the "Create SSID" page
   - ✓ As shown:
   - ✓ WLAN issued
2. Created in the WLAN Service (Expert) page:

   Created in the "Home-->Unified Access-->Unified Profile-->Template-->WLAN Service (Expert)" page, the same steps as other types of WLAN.

5.13.3 Notes & Restrictions

- The support of each AP for the WPA3 encryption type is as follows:

	Personal	Enterprise
AP	WPA3_SAE_AES/wpa3-personal	WPA3_PSK_SAE_AES/Both(wa2&wpa3)
AP1101	support	support
AP1201H	support	support
AP1201	support	support
AP1221	support	support
AP1231	support	support
AP1251	support	support

- OAW-AP1101 full band, OAW-AP1201H 2.4G band do not support WPA3_AES256 authentication; If the AP can’t support WPA3 feature for CNSA, AP will set wpa3-enterprise CNSA disable or WPA3_AES.
- WPA3 roaming and PMF STATUS support:
- WPA3_SAE_AES/wpa3-personal: WPA3 with AES encryption using a pre-shared key, which only allow WPA3 capable client accessing.
- WPA3_PSK_SAE_AES/Both (wpa2&wpa3):WPA3 and WPA2 mixed mode, which allow both WPA3 capable client as well as only WPA2 capable client accessing.
- WPA3_AES256/wpa3-enterprise (CNSA enable): only allow WPA3 capable client accessing.
- WPA3_AES/wpa3-enterprise (CNSA disable): supports wpa3/wpa2 device access.
- Please check the version when IOS device cannot access wpa3-both (wpa2&wpa3)/WPA3_PSK_SAE_AES. The system version before iPhone IOS12.2 does not support the encryption type.

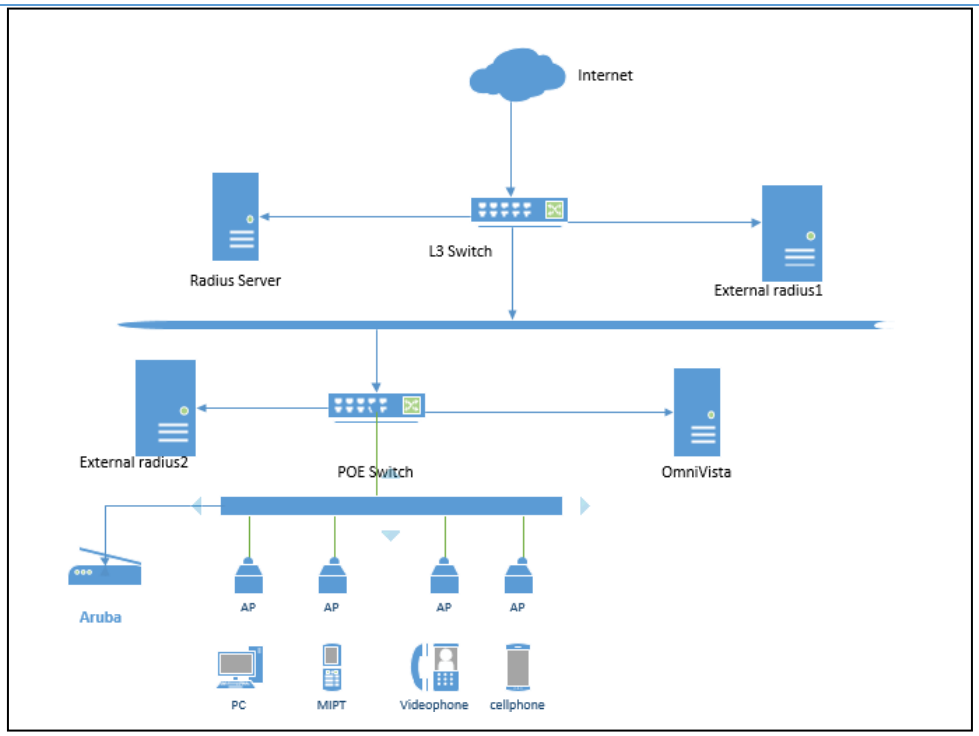
5.14 Multiple External Radius

5.14.1 Feature description

When UPAM is used as proxy for authentication, we are limited to a single External Radius server. In large universities, it is typical to segregate the radius server between Students & Staff. In Saturn we add this new function to support the requirement and user can add 8 external radiuses at the most.

In order to adapt to other manufacturers AP, we improved the Mapping Condition in access policy, user can select Basic Attribute or Advanced Attribute according to actual needs. For example, if user want to use UPAM as authentication server for Aruba AP, user can select advanced attribute for mapping condition.

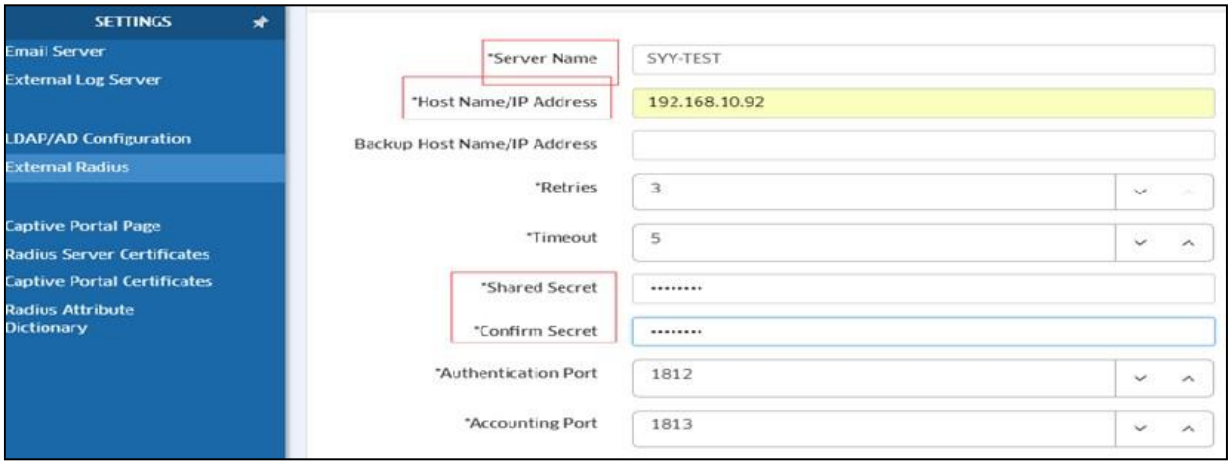
5.14.2 Topology



5.14.3 Configuration and Recommendation

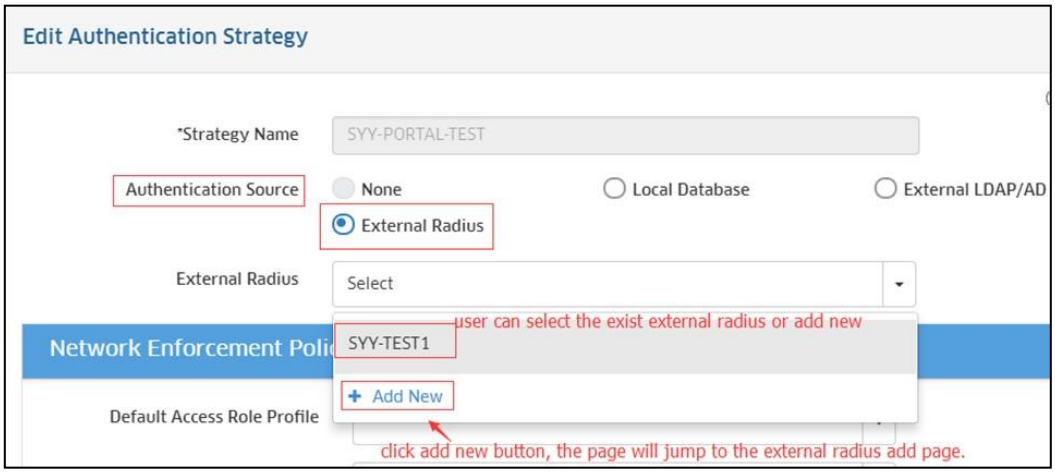
User can add the external radius server following the link: Home->UPAM->Setting->External Radius

Click the add button and input parameters in the new page as required.



For MAC authentication and 802.1x authentication

Create WLAN with SSID and Click the advanced configuration, in the new page, user can select external radius as required.

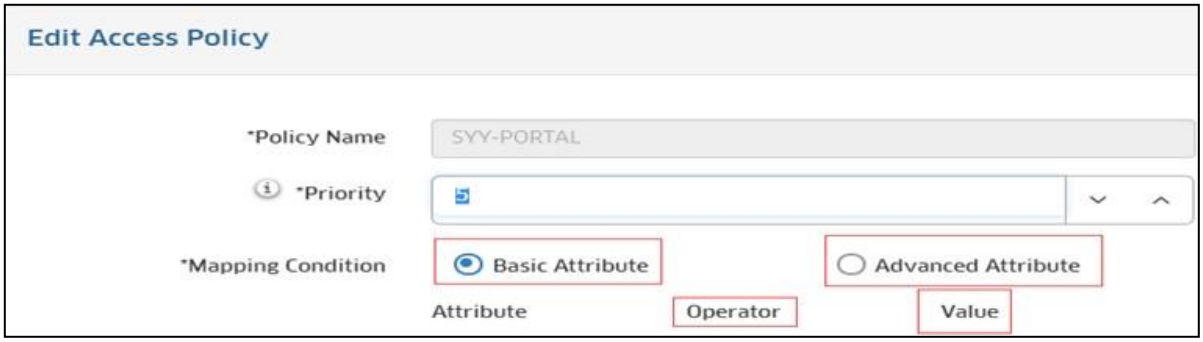


NOTE: if select external radius as MAC auth server, user should add the MAC of client in the server, and the same if select external radius as 802.1X auth server, user should create account for client in the server.

For BYOD authentication, when create a new WLAN as required, user should select an external radius from the list when set External Radius as Authentication Source.

For Mapping condition

In access policy configuration page, we offered more attribute for different Aps shown as following, as for the details, please refer to the help documentation.



If user selects LDAP/AD as auth server, and enable role mapping function, user should add the LDAP/AD server first and then fetch Attribute for LDAP by clicking “Fetch” button, and user can create policy for role mapping.

5.15 AP1201H - trusted tag supported on Ethernet Ports

5.15.1 Feature description

Today with the AP1201H we are able to get the phone into VLAN 1675 and we are able to go through in VLAN 1616. The Access Classification Rule VLAN Tag can be pushed to the AP group. Trust Tag enabled in the Access Authentication Profile of the AP can be seen in the Device Config. So user could implement AP1201H and attach their phone to the PoE port.

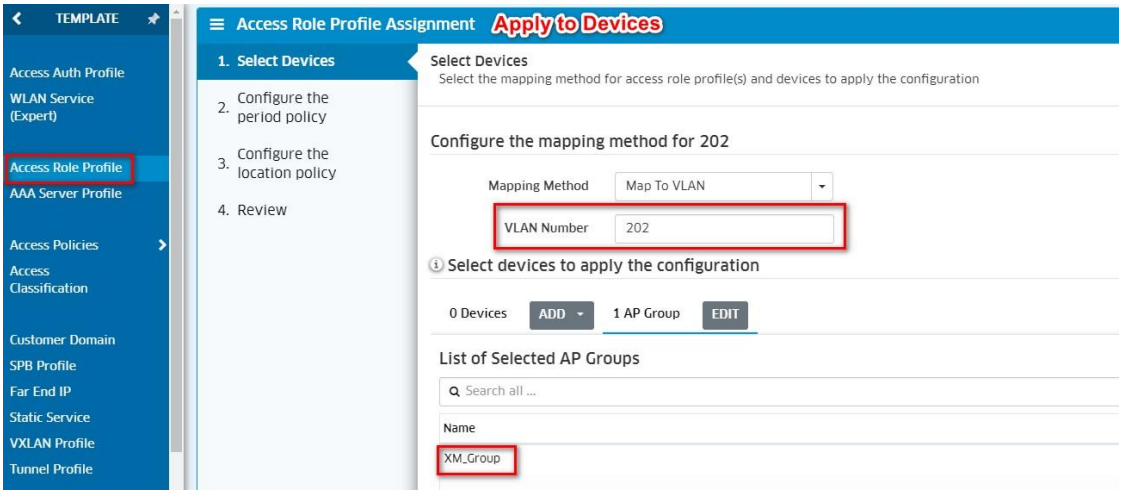
By default, the downlink port is disabled and does not send or receive any package. Each port has its own independent switch, and which can be used when the VLAN id is configured.

5.15.2 Configuration and Recommendation

OVE & OVC vlan id depend on Role. Express vlan id depend on manual input. OVE & OVC tagged vlan depend on AAP. Express tagged vlan depend on manual input.

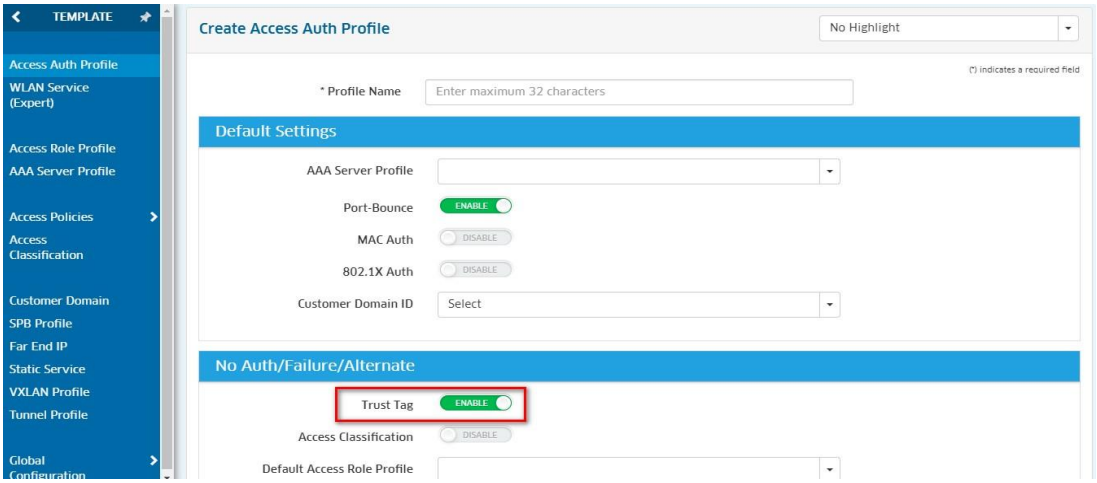
Trust tag Configuration(OVE & OVC)

1) In the Unified Access->Unified Profile->Template->create ARP, Apply to devices.

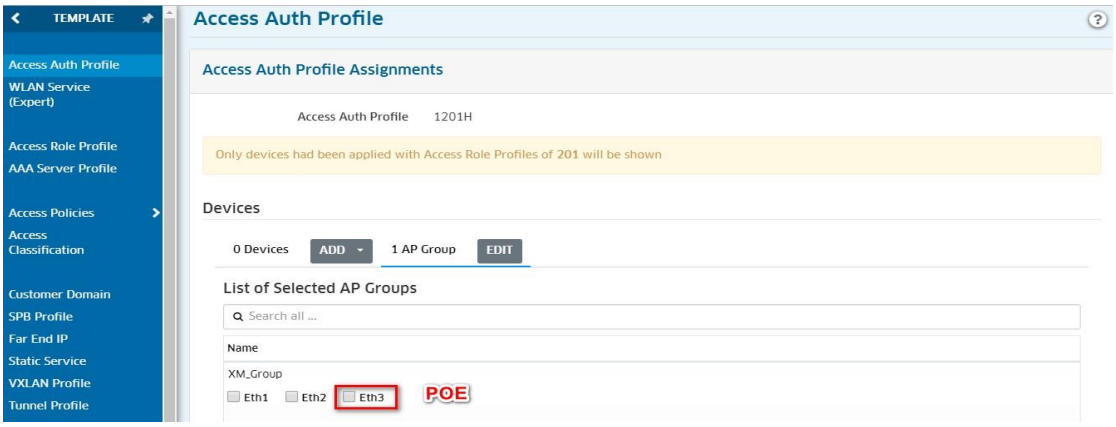


Pic 5.16.3-1 ARP vlan number

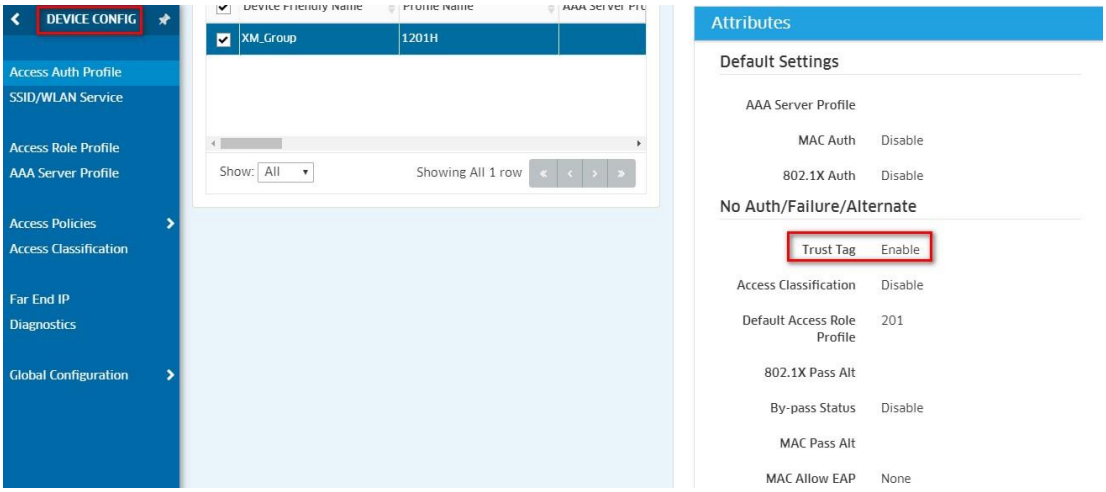
2) In the Unified Access->Unified Profile->Template->AAP, enabled ‘Trust tag’.



Pic 5.16.3-2 trust tag



3) In Home>Unified Access>Unified Profile>Device Config>AAP check



Trust tag configuration (Express mode)

Add the Tagged VLAN attribute to the Network page. The range of tagged VLAN is 2-4090. The max number of tagged VLAN is 16, which divided in “,” . It can be set null. User can create tagged VLAN for each downlink port, and control the function enable or disable. If the downlink port not configure any tagged VLAN, the link port will only forward packets with no VLAN tag.

Pic 5.16.3-5 Express tagged Vlan

With support account check Configuration

Command: cat /var/config/wired.conf

```
support@AP-33:00:~$ cat /var/config/wired.conf
{
        "wired_profile":[
                {
                        "name":"ap211h_Eth1_4096",
                        "board":"ap211h",
                        "model":"OAW-AP1201H",
                        "port":"Eth1",
                        "vlanNumber":4096,
                        "upload":0,
                        "download":0,
                        "enable":"enable",
                        "tagged_vlan":[
                                201,
                                1616
                        ]
                },
                {
                        "name":"ap211h_Eth2_4096",
                        "board":"ap211h",
                        "model":"OAW-AP1201H",
                        "port":"Eth2",
                        "vlanNumber":4096,
                        "upload":0,
                        "download":0,
                        "enable":"enable",
                        "tagged_vlan":[
                                201,
                                1616
                        ]
                },
                {
                        "name":"ap211h_Eth3_4096",
                        "board":"ap211h",
                        "model":"OAW-AP1201H",
                        "port":"Eth3",
                        "vlanNumber":4096,
                        "upload":0,
                        "download":0,
                        "enable":"enable",
                        "tagged_vlan":[
                                201,
                                1616
                        ]
                }
        ]
}
```

Pic 5.16.3-6 support - tagged vlan

5.16 Range of TX Power

5.16.1 Feature description

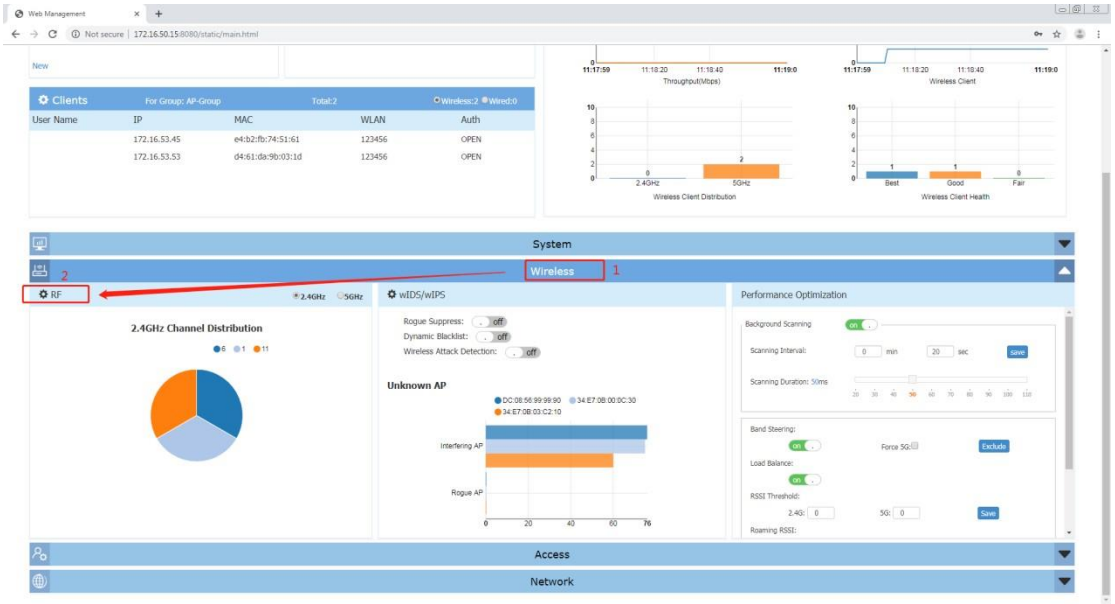
Customers demand that they must be able to control the range of allowed TX power.

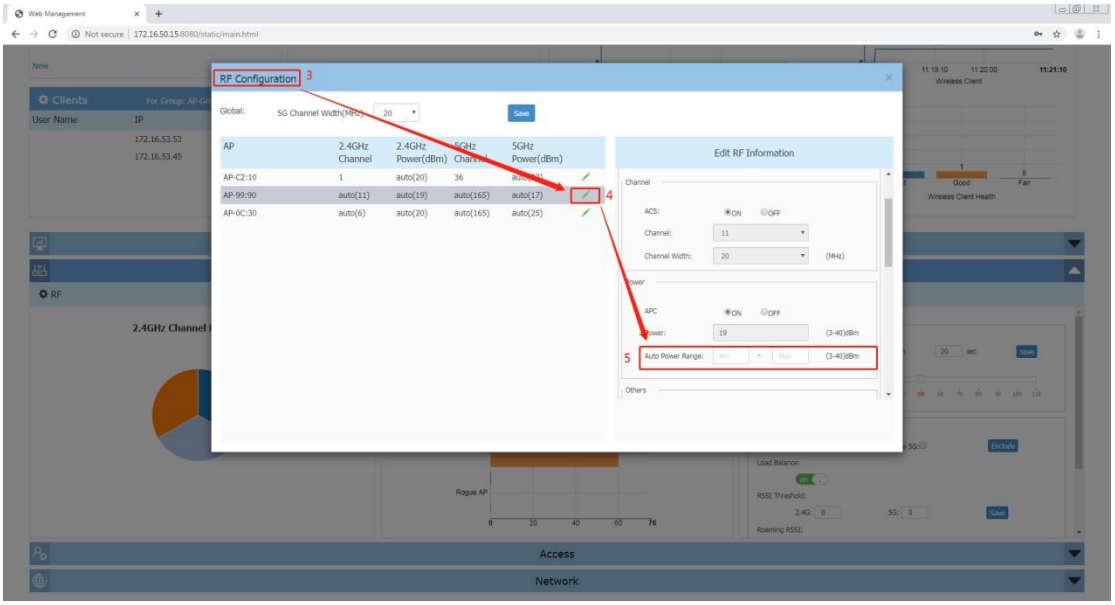
- Today in OV under RF Power Setting option pull down there is Min and Max. This requires the user to statically select Min or Max. Doesn’t make much sense but we can leave it as is for now.
- When Power Setting is Auto, allow configuring a range of TX power per band (min & max). Note the user may specify either one of them or both.
- The auto transmit power algorithm then must select TX power of the AP within the minimum and maximum specified.
- If Min is not specified, the algorithm to select the minimum TX power within compliance
- If Max is not specified, the algorithm to select the maximum TX power within compliance
- Cluster/OVE/OVC mode all support the feature.

5.16.2 Configuration and Recommendation

Cluster mode

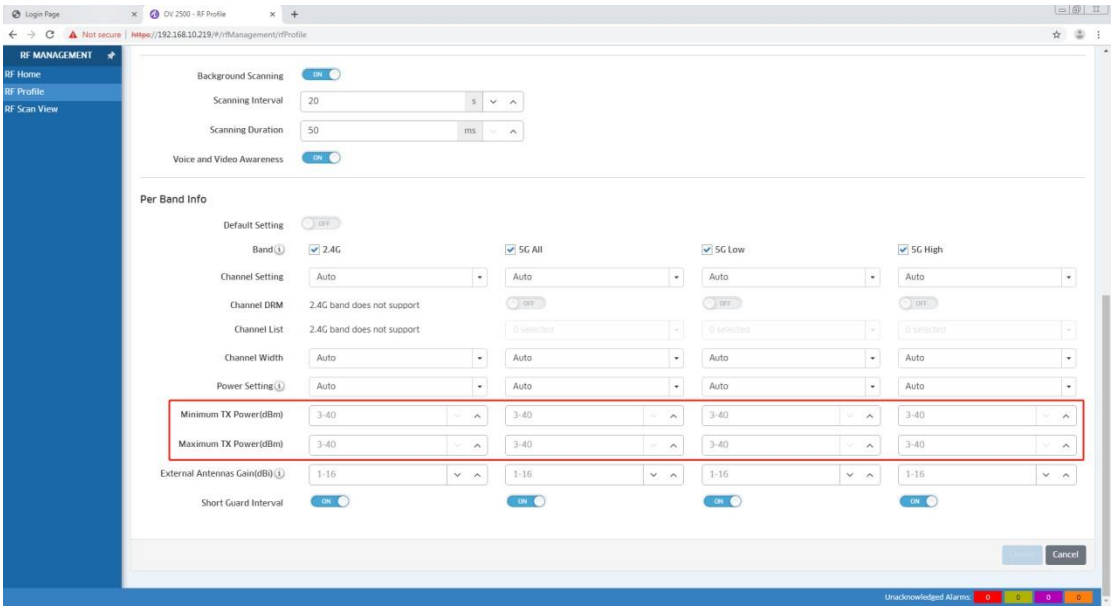
In Cluster main WEB, Wireless-> RF->RF Configuration-> Edit->Auto Power Range, you can configure 2.4G/5G auto power range. The APC must be ON state.

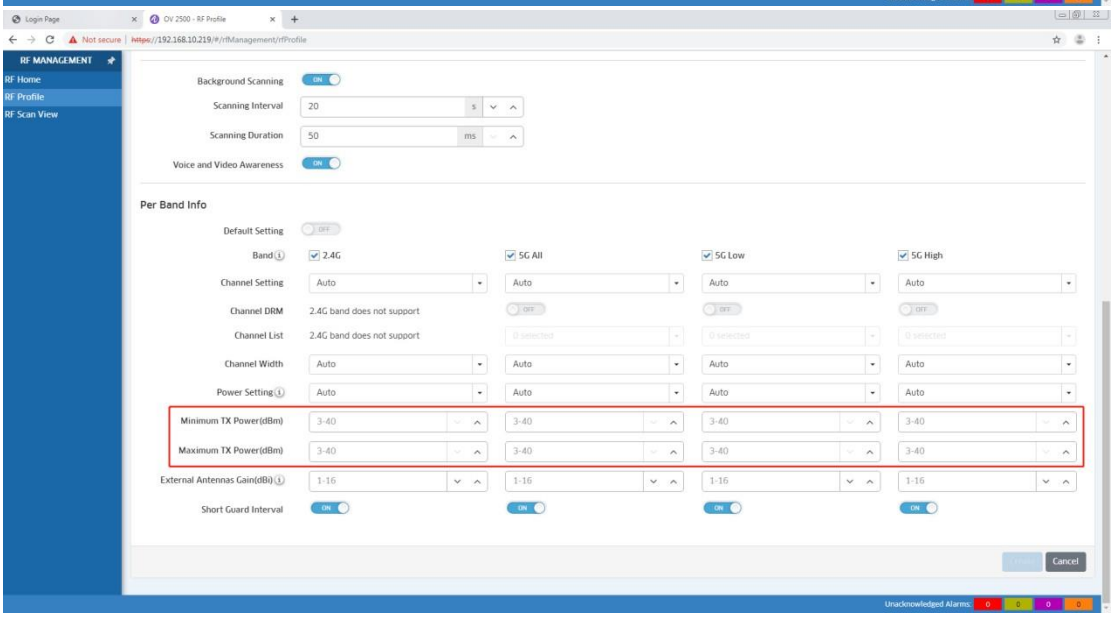




OV mode (OVE&OVC)

Home->WLAN->RF Management->RF Profile->Add New RF Profile/Edit RF Profiles





5.16.3 Notes

- The APC must be ON state in Cluster mode.
- The Power Setting must choice ‘Auto’ in OVE and OVC mode.
- The range of Minimum TX Power is 3-40, and the range of Maximum TX Power is 3-40 in cluster and OV web. The Minimum TX Power can not be greater than Maximum TX Power.
- The AP will choice TX power in the range it supports when you configure minimum and maximum power in web not match the range AP supports.

5.17 Client detail roaming & RSSI history

5.17.1 Feature description

In today's network environment, we need to know the client's roaming records and changes in RSSI values to optimize the existing network environment.

In the client list we support viewing roaming records and RSSI history so that we can observe the client's connection behavior for a client.

5.17.2 Topology

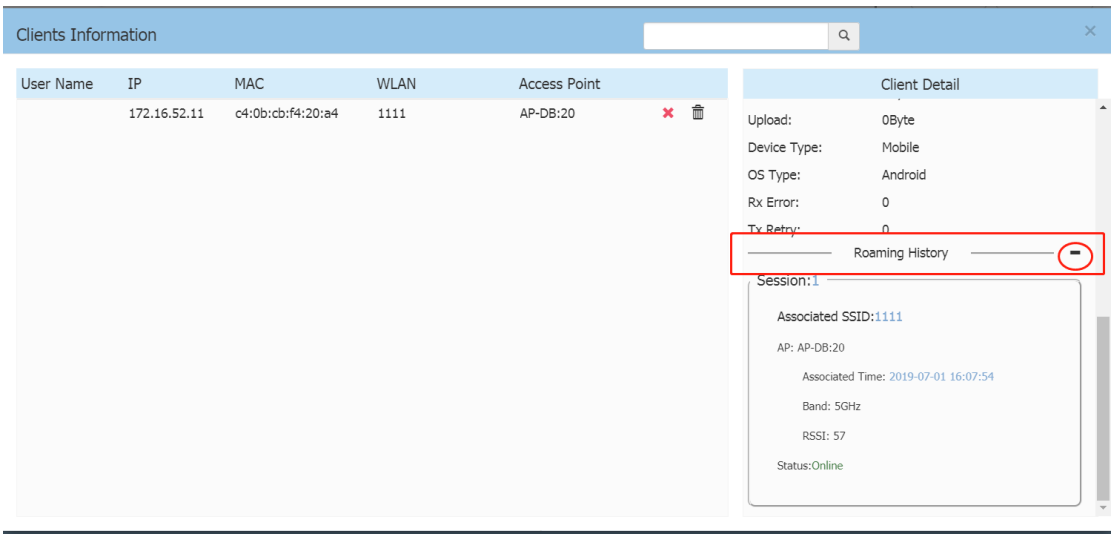
Same topology as in section 5.9.2.

5.17.3 Configuration and Recommendation

On the client list page, you can view the roaming history and RSSI history of a client. The cluster mode does not need to be configured. The OV mode needs to be configured to view roaming records.

Cluster Configuration

In Cluster mode, we don't need other configuration, we can view the client's roaming record and RSSI history in the client list.



Pic 5.18.3-1 Client detail roaming & RSSI history

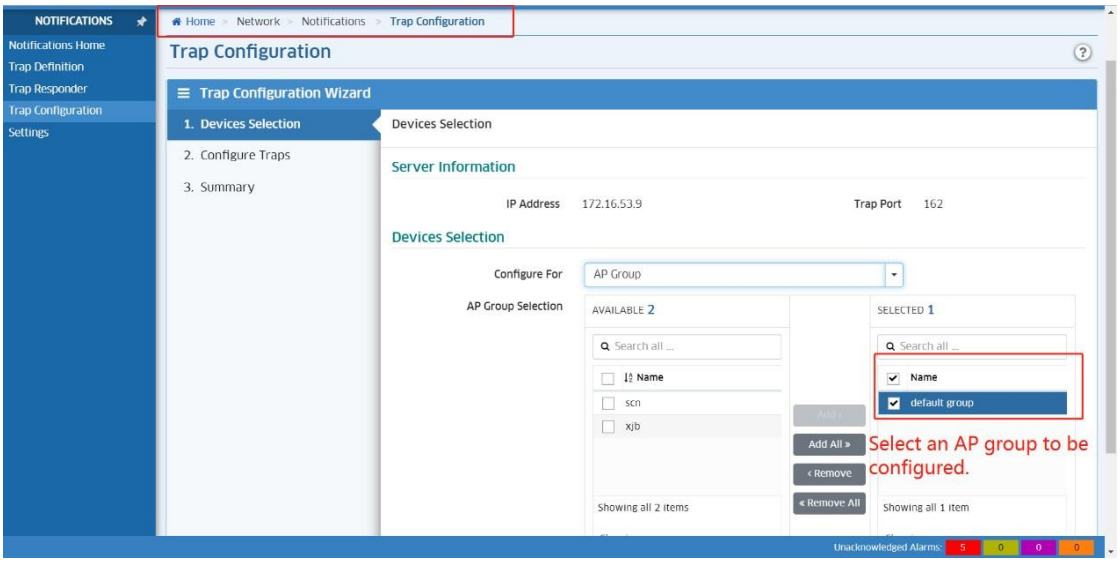
We must synchronize the time of the AP in the entire cluster, otherwise there will be record loss or confusion.

OV Configuration

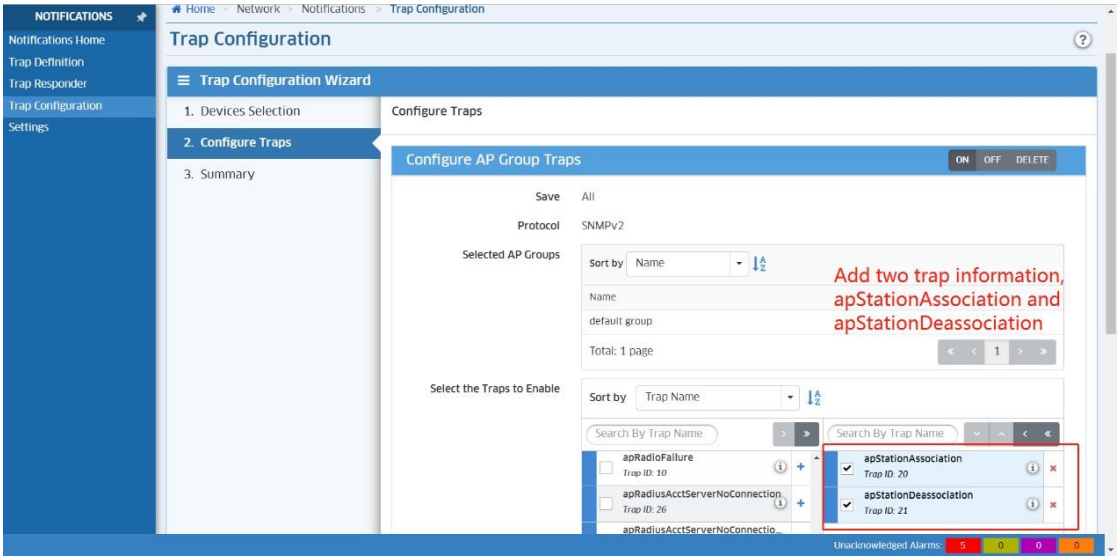
In the OV mode, we need to configure the Trap function to view the roaming record; we need to configure the two APs to the AP group to apStationAssociation and apStationDeassociation.

1) Trap Configuration

Open the Trap ConfigurationPage in Home>Network>Notifications>Trap Configuration.



Pic 5.18.3-2 Client detail roaming & RSSI history

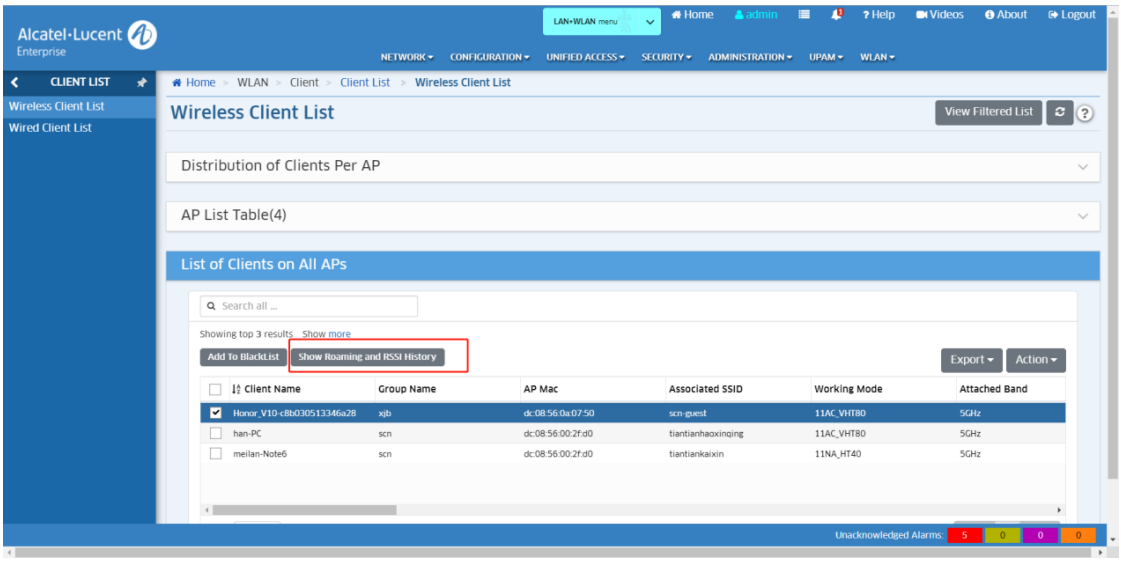


Pic 5.18.3-3 Client detail roaming & RSSI history

2） Show Roaming and RSSI History

Home>WLAN>Client>Client List(Client Session)>Wireless Client List(Wireless Client Session), Can view the client roaming information we need.

We must synchronize the time of the AP in the entire cluster, otherwise there will be record loss or confusion.



Pic 3.4 Client detail roaming & RSSI history

5.18 WEP Authentication Supporting

5.18.1 Feature description

In personal Encryption Type, you can select STATIC_WEP authentication, which is a static wired equivalent privacy security algorithm for authentication.

5.18.2 Topology

Same topology as in section 5.14.2.

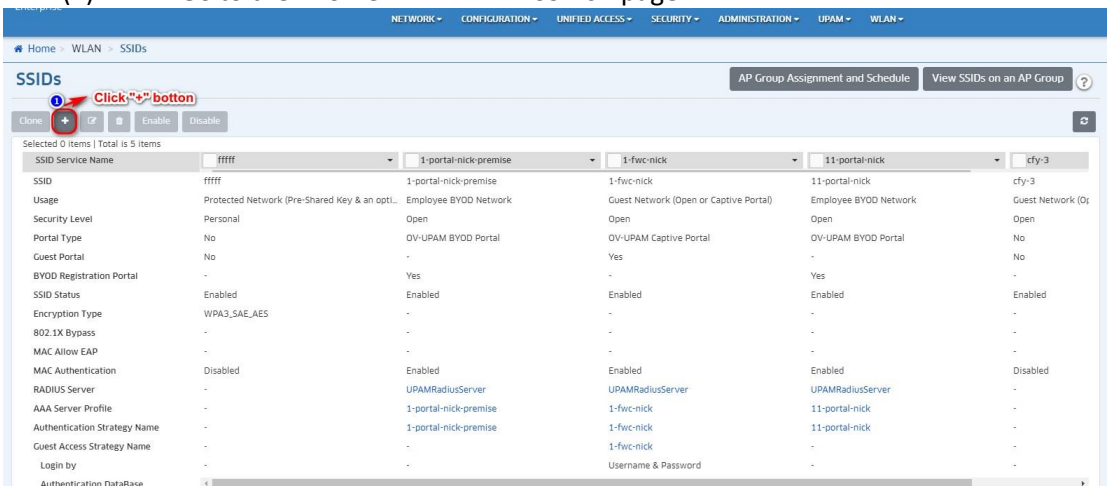
5.18.3 Configuration and Recommendation

1.1 Both OV mode

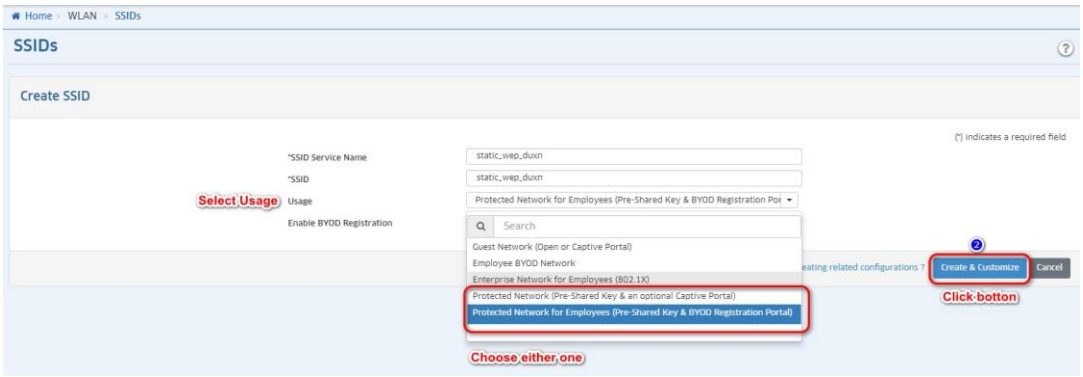
There are 2 scenarios in OVE&OVC mode to create WLAN of STATIC_WEP type.

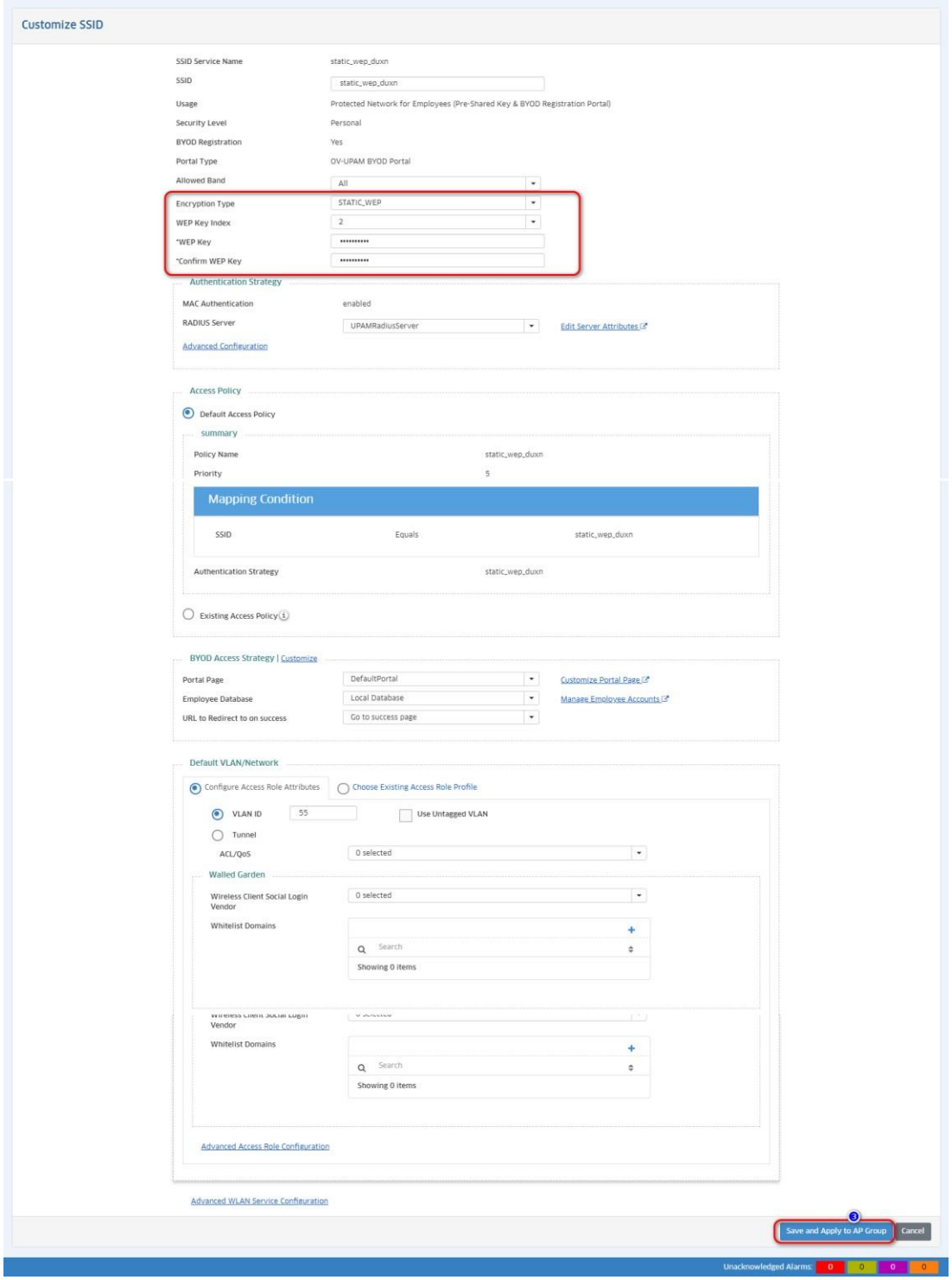
3. Created in the SSIDs page:

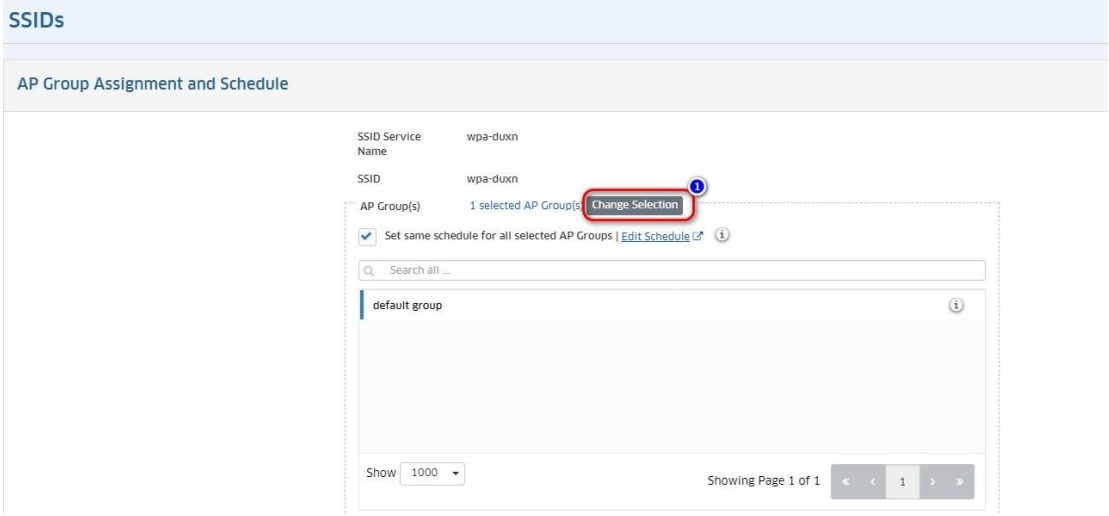
(1) Go to the "Home-->WLAN --> SSIDs " page.

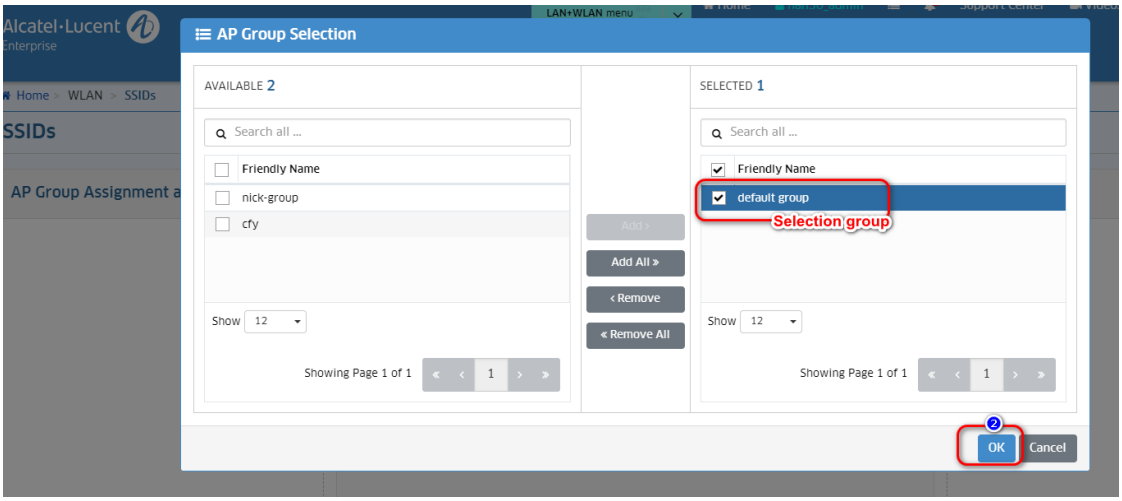


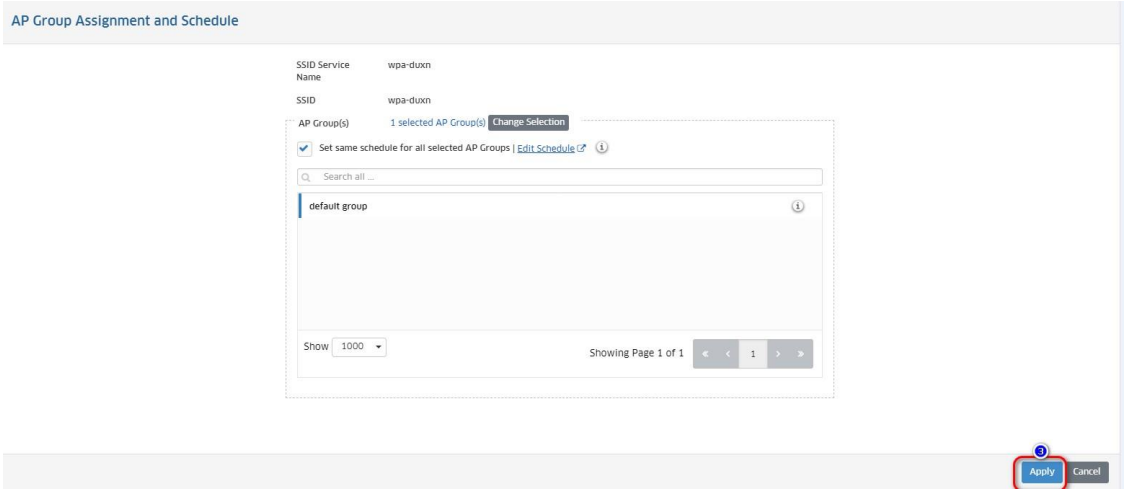
(2) Go to the "Create SSID" page


Home > WLAN > SSIDs
SSIDs
Create SSID
(*) indicates a required field
*SSID Service Name
static_wep_duxn
*SSID
static_wep_duxn
Select Usage
Usage
Protected Network for Employees (Pre-Shared Key & BYOD Registration Por
Enable BYOD Registration
Search
Guest Network (Open or Captive Portal)
Employee BYOD Network
Enterprise Network for Employees (802.1X)
Protected Network (Pre-Shared Key & an optional Captive Portal)
Protected Network for Employees (Pre-Shared Key & BYOD Registration Portal)
eating related configurations ?
Create & Customize
Cancel
Click botton
Choose either one

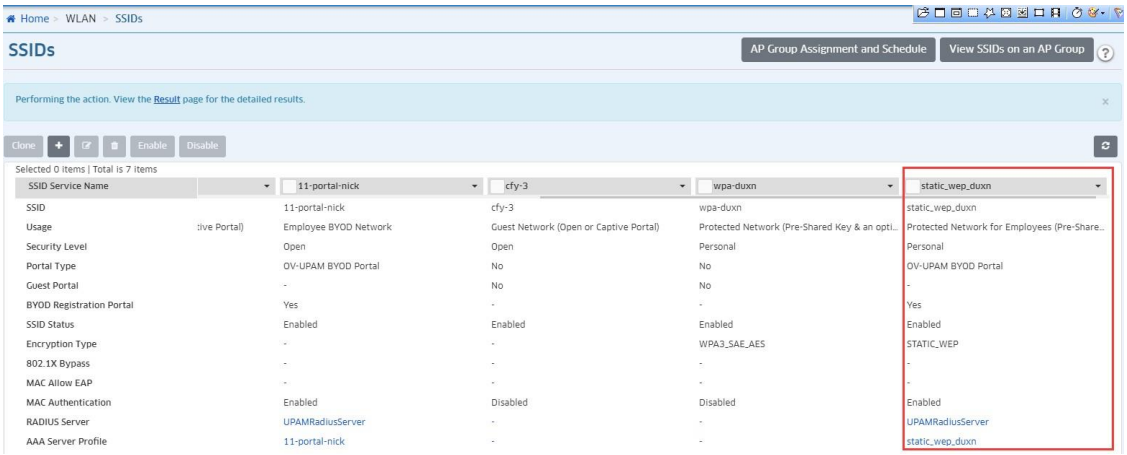

Customize SSID
SSID Service Name
static_wep_duxn
SSID
static_wep_duxn
Usage
Protected Network for Employees (Pre-Shared Key & BYOD Registration Portal)
Security Level
Personal
BYOD Registration
Yes
Portal Type
OV-UPAM BYOD Portal
Allowed Band
All
Encryption Type
STATIC_WEP
WEP Key Index
2
*WEP Key
*Confirm WEP Key
Authentication Strategy
MAC Authentication
enabled
RADIUS Server
UPAMRadiusServer
Edit Server Attributes
Advanced Configuration
Access Policy
Default Access Policy
summary
Policy Name
static_wep_duxn
Priority
5
Mapping Condition
SSID
Equals
static_wep_duxn
Authentication Strategy
static_wep_duxn
Existing Access Policy
BYOD Access Strategy | Customize
Portal Page
DefaultPortal
Customize Portal Page
Employee Database
Local Database
Manage Employee Accounts
URL to Redirect to on success
Go to success page
Default VLAN/Network
Configure Access Role Attributes
Choose Existing Access Role Profile
VLAN ID
55
Use Untagged VLAN
Tunnel
ACL/QoS
0 selected
Walled Garden
Wireless Client Social Login Vendor
0 selected
Whitelist Domains
Search
Showing 0 items
Vendor
Whitelist Domains
Search
Showing 0 items
Advanced Access Role Configuration
Advanced WLAN Service Configuration
Save and Apply to AP Group
Cancel
Unacknowledged Alarms:







Can be viewed on the "Home-->WLAN --> SSIDs " page



Created in the WLAN Service (Expert) page:

Created in the "Home-->Unified Access-->Unified Profile-->Template-->WLAN Service (Expert)" page, the same steps as other types of WLAN.

Notes The WEP Key Index of the client must be consistent with the WEP Key Index of the WLAN to access.

5.19 WMA-Support Airtime Fairness

5.19.1 Feature description

Turn on the airtime fairness so slower clients like 802.11b or 802.11g do not monopolize the BW. It gives fair time in the air to all clients.

For stellar AP, when the switch is turned on, the AP will assign the same time slice to each client. When a client time slice is over, wait for the next round of time slices.

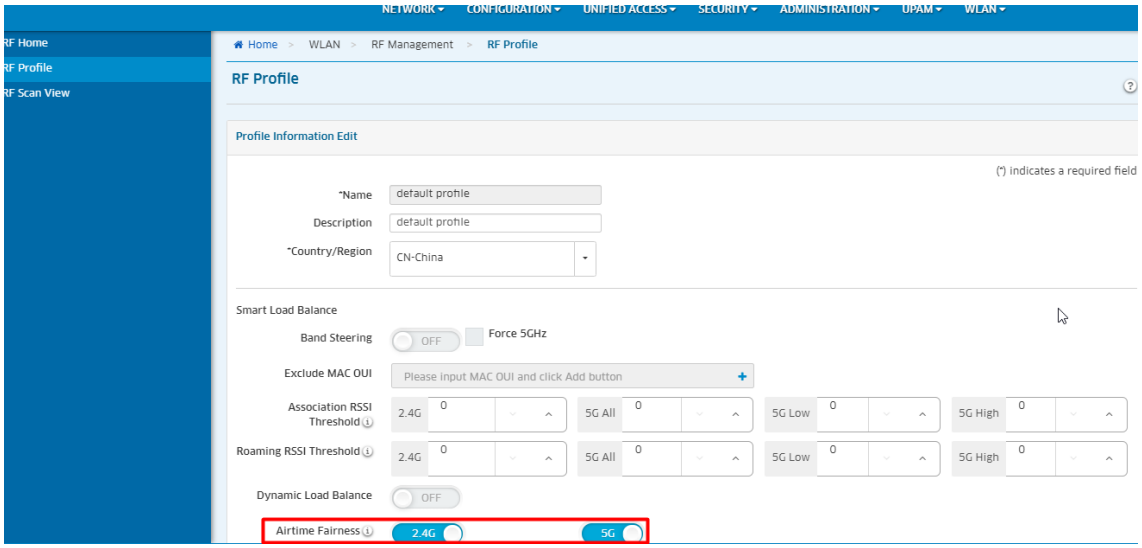
5.19.2 Configuration and Recommendation

It can be configured under both OVE/OVC mode and Cluster mode.

OVE/OVC Mode

Add/Edit the airtime fairness configuration

Path: Home >>WLAN >RF>> RF Profile

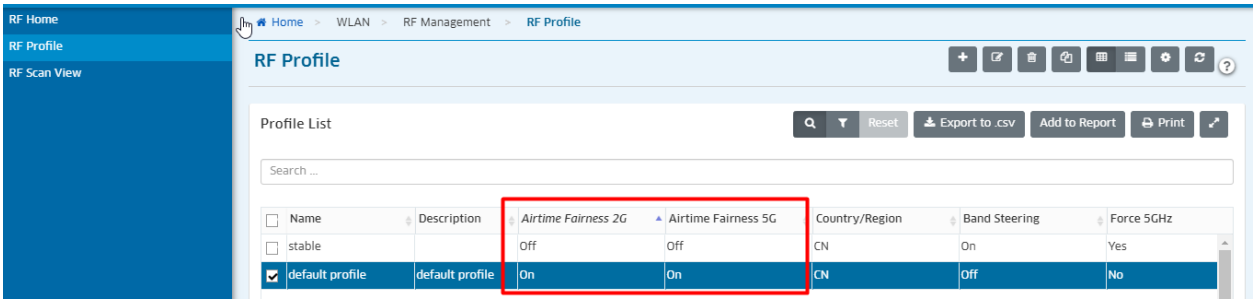


Note:

- After the WMA sends the Airtime fairness switch to the AP, the user must manually restart the AP for the configuration to take effect.
- When a new AP registers the OV system, the AP can save the configuration of airtime fairness to flash, but it will only take effect on the next reboot.

2)Display the airtime fairness configuration

After the configuration takes effect, user can see the Airtime Fairness configuration on the RF Profile list page.



Cluster Mode

Add/Edit/display the airtime fairness configuration

Path: login AP Web>>Wireless>> Performance Optimization

Note:

- After edit the airtime fairness configuration, it shall only take effect after reboot.
- When a new AP join the cluster, the AP can synchronize the configuration of airtime fairness, but it will only take effect on the next reboot.

5.19.3 Related Commands

Check the airtime fair configuration

support@AP-1B:60:~$ support_cmd 10

For example:

```
support@AP-1B:60:~$ support_cmd 10
Airtime Fairness is enabled
support@AP-1B:60:~$
```

```
support@AP-1B:60:~$ support_cmd 10
Airtime Fairness is enabled now, need reboot to disable
support@AP-1B:60:~$
```

5.20 mDNS Multicast Control (Cluster Mode)

5.20.1 Feature description

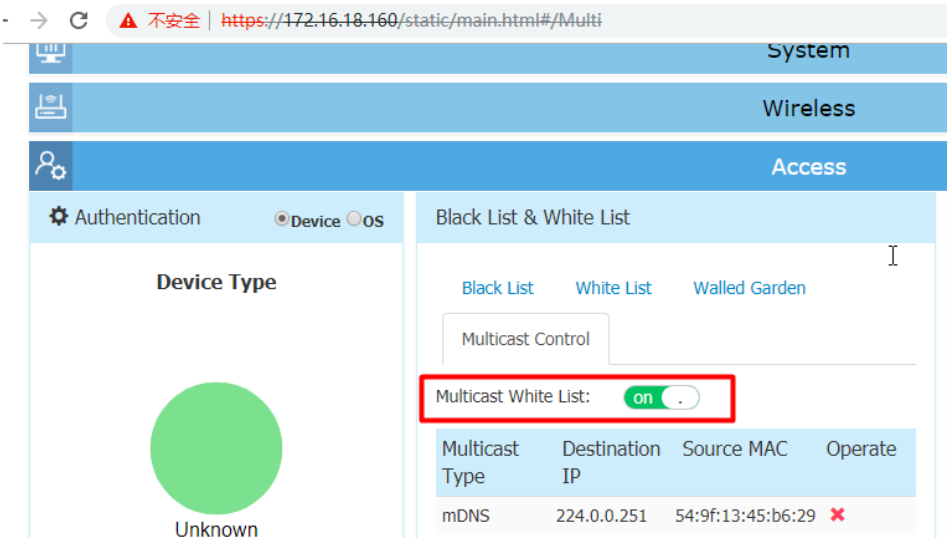
In computer networking, multicast is group communication where data transmission is addressed to a group of destination computers simultaneously. Multicast can be one-to-many or many-to-many distribution. Multicast should not be confused with physical layer point-to-multipoint communication.

Multicast control configures a filtering policy to filter and control multicast packets forwarded by AP devices.

5.20.2 Configuration and Recommendation

Login the AP Web UI, and click>Acess> Black List & White List.

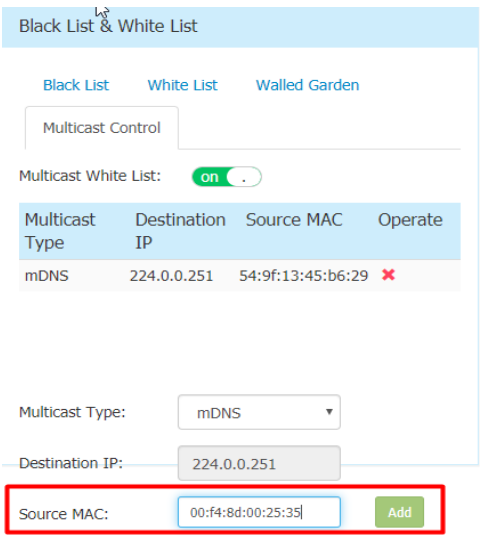
Enable/Disable the switch of Multicast White List



When the Multicast switch is enabled, multicast filtering is enabled, otherwise multicast filtering is disabled. It is disabled by default.

Configure a multicast filtering list

Configure a multicast filtering list, including the multicast protocol type, mulitcast IP address, and MAC address for sending multicast packets, after multicast filtering is enabled, only the multicast packets sent by the client whose MAC address is on the whitelist are allowed to pass, and other multicast packets are drop.



Note:

- The number of Multicast White List cannot exceed 8.
- Multicast Type (Mdns) and the Destination IP (224.0.0.251) is fixed now, which may be optimized in future according to the product requirment.

5.20.3 Related Commands

Check the Multicast Whitelist under support/root account

```
support@AP-1B:60:~$ cat /tmp/config/multicast-whitelist.conf
```

```
support@AP-1B:60:~$ cat /tmp/config/multicast-whitelist.conf
{
        "Multicast":{
                "multicastSwitch":true,
                "multicastList":[
                        {
                                "mutilcastWhitelistType":"mDNS",
                                "multicastWhitelistIP":"224.0.0.251",
                                "multicastWhitelistMac":"54:9f:13:45:b6:29"
                        }
                ]
        }
}
```

Check the iptables under root account

```
root@AP-1B:60:~# iptables -nvL
```

```
root@AP-1B:60:~# iptables -nvL
Chain INPUT (policy ACCEPT 6698K packets, 1334M bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 1818K packets, 322M bytes)
 pkts bytes target     prot opt in     out     source               destination
1845K  329M CP_DNSS    all  --  *      *       0.0.0.0/0            0.0.0.0/0
1845K  329M CP_FILTER  all  --  *      *       0.0.0.0/0            0.0.0.0/0
1831K  324M isolation_cli  all  --  *      *       0.0.0.0/0            0.0.0.0/0
10496 1156K multicast  all  --  *      *       0.0.0.0/0            0.0.0.0/0            match-set multicast_v4 dst

Chain OUTPUT (policy ACCEPT 13M packets, 2419M bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain CP_DNSS (1 references)
 pkts bytes target     prot opt in     out     source               destination

Chain CP_FILTER (1 references)
 pkts bytes target     prot opt in     out     source               destination
1845K  329M CP_F_DEFAULT  all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain CP_F_DEFAULT (1 references)
 pkts bytes target     prot opt in     out     source               destination
  473 72257 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:53
  963 84689 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:53
  111 36408 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:67 dpt:68
12809 4215K ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:68 dpt:67

Chain isolation_cli (1 references)
 pkts bytes target     prot opt in     out     source               destination

Chain multicast (1 references)
 pkts bytes target     prot opt in     out     source               destination
 1854  196K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            match-set multicast_mac4 src
 8642  960K DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0
root@AP-1B:60:~#
```

Check by capture packets

```
root@AP-C1:C0:/tmp# tcpdump -i eth0 -net -w /tmp/mdns3.pcap
```

5.21 Troubleshooting Onboarding

5.21.1 Feature description

Enabling supporting personnel to troubleshoot network devices by performing some provided commands on the specific APs in the OVC web.

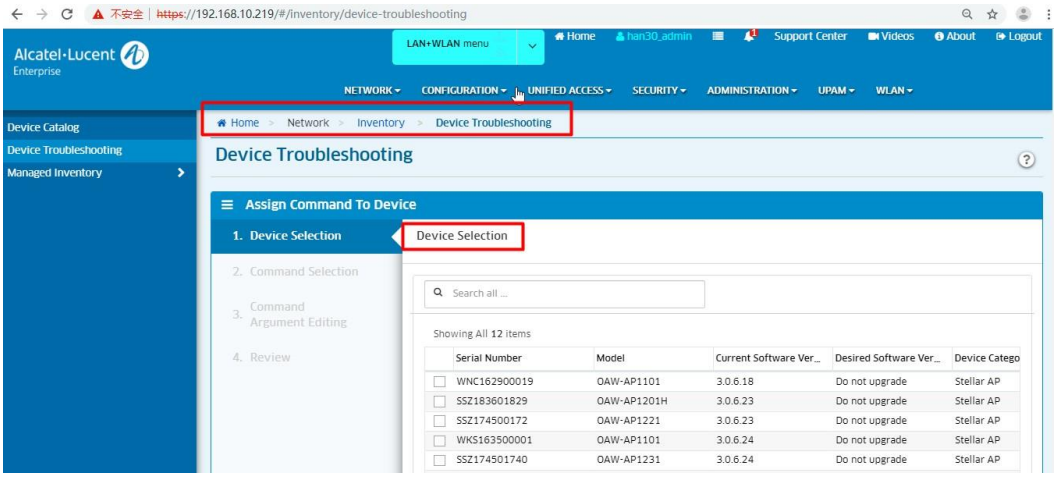
5.21.2 Configuration and Recommendation

Enter the page of Device Selection by the following 2 ways:

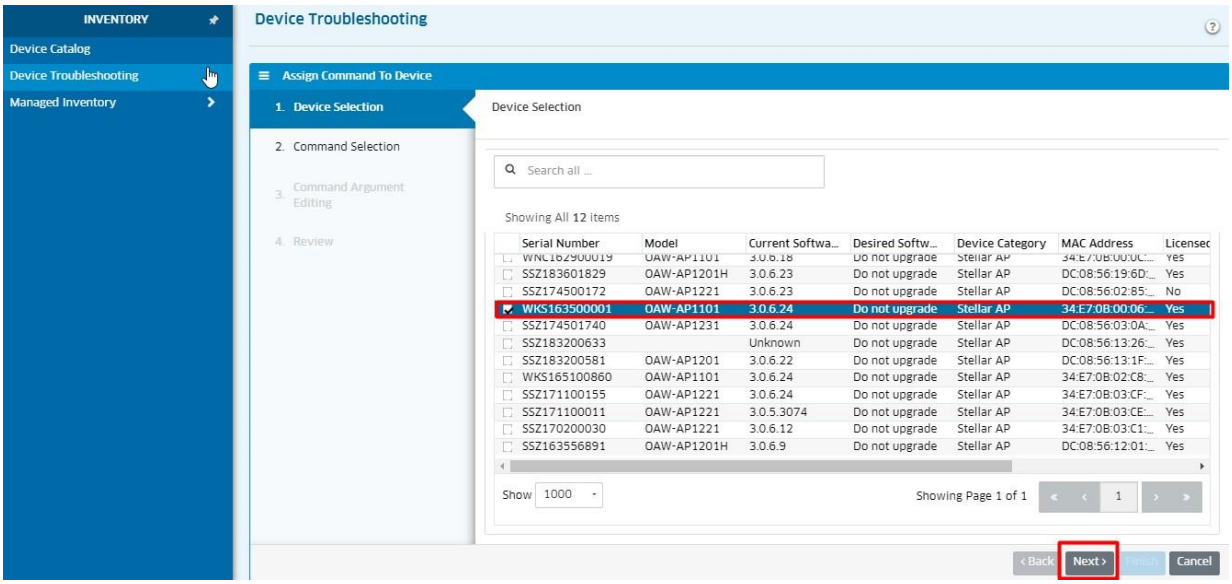
Home>>NETWORK>>INVENTORY>>Device Catalog>>Troubleshoot Device

Home>>NETWORK>>INVENTORY>>Device Troubleshooting>>Troubleshoot Device>>Assign Command)

Then enter the Device Selection page by either above one path.



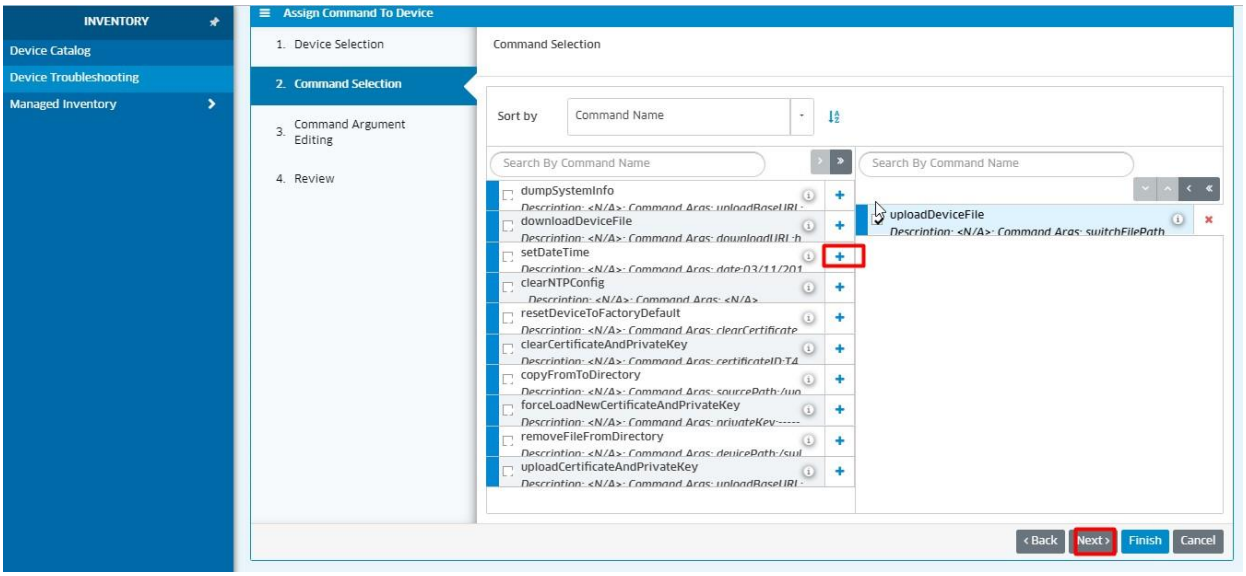
Select one or more APs



Then click “Next” and enter the Command Selection page.

Command Selection

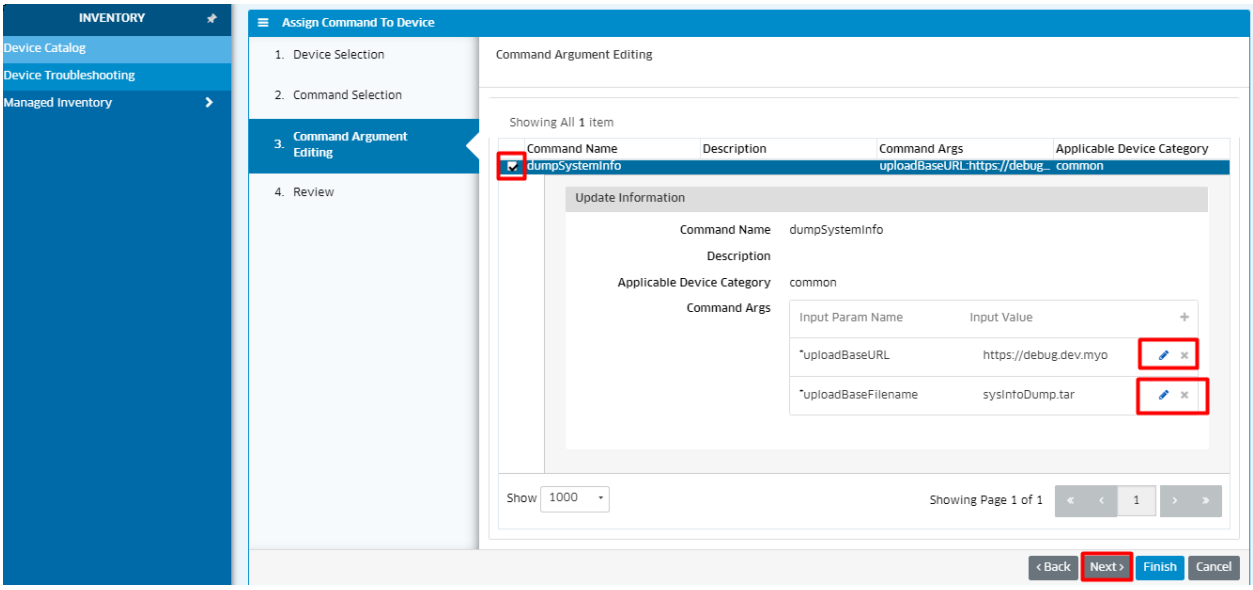
Select one command you want and click the ""+""icon



Then click ""Next"" and enter the Command Argument Editing page.

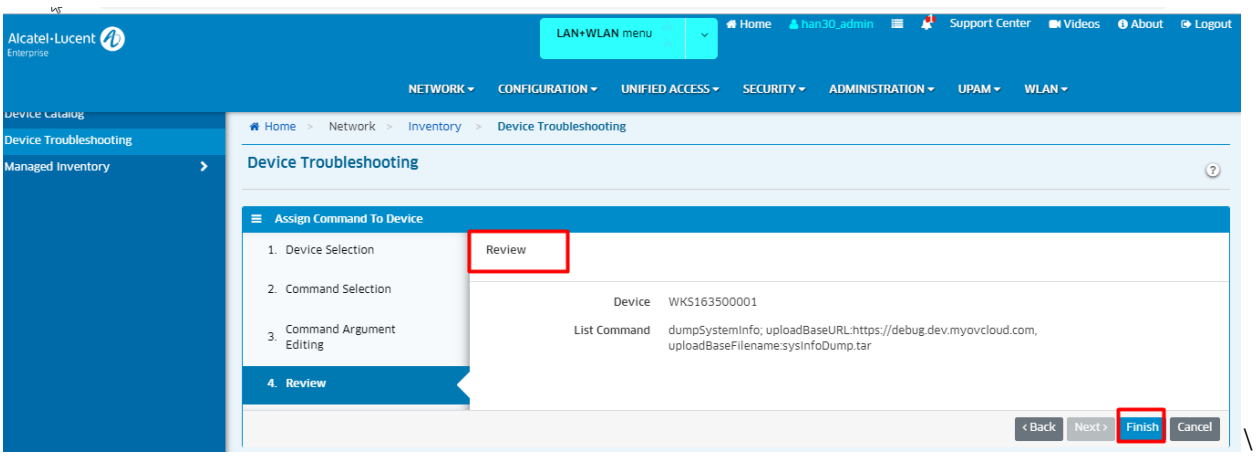
Command Argument Editing

There are different displays for different command, take ""dumpSystemInfo"" for example:

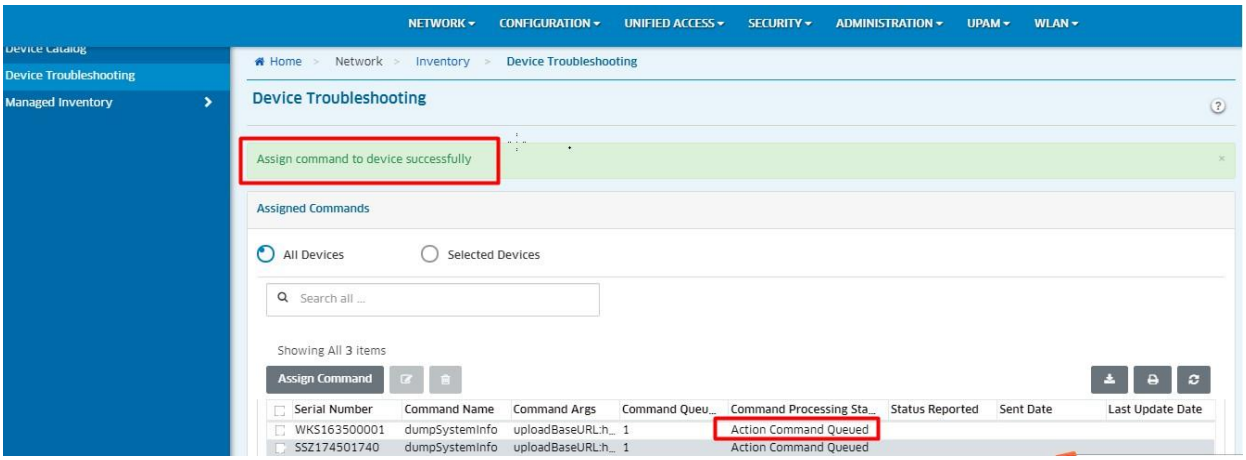


Then click ""Next"" and enter the Review page.

Operation Review



Then click “Finish” and popup the tips “Assign Command to Device Successfully” and displays the Assigned Commands page, which can view the assigned commands and its processing status.



5.22 Collect support info on stellar AP

5.22.1 Feature description

Perform a one-click collection of logs on the AP and upload it to OV.

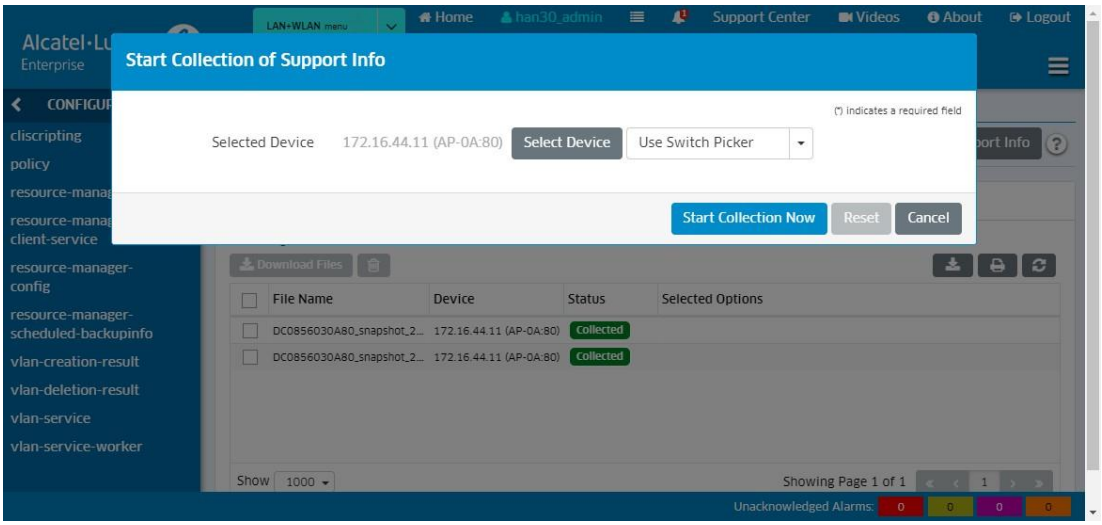
5.22.2 Topology

Same topology as in section 5.14.2.

5.22.3 Configuration and Recommendation

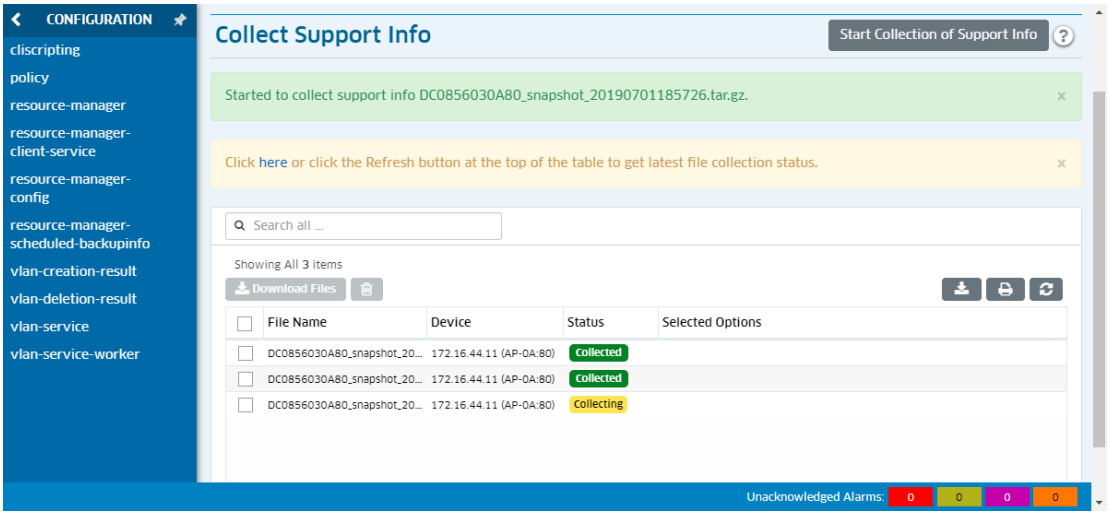
Path：Home -> Administration -> Audit -> Collect Support Info

Select Device:



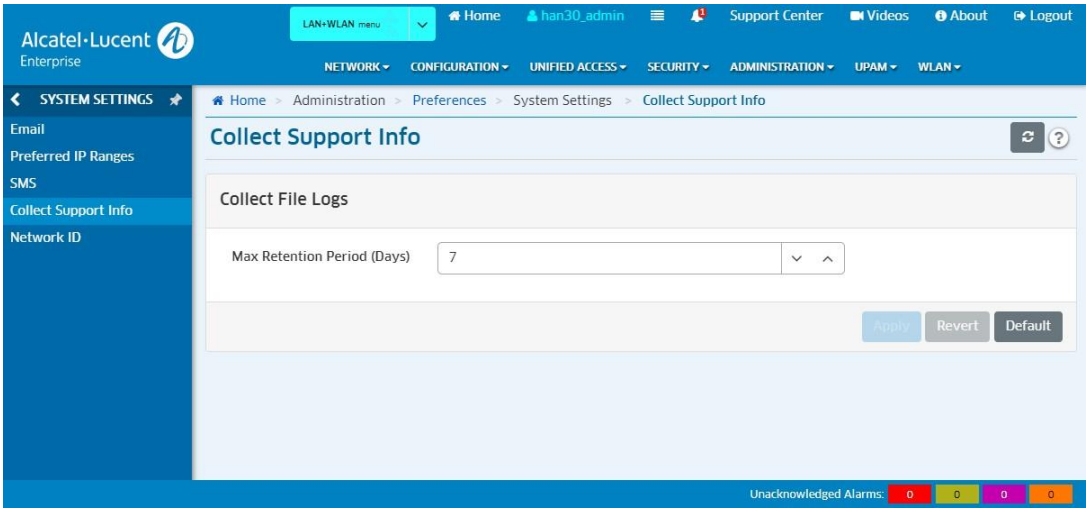
Collect status

When collecting the status of the log from collecting to collected, you can download or delete the collected logs.The collected log content and format are consistent with those collected on Express.



Log Files Save Time

You can set the save time when the log file is saved on OV here.



5.23 Issue with the captive portal redirection

5.23.1 Feature description

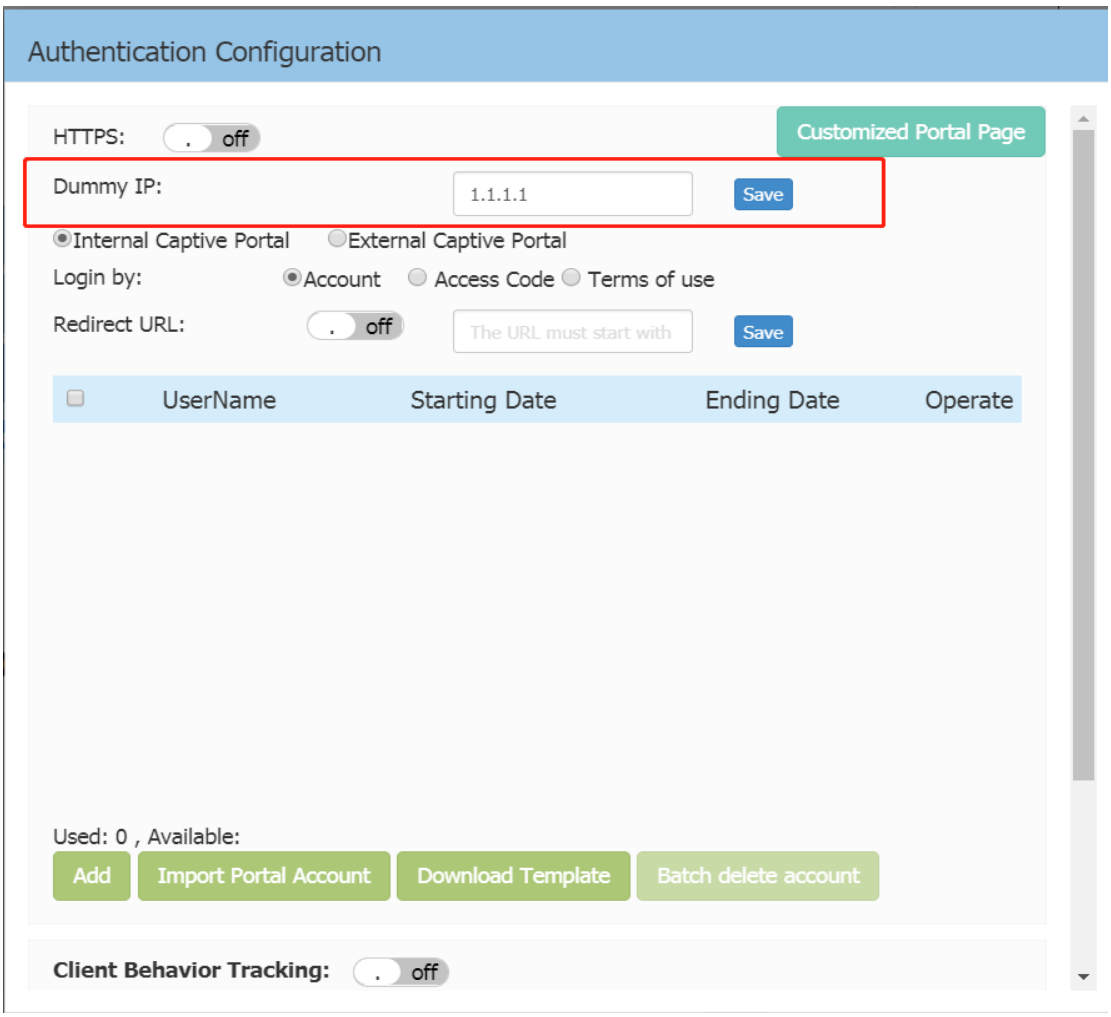
We need a virtual address to process the authentication request during authentication. The default is 1.1.1.1, but sometimes we need to access the 1.1.1.1 website, so we added a configuration box called Dummy IP to configure this virtual. address.

5.23.2 Topology

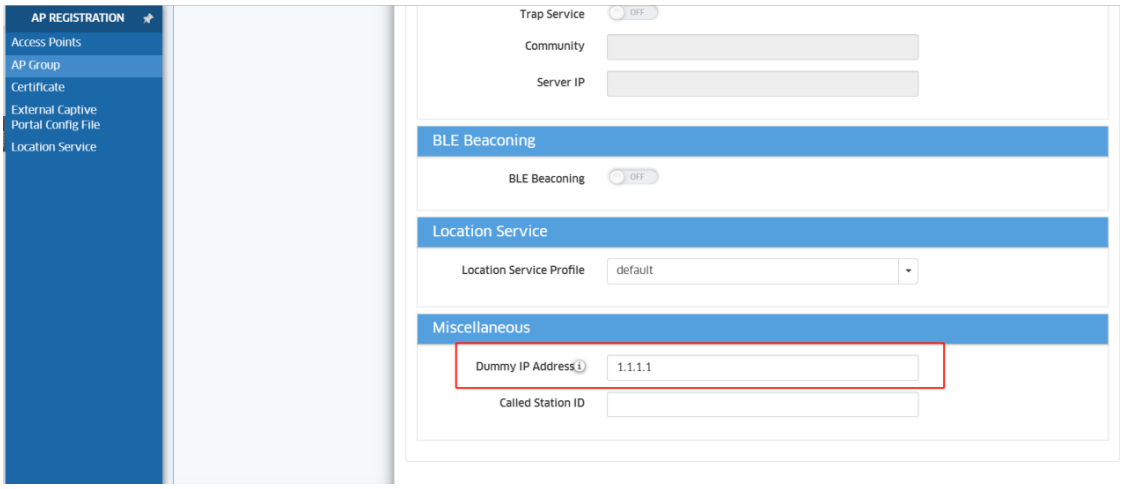
Same topology as in section 5.9.2.

5.23.3 Configuration and Recommendation

We only need to change the value in Dummy IP to configure this function (default is 1.1.1.1).
Express Configuration
Configure Dummy IP in the Cluster page Access-Authentication.



OV Configuration
Configure Dummy IP in the OV page Network - AP Registration - AP Group.



We do not configure the Dummy IP to be an in-use address, such as the login address of a device or the IP address of a website, which would make it impossible to access the address.

5.24 AP1222 support dual 2*2 working mode

5.24.1 Feature description

AP1222 This type of AP uses an external antenna. Two antennas are multiplexed with 2.4G and 5G signals. Sometimes the signals of these two bands need to be separated, so this function can be used.

5.24.2 Topology

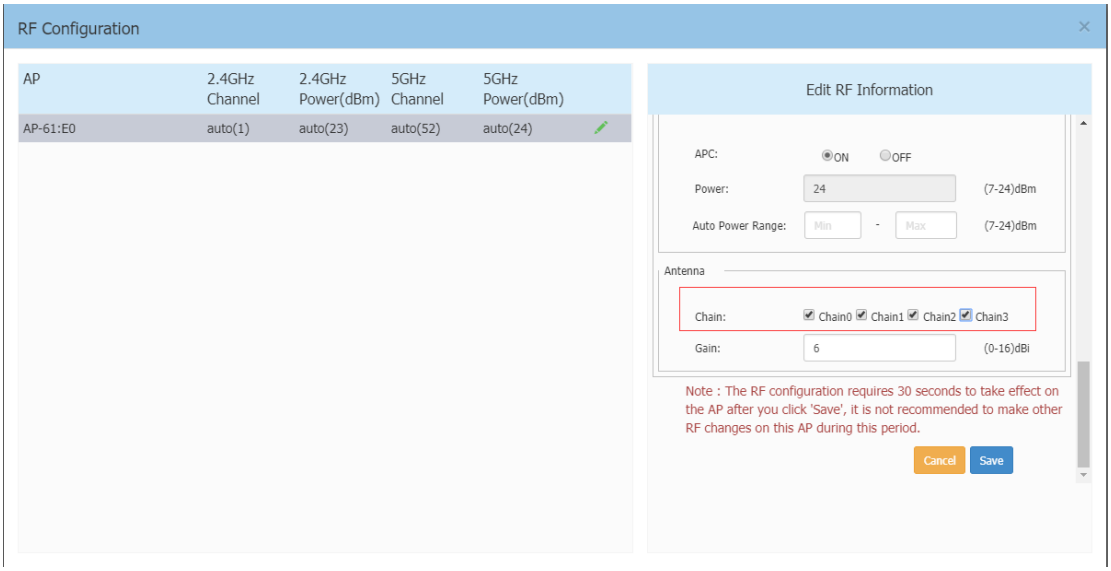
Same topology as in section 5.9.2.

5.24.3 Configuration and Recommendation

This configuration is only for AP1222 AP. Other APs do not have this configuration; the default is chain0-chain3 mode.

Cluster Configuration

On the Cluster page, we can configure the antenna working mode of the AP1222. If you want to separate the 2.4G and 5G signals, configure the chain0+chain1 mode.(Chain0 and Chain1 only release 5G signals, Chain2 and Chain3 release 2.4G and 5G signals)



Pic 5.26.3-1 AP1222 support dual 2*2 working mode

5.25 Fixed Channel width

5.25.1 Feature description

Mainly modified in express mode, providing a place to set the 5G global channel width.In order to be able to uniformly configure a channel width for the APs.OVE and OVC are supported in previous versions, and a channel width is uniformly configured in RF.

5.25.2 Topology

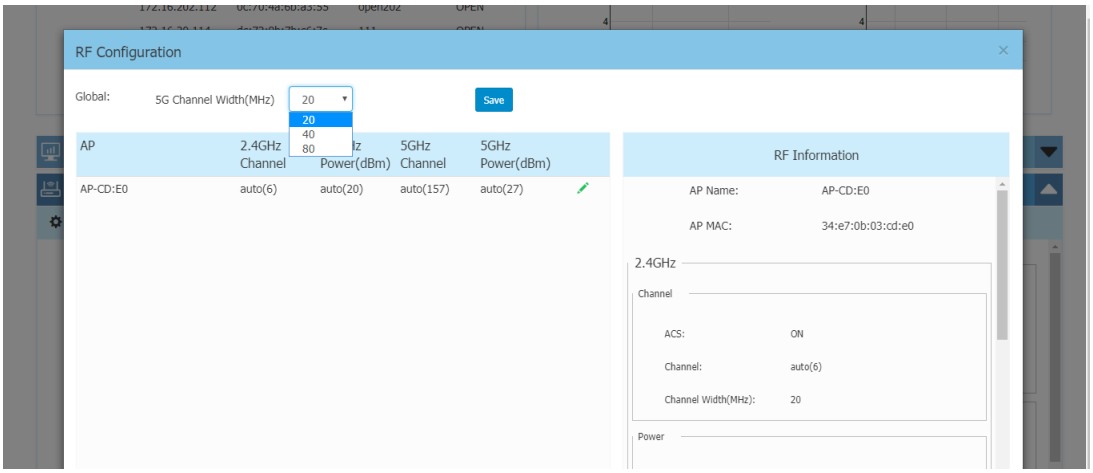
Same topology as in section 5.14.2.

5.25.3 Configuration and Recommendation

Express:

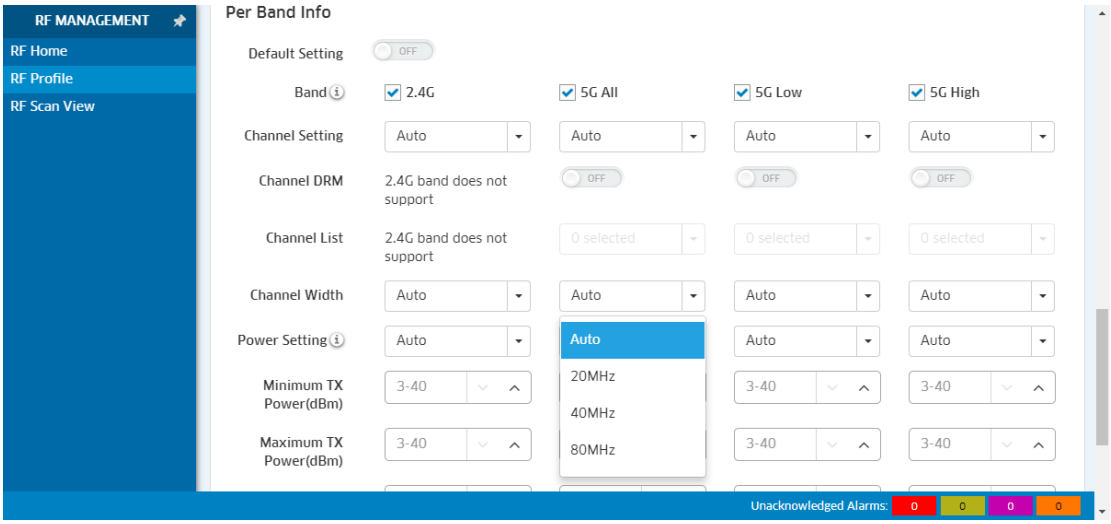
Path:wireless -> RF configuration

Global 5G channel width can choice 20/40/80/160 MHz



OVE&OVC

Path:Home -> WLAN -> RF Management -> RF Profile



5.25.4 Notes

If the current channel is set to automatically select the channel and the channel selection is 5G high frequency (for example, 165), the current setting 40/80 does not take effect. When the channel is automatically selected next time, a channel supporting 40/80 will be selected. In order to select 160MHz the channel setting must be set manually.

5.26 Long Interval background-scanning

5.26.1 Feature description

Applicable AP models: All types of AP, users can configure the interval background scanning through the web performance optimization setting.

Long interval background scanning time requires manual setting of web interface, Configuration scope is 5s ~10800s(3hour).

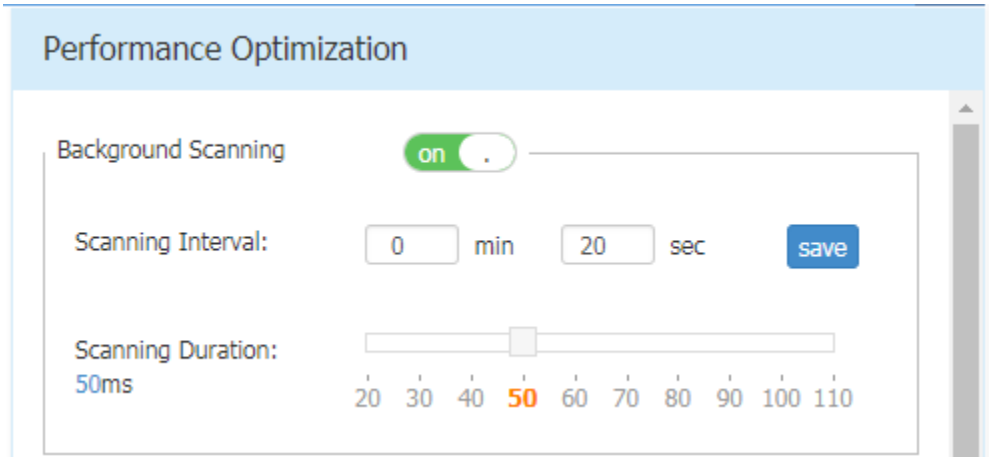
5.26.2 Topology

Same topology as in section 5.14.2.

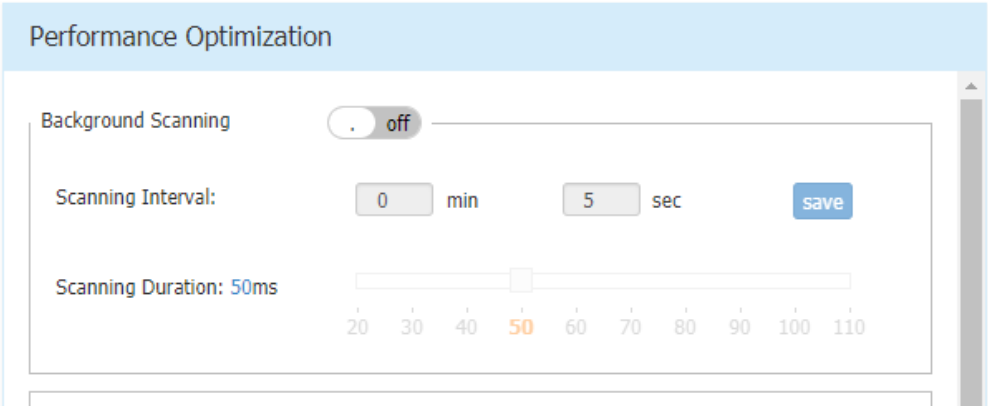
5.26.3 Configuration and Recommendation

Cluster mode

Go to "wireless", you can configure the scan interval

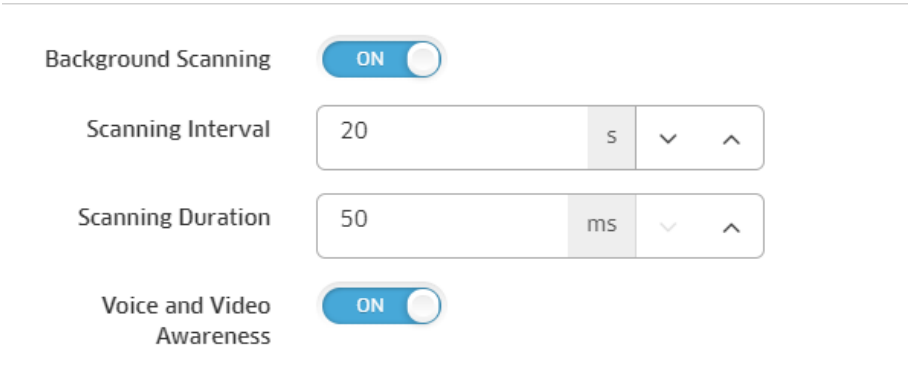


If the background scan switch is off, the scanning interval is not configurable.



Both OV mode

Go to the Home-->WLAN -->RF Management-->RF Profile page and select the RF file to be edited. You can configure the scan interval and finally apply it to the group.



5.26.4 Notes

It is recommended to set the background scan interval to within 60s. If the value is greater than 60, the scan may affect the automatic power and affect the detection and suppression of the rogue AP on different channels. After apply new configuration, wait for 15mins at least.

5.27 Improve DHCP option-43 and option-138 handling

5.27.1 Feature description

Priority selection of DHCP option138 and option43.

Option 138 has a higher priority than option43.

The order of preference for multiple DHCP services in Cluster mode:

In option43, there is suboption1=” alenterprise” -> option43=” alcatel.a4400.0” or option43=” alcatel.nms.ov2500 ” -> Other.

The order of preference for multiple DHCP services in Enterprise mode:

When the AP is started in non-CLUSTER mode, there are two cases: one is that the AP works in OV mode, and the other is working in OVC mode.

In OV mode, when a DHCP service has both option 138 and option 43, the OVE registration address is option 138. If there is only option43, which happens to be option43 = "IP" or option43 = "IP: Port", the OVE registration address is the IP in option43.

When there are both option 138 and option43 in multiple DHCP servers, select the DHCP SERVER with option43 suboption1 = "alenterprise" to provide the service and give priority to option138.

5.27.2 Topology

Same topology as in section 5.14.2.

5.28 802.11v enhancement

5.28.1 Feature description

When steering between AP, before sending the client BSS Transition Request, we check whether the BSSID from the client previous beacon report is in the cluster neighbor's VAP list, if it exists BTM will be sent, if not direct interruption of processing

5.28.2 Topology

Same topology as in section 5.14.2.

5.28.3 Configuration and Recommendation

The function is invisible for customer, please insure that have enabled 11k/v switch (This function is enabled by default)
It also needs to configure roaming RSSI, when client RSSI is less than roaming RSSI, this function will work.
Notes:
This function is based load balance function, so you need to create the WLAN with dual bands

5.29 Allow decimal digit in scale specification on Heatmap and Floorplan application

5.29.1 Feature description

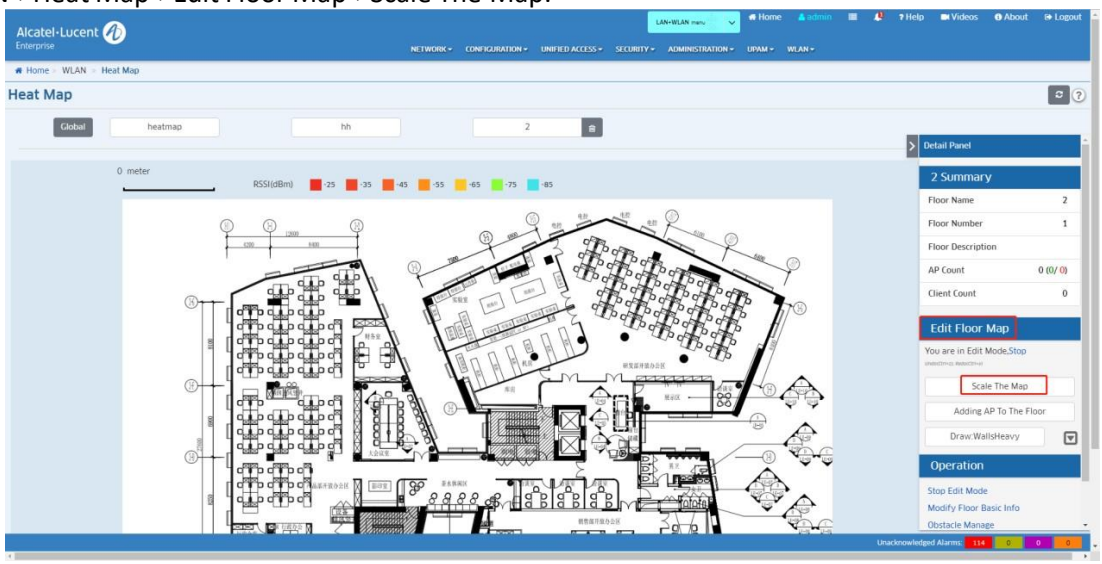
Allow single digit decimal value as part of Heatmap and Floorplan scale. Usually customers deal with plans where there is maybe one or few dimensions marked, and we are going for longest one for ease of use. The influence of precise map scaling on planning results may be marginable, but nevertheless it's desirable to allow decimal point in map scaling.

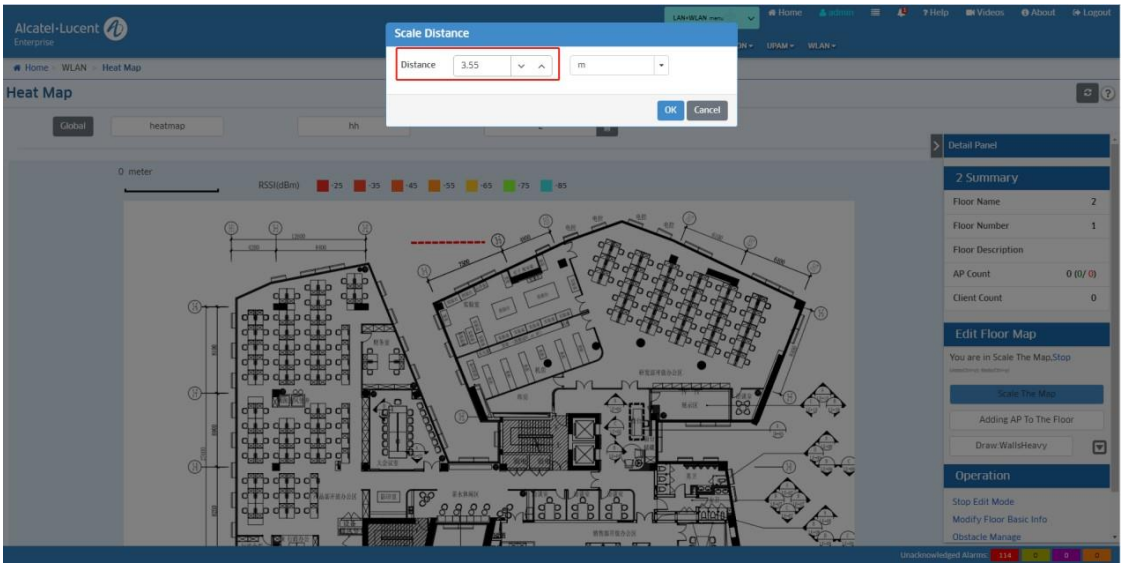
5.29.2 Topology

Same topology as in section 5.14.2.

5.29.3 Configuration

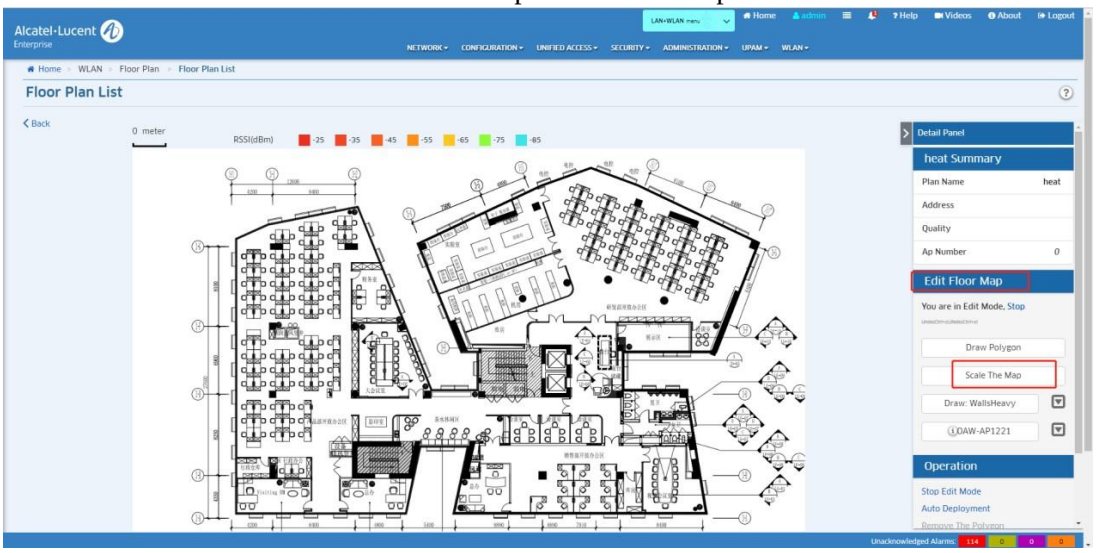
Home->WLAN->Heat Map->Edit Floor Map->Scale The Map:

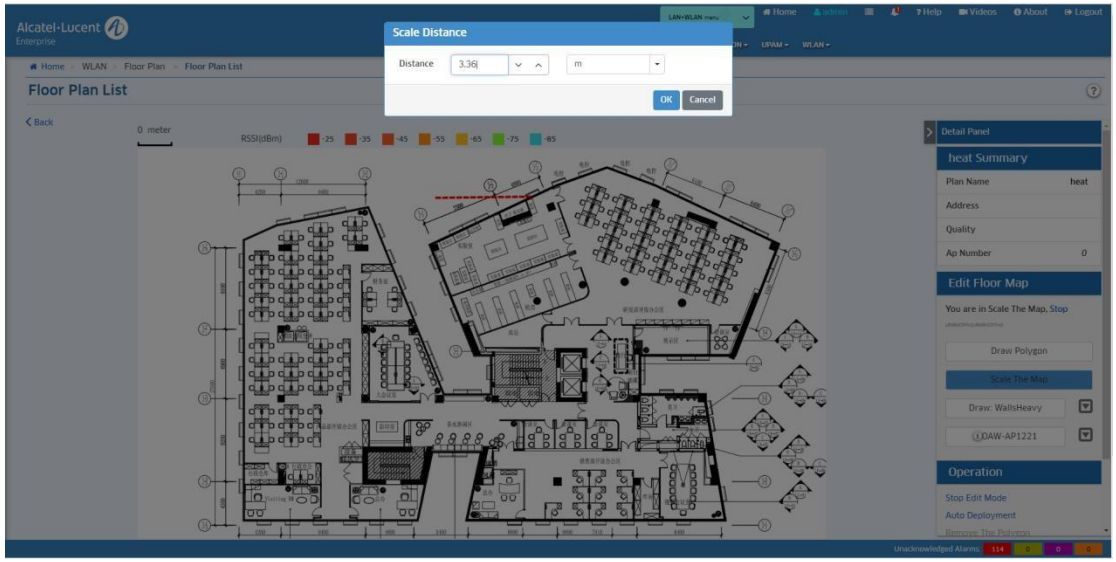


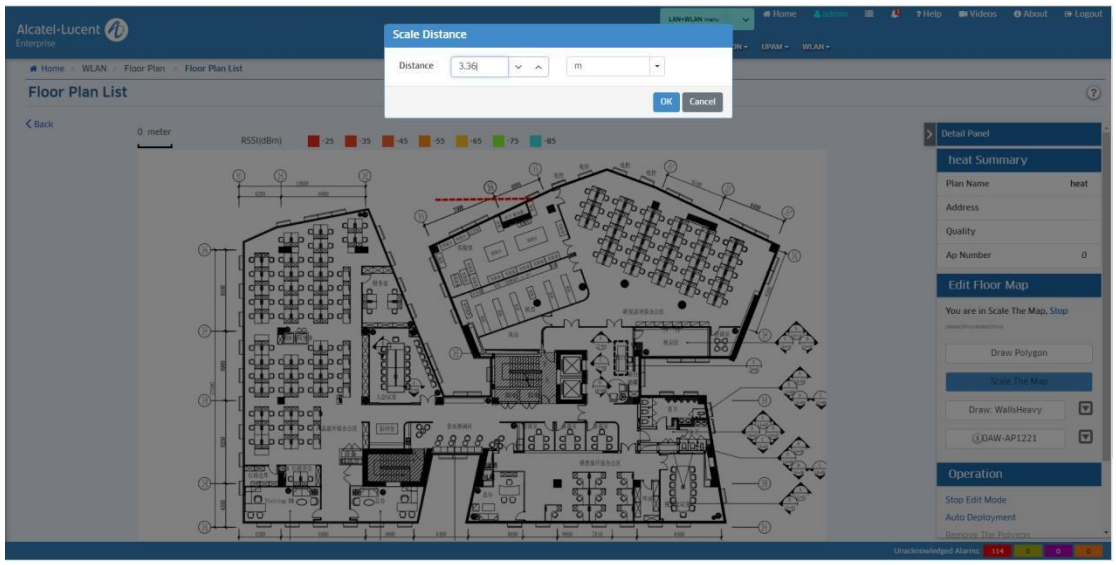


Then you can edit Distance with two decimal points.

Home->WLAN Floor Plan->Floor Plan List->Edit Floor Map->Scale The Map.







Then you can edit Distance with two decimal points.

5.30 Guest Strategy improvements

5.30.1 Functional Description

In some scenarios, we need to distinguish the service level of the Guest user, so we now support the Guest self-registered user to differentiate the service level.

5.30.2 Topology

Same topology as in section 5.14.2.

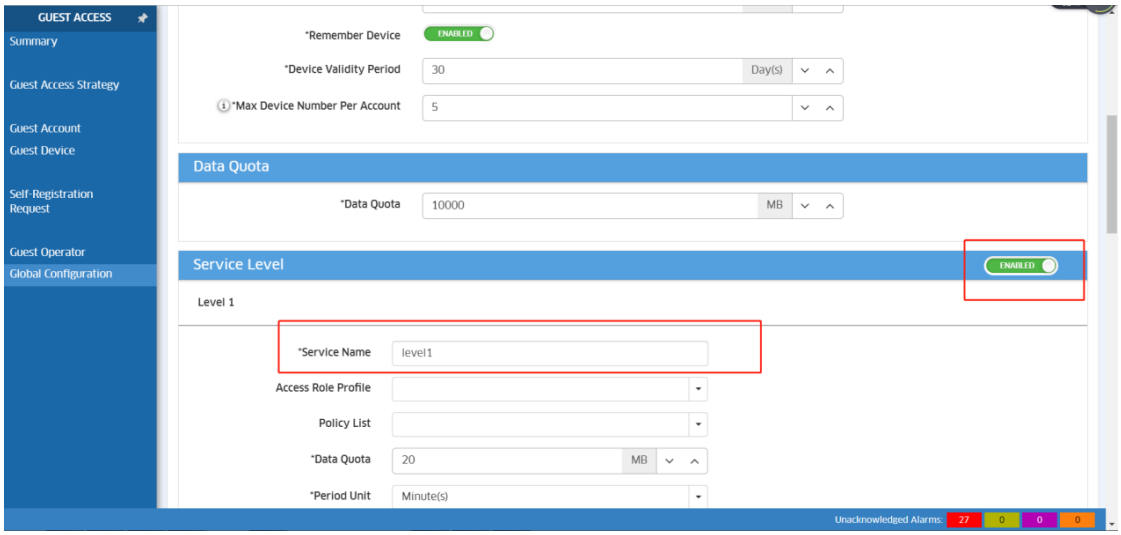
5.30.3 Configuration

When create and edit a new SSID (open&portal type), many configuration should be changed.

Global Configuration

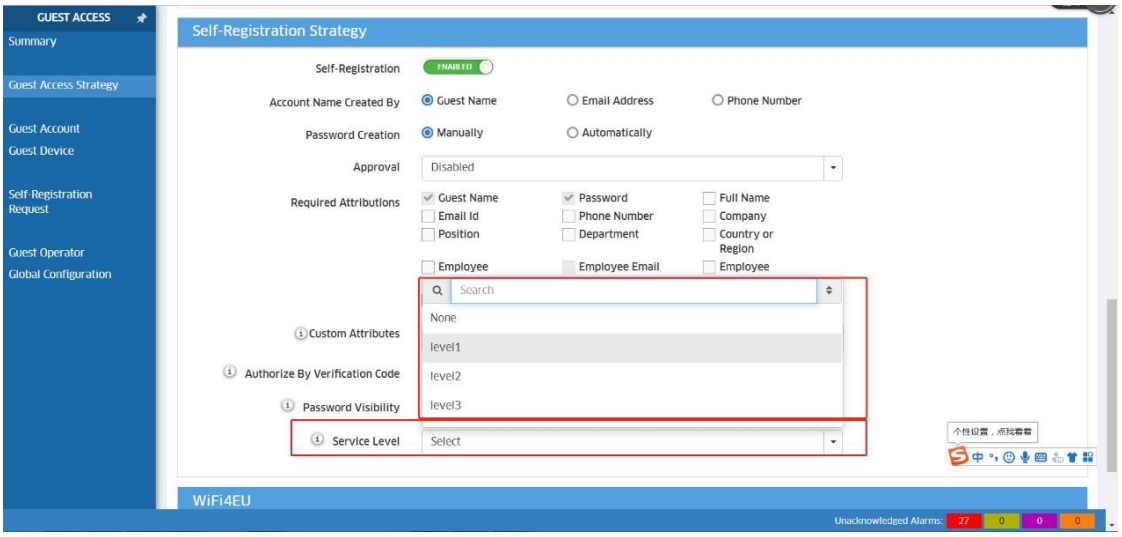
Service level

Need to open the service level and configure in the global configuration.



Guest strategy

Need to select service level in the guest strategy.



5.31 Support AP Product Legal Update with FW version

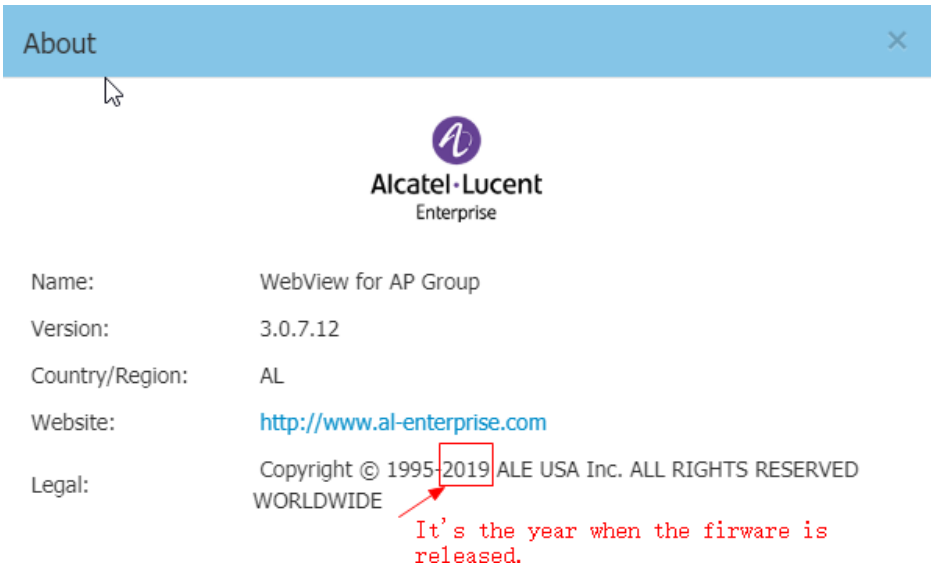
5.31.1 Feature Description

AP Product legal shall update with FW version

5.31.2 Configuration

It can be checked by both WEB GUI and CLI

Path: Login>>More button>>About>>Legal



Display under CLI

```
support@AP-1B:60:~$ showsysinfo
    Company Name:ALE USA Inc.
              SN:WKS163300092
    Device Model:OAW-AP1101
             MAC:34:E7:0B:00:1B:60
         Country:RW
   Software Name:AWOS
Software Version:3.0.7
Hardware Version:1.10
             Oid:1.3.6.1.4.1.6486
     Part Number:903917-90
        Revision:
    Essid Prefix:mywifi
Cluster Describe:AP Group
         Website:http://www.al-enterprise.com
           Legal:Copyright 漏 1995-2019 ALE USA Inc.   ALL RIGHTS RESERVED WORLDWIDE
        Describe:AWOS 30
support@AP-1B:60:~$
support@AP-1B:60:~$
support@AP-1B:60:~$
support@AP-1B:60:~$ productinfo show
vendor=ALE USA Inc.
model=OAW-AP1101
product_version=1.0
sw_name=AWOS
url=http://mywifi.al-enterprise.com
cluster_describe=AP Group
website=http://www.al-enterprise.com
legal=Copyright 漏 1995-2016 ALE USA Inc.   ALL RIGHTS RESERVED WORLDWIDE
description=AWOS 30
pn=903917-90
resource:logo_icon.png  type:imginfo
resource:logo_img.png  type:imginfo
support@AP-1B:60:~$
support@AP-1B:60:~$
support@AP-1B:60:~$ showver
3.0.7.12
support@AP-1B:60:~$
support@AP-1B:60:~$ cat /proc/version
Linux version 3.14.77 (c163ci) (gcc version 5.2.0 (HOS GCC 5.2.0 d79203c+r49254) ) #1 Wed Aug 28 23:26:10 CST 2019
support@AP-1B:60:~$
```

5.32 Support Disable/Enable AP Radio in OVE/OVC mode

5.32.1 Feature Description

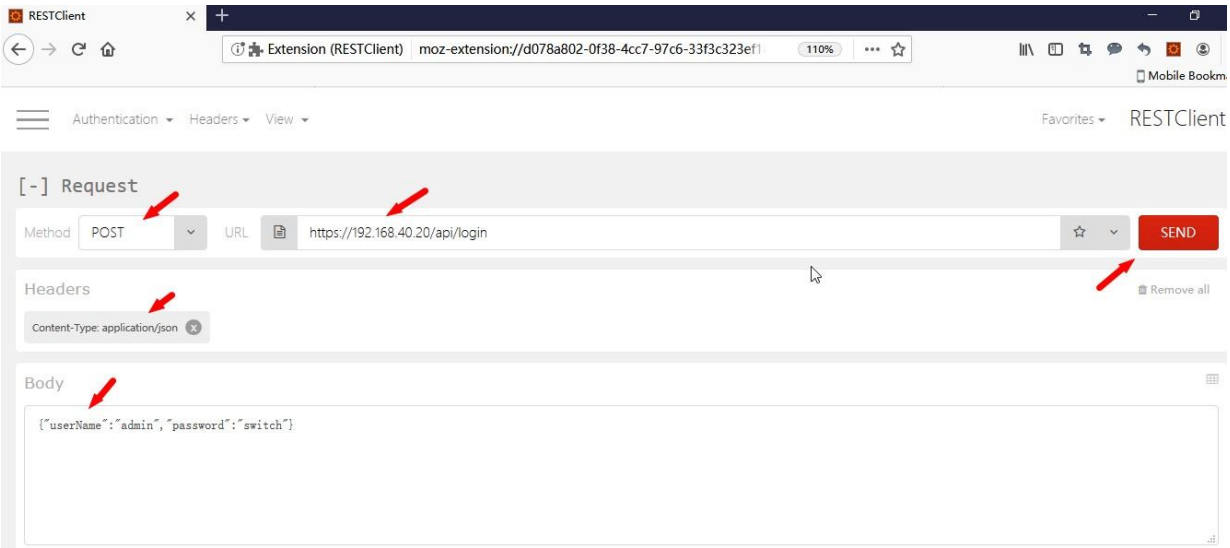
Provide Open API to disable/enable AP Radio in OVE/OVC mode

5.32.2 Configuration

First login the OV with https://OVIP/api/login on RESTClient as below

Method: POST

```
URL: https://OVIP/api/login
Headers: Content-Type:application/json
Body: {"userName":"admin","password":"switch"}
```



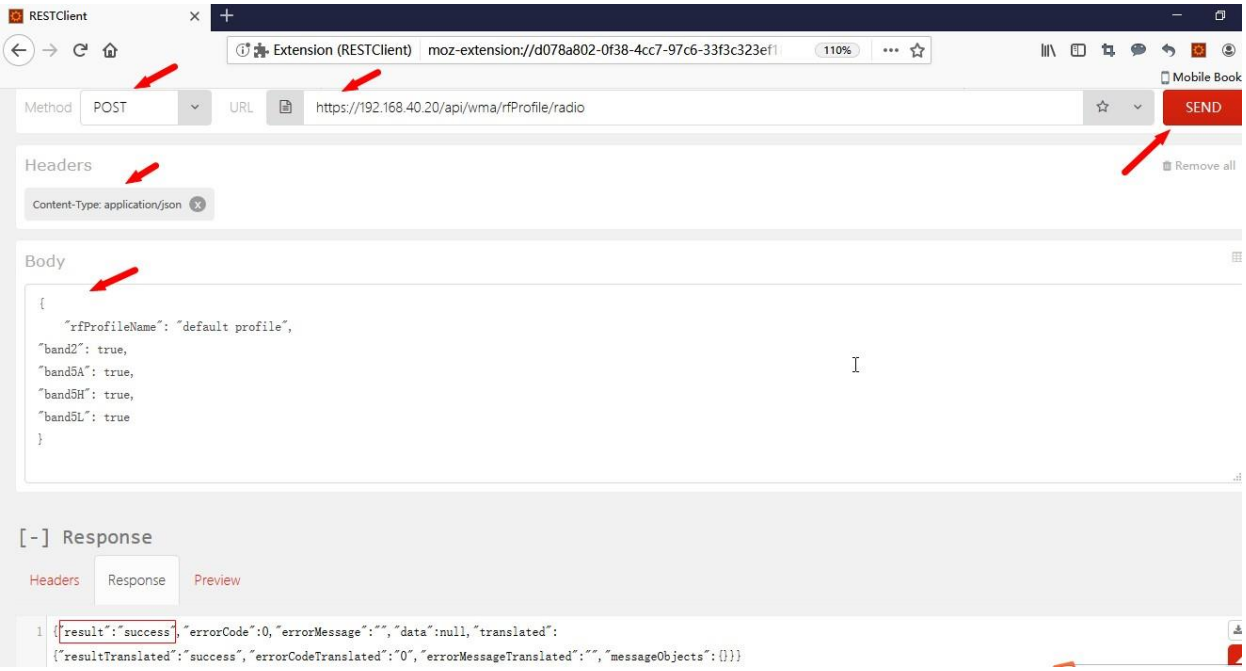
After click “SEND”, the response can be seen as below screenshot.

Edit the radio of the RF profile with https://OVIP/api/wma/rfProfile/radio on RESTClient as below

```
Method: POST
URL: https://OVIP/api/wma/rfProfile/radio
Headers: Content-Type:application/json
Body: { "rfProfileName": "default profile", "band2": true, "band5A": true,
"band5H": true, "band5L": true }
```

	2.4G	5G All	5G High	5G Low
1	true	true	true	true
2	true	true	true	false
3	true	true	false	true
4	true	true	false	false
5	true	false	true	true
6	true	false	true	false
7	true	false	false	true
8	true	false	false	false
9	false	true	true	true
10	false	true	true	false
11	false	true	false	true
12	false	true	false	false
13	false	false	true	true
14	false	false	true	false
15	false	false	false	true
16	false	false	false	false

After click “SEND”, the response can be seen as below screenshot.



The configured radio value is displayed on OVE/OVC—RF Profile web

5.33 Support Disable/Enable AP Radio in cluster mode

5.33.1 Feature description

Provide Open API to disable/enable AP Radio in cluster mode

Support disable/enable the AP radio switch on Cluster Web GUI

5.33.2 configuration

How to access the API interface and configure the radio in cluster mode:

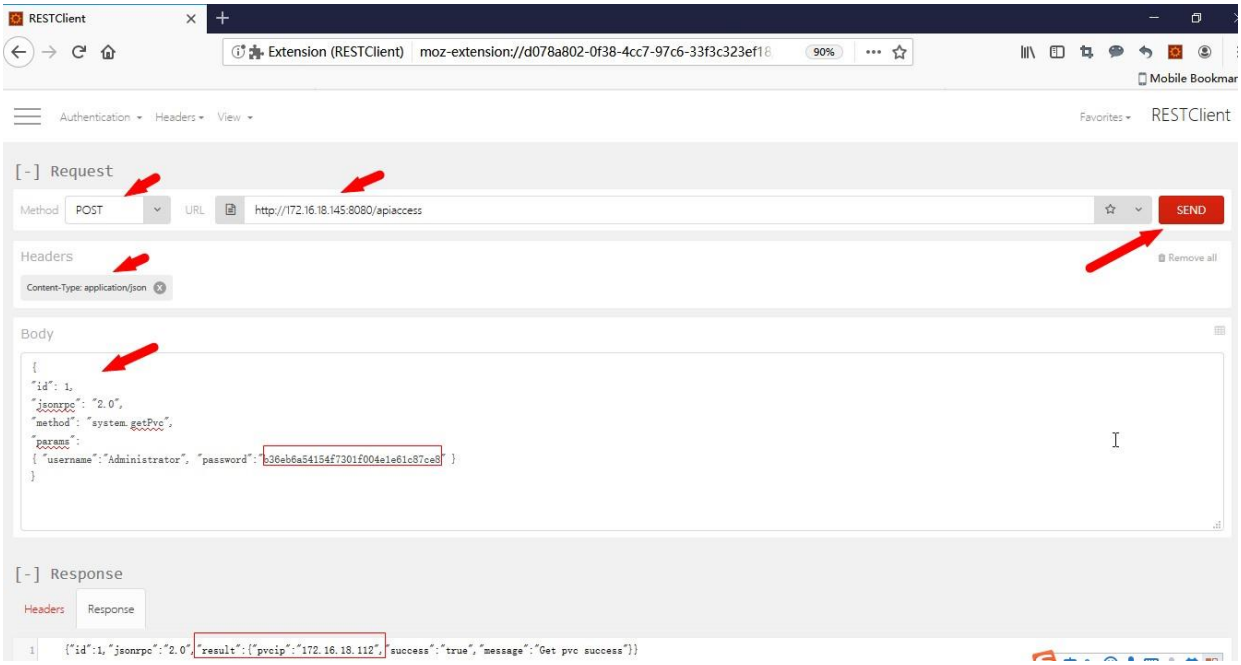
Get PVC IP address by access any AP of the cluster on RestClients.

```
Method: POST
URL: http://anyip address:8080/apiaccess
Headers: Content-Type:application/json
Body:
```

```
{
"id": 1,
"jsonrpc": "2.0",
"method": "system.getPvc",
"params":
{ "username":"Administrator", "password":"b36eb6a54154f7301f004e1e61c87ce8" }
}
```

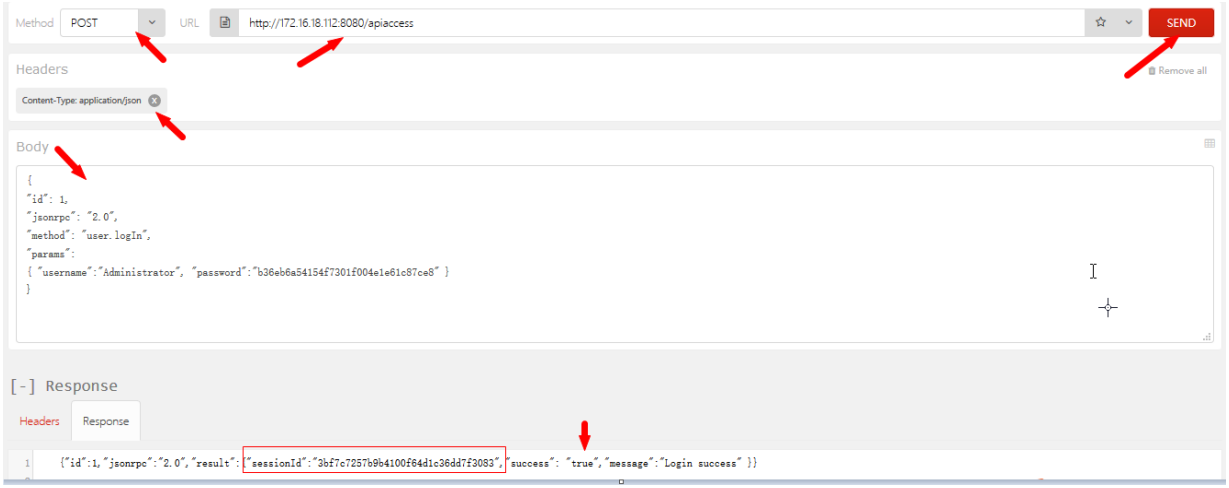
Note: Only use the Administrator account to log in.

The password is the md5 hash of “Administrator” and can be get by the result of “cat /var/config/man_user.conf”.



Login to PVC on RestClients

```
Method: POST
Headers: Content-Type:application/json

URL:http://pvcip address:8080/apiaccess
Body:
{
"id": 1,
"jsonrpc": "2.0",
"method": "user.logIn",
"params":
{ "username":"Administrator", "password":"b36eb6a54154f7301f004e1e61c87ce8" }
}
```

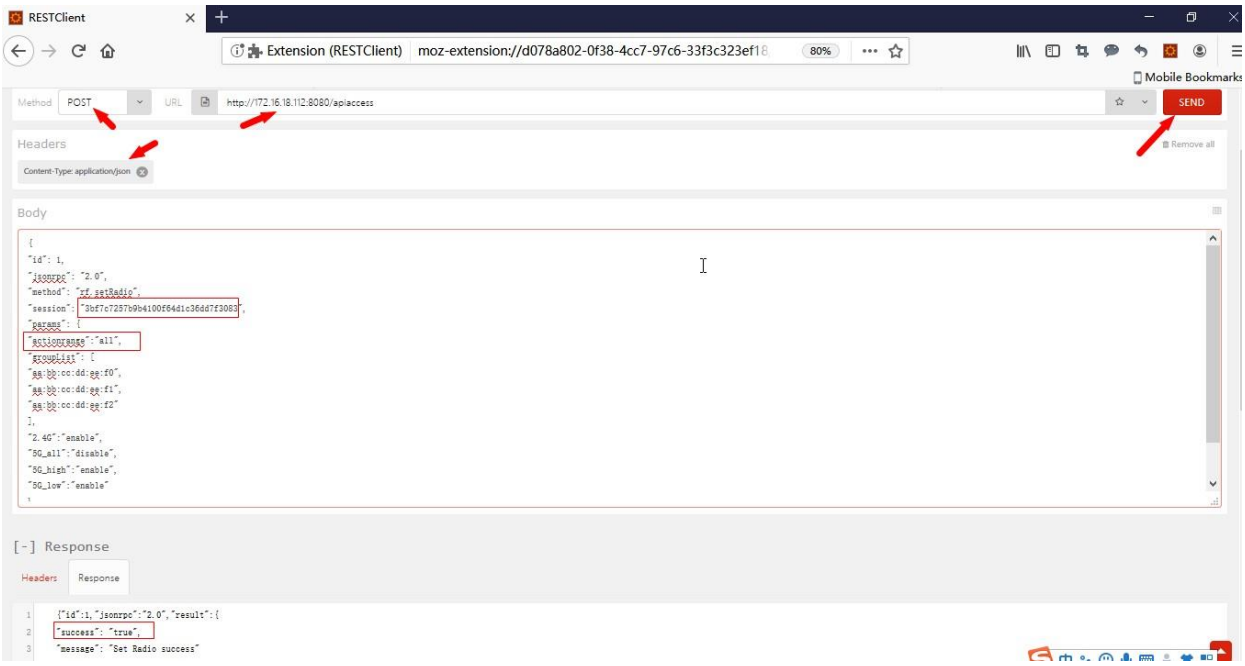


Note:
You must copy the sessionID for the next Step.
If the PVC switch, you need to rerun Step1 to get a new pvcip.

API access

```
Method: POST
Headers: Content-Type:application/json
Url: http://pvcip address:8080/apiaccess
Body:
{
"id": 1,
"jsonrpc": "2.0",
"method": "rf.setRadio",
"session": "3bf7c7257b9b4100f64d1c36dd7f3083",
"params": {
"actionrange":"all",
"groupList": [
"aa:bb:cc:dd:ee:f0",
"aa:bb:cc:dd:ee:f1",
"aa:bb:cc:dd:ee:f2"
],
"2.4G":"enable",
"5G_all":"disable",
"5G_high":"enable",
"5G_low":"enable"
}
}
```

	2.4G	5G All	5G High	5G Low
1	enable	enable	enable	enable
2	enable	enable	enable	disable
3	enable	enable	disable	enable
4	enable	enable	disable	disable
5	enable	disable	enable	enable
6	enable	disable	enable	disable
7	enable	disable	disable	enable
8	enable	disable	disable	disable
9	disable	enable	enable	enable
10	disable	enable	enable	disable
11	disable	enable	disable	enable
12	disable	enable	disable	disable
13	disable	disable	enable	enable
14	disable	disable	enable	disable
15	disable	disable	disable	enable
16	disable	disable	disable	disable



If no method is called within 10 minutes, the session will be invalid. Only by re-executing Step2 can get a valid session.

Note:

We can configure the radio for all the AP of the cluster by filling “all” in the body, also we can configure specific APs by filling “group” and filling the mac addresses in the grouplist.

How to access the API interface and configure the radio in cluster mode:

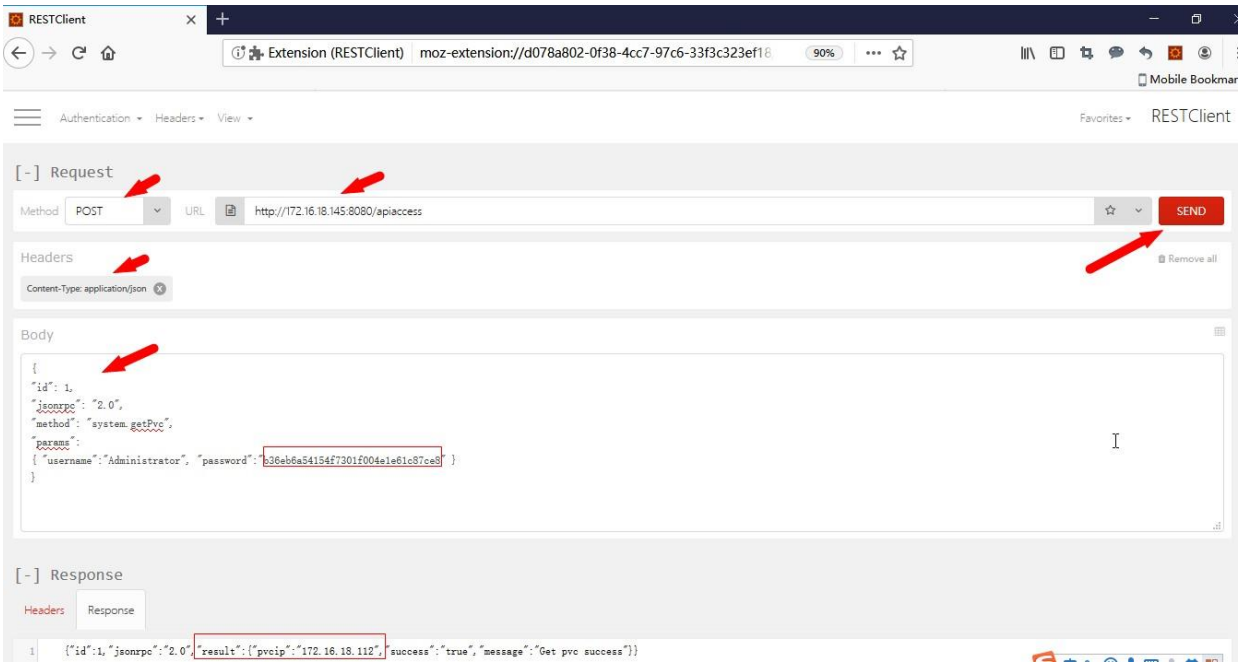
Get PVC IP address by access any AP of the cluster on RestClients.

```
Method: POST
URL: http://anyip address:8080/apiaccess
Headers: Content-Type:application/json
Body:
{
"id": 1,
"jsonrpc": "2.0",
"method": "system.getPvc",
"params":
```

```
{ "username":"Administrator", "password":"b36eb6a54154f7301f004e1e61c87ce8" }
}
```

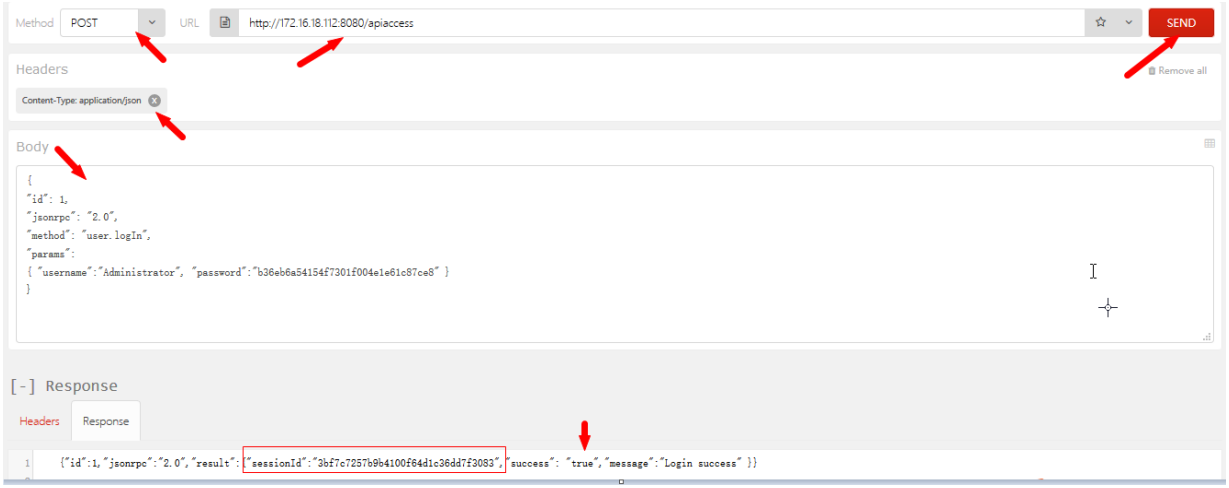
Note: Only use the Administrator account to log in.

The password is the md5 hash of “Administrator” and can be get by the result of “cat /var/config/man_user.conf ”



Login to PVC on RestClients

```
Method: POST
Headers: Content-Type:application/json

URL:http://pvcip address:8080/apiaccess
Body:
{
"id": 1,
"jsonrpc": "2.0",
"method": "user.logIn",
"params":
{ "username":"Administrator", "password":"b36eb6a54154f7301f004e1e61c87ce8" }
}
```

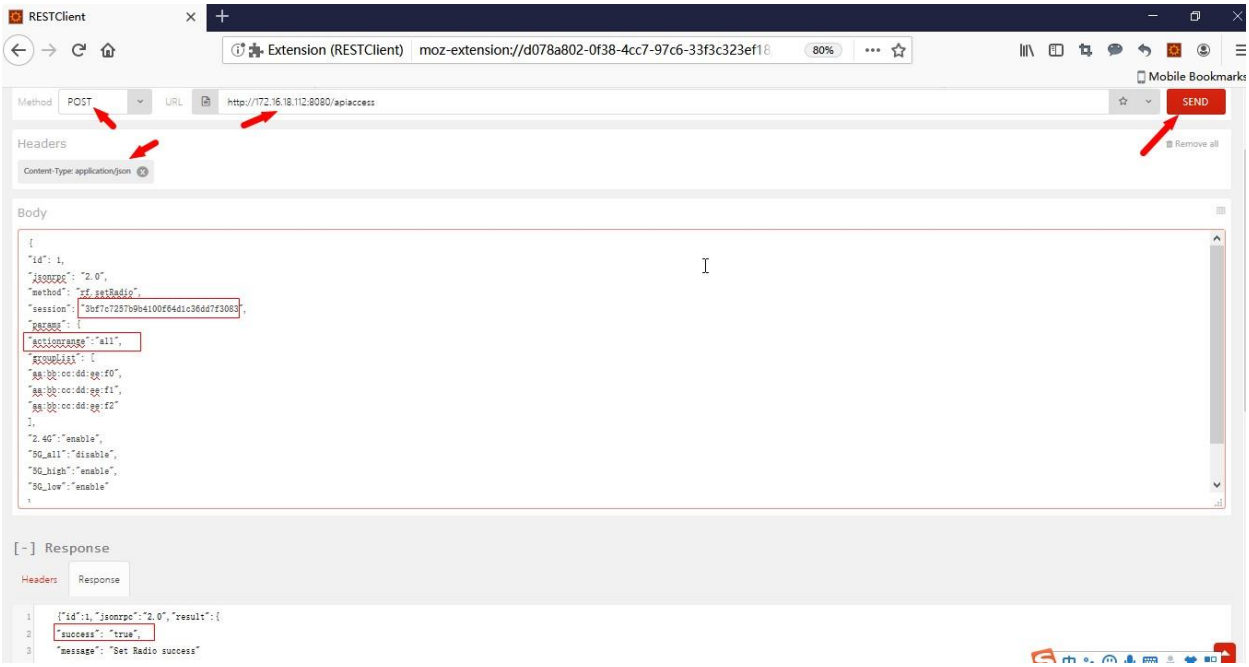


Note:
You must copy the sessionID for the next Step.
If the PVC switch, you need to rerun Step1 to get a new pvcip.

API access

```
Method: POST
Headers: Content-Type:application/json
Url: http://pvcip address:8080/apiaccess
Body:
{
"id": 1,
"jsonrpc": "2.0",
"method": "rf.setRadio",
"session": "3bf7c7257b9b4100f64d1c36dd7f3083",
"params": {
"actionrange":"all",
"groupList": [
"aa:bb:cc:dd:ee:f0",
"aa:bb:cc:dd:ee:f1",
"aa:bb:cc:dd:ee:f2"
],
"2.4G":"enable",
"5G_all":"disable",
"5G_high":"enable",
"5G_low":"enable"
}
}
```

	2.4G	5G All	5G High	5G Low
1	enable	enable	enable	enable
2	enable	enable	enable	disable
3	enable	enable	disable	enable
4	enable	enable	disable	disable
5	enable	disable	enable	enable
6	enable	disable	enable	disable
7	enable	disable	disable	enable
8	enable	disable	disable	disable
9	disable	enable	enable	enable
10	disable	enable	enable	disable
11	disable	enable	disable	enable
12	disable	enable	disable	disable
13	disable	disable	enable	enable
14	disable	disable	enable	disable
15	disable	disable	disable	enable
16	disable	disable	disable	disable



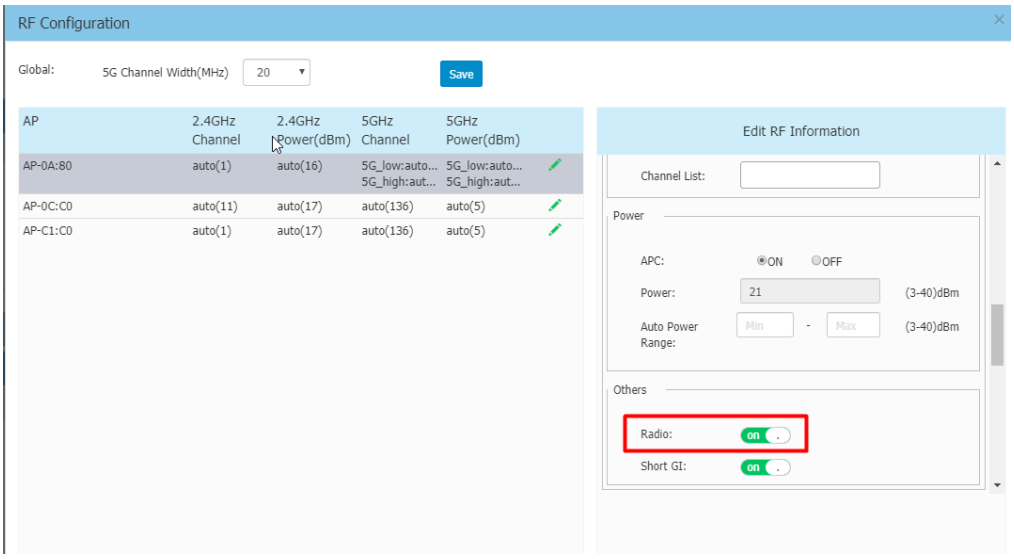
If no method is called within 10 minutes, the session will be invalid. Only by re-executing Step2 can get a valid session.

Note:

We can configure the radio for all the AP of the cluster by filling “all” in the body, also we can configure specific APs by filling “group” and filling the mac addresses in the grouplist.

How to configure the radio in WEB GUI directly in cluster mode

Path: login AP Web>>Wireless>> RF>> RF Configuration>> Edit RF Information



5.34 Hotspot2.0

5.34.1 Feature description

More often in public venues, a Hotspot 2.0 network helps facilitate wireless clients to seamlessly connect (offload) to known Wi-Fi services from the expensive 3G/4G wireless network. Passpoint is the WFA certification that APs and wireless devices comply with to work in a Hotspot 2.0 network. In summary a Hotspot 2.0 network supports Passpoint certified devices in the process of network discovery, registration, provisioning and access.

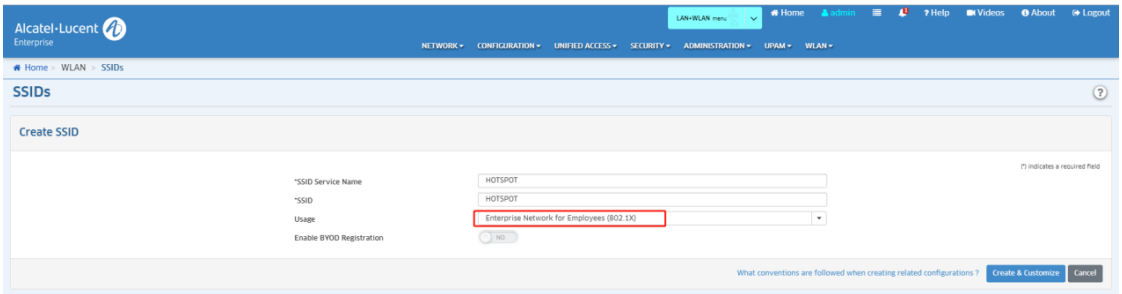
5.34.2 Topology

Same topology as in section 5.14.2

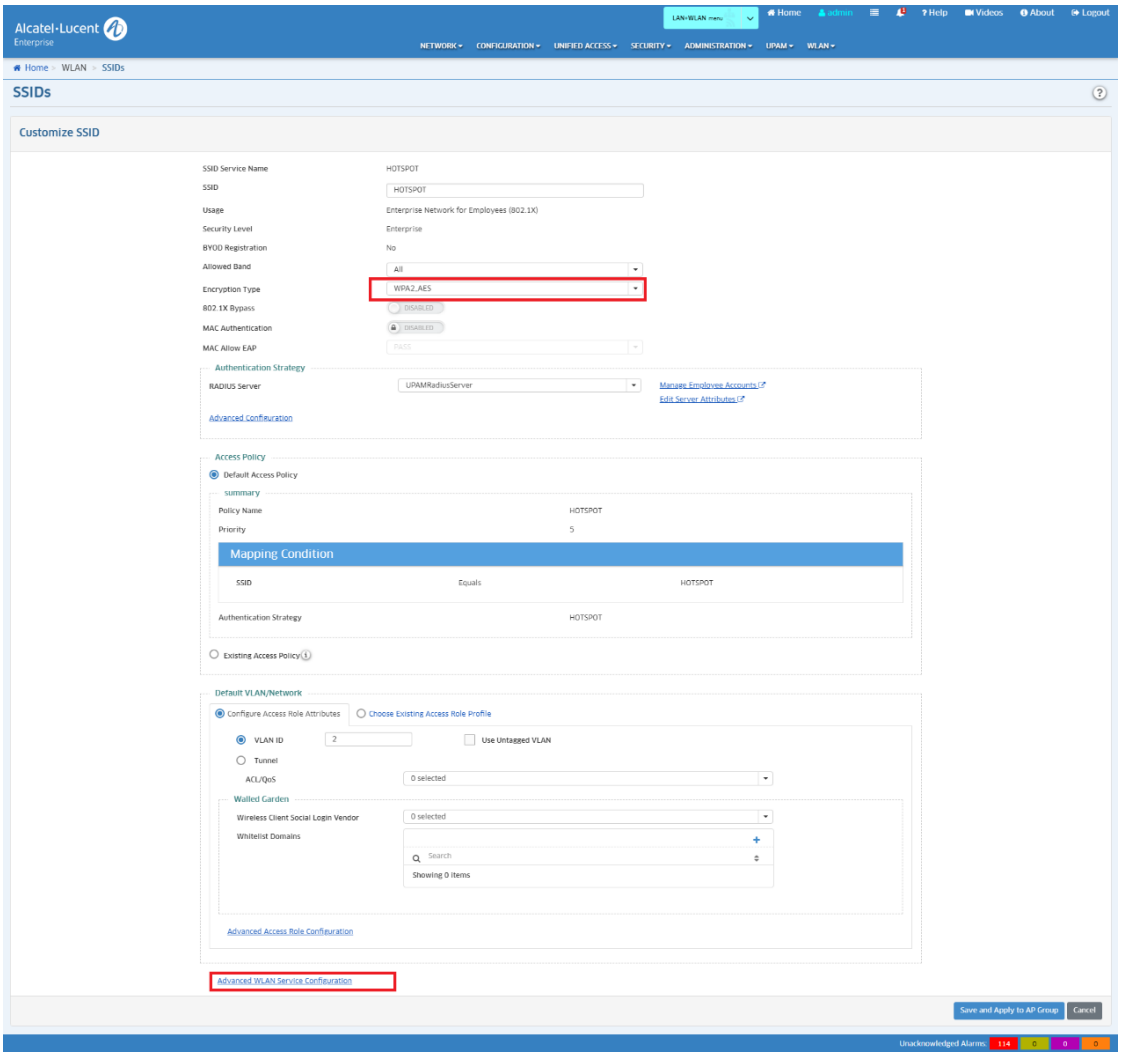
5.34.3 Configuration

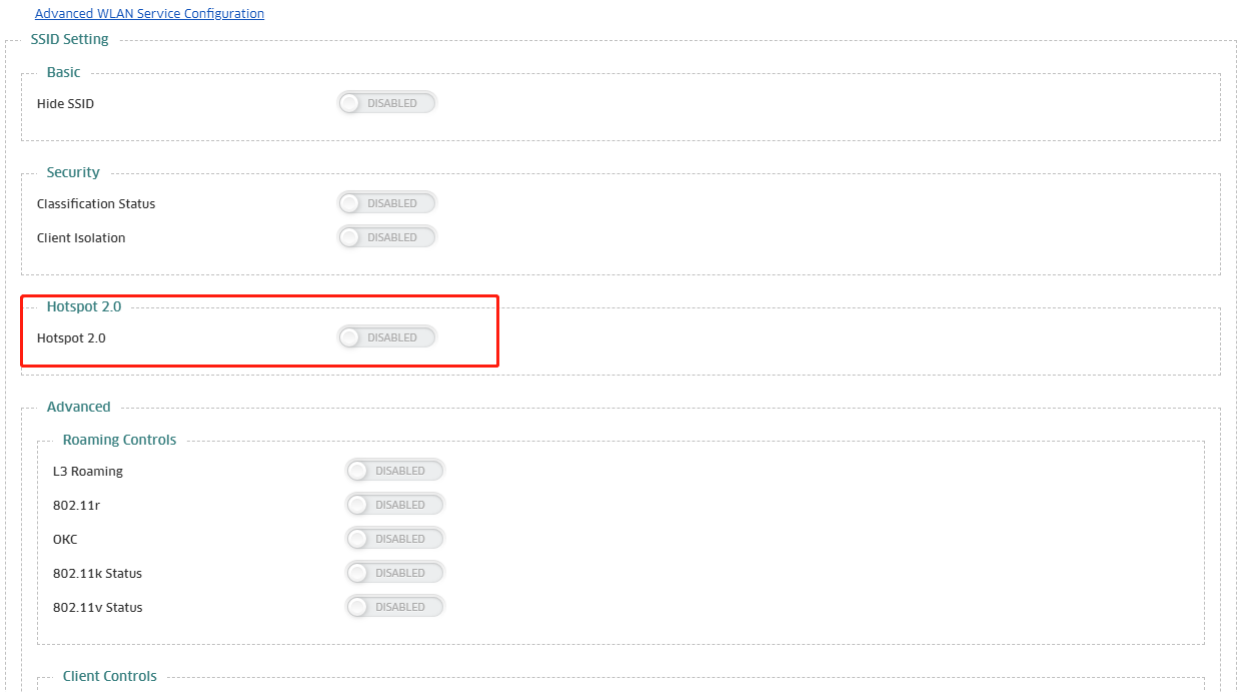
OV configuration:

Home->WLAN->SSIDs,create SSID with Enterprise Network for Employees (802.1X):

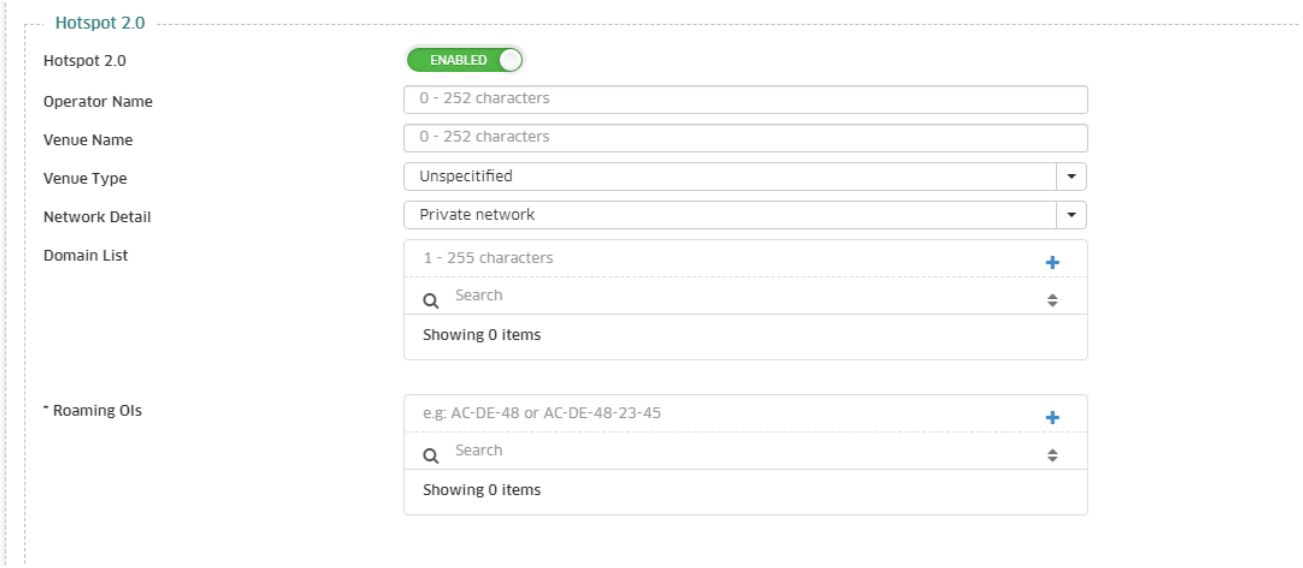


Choose Encryption Type with WPA2_AES or WPA3_AES256,click Advanced WLAN Service Configuration:



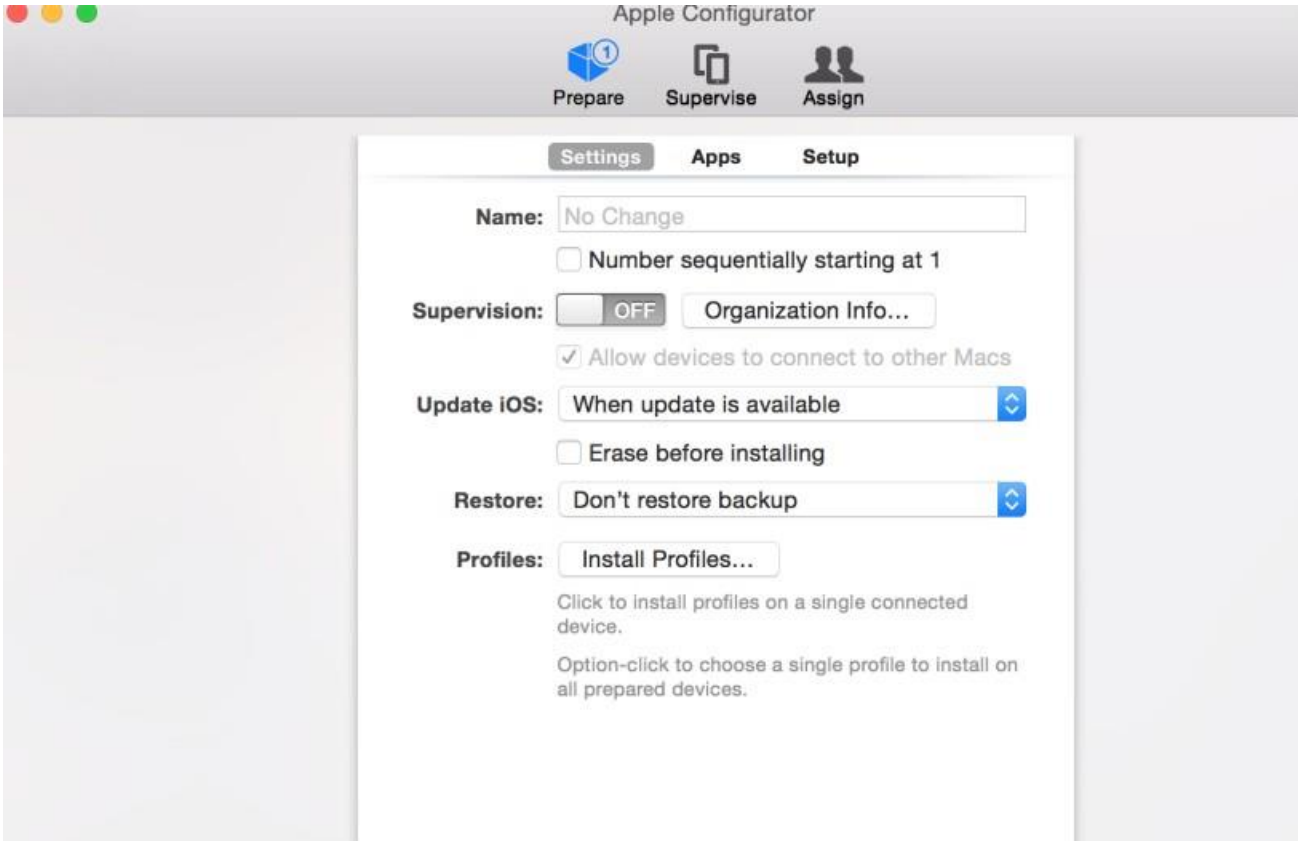


Enable Hotspot2.0 and configure the parameters,then apply to your group:



(1) Client-side configuration:

When Apple Configurator first opens, click the Prepare button at the top of the page, then click the Install Profiles... button:



Ensure that you have an iOS device plugged in, then click the Next button when it appears:

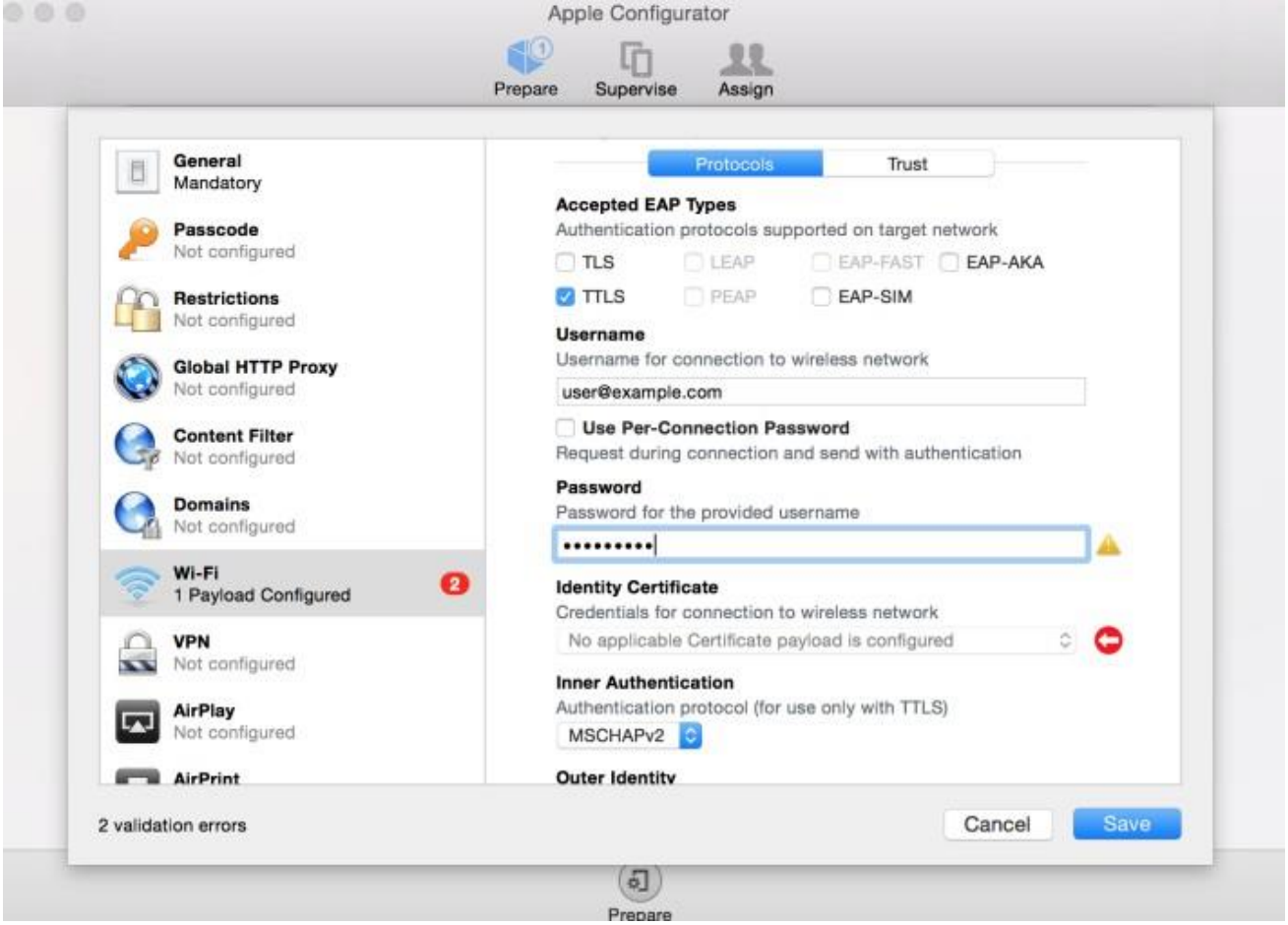
Click New Profile and give it a unique name. For this example, the iOS profile is named Meraki Hotspot 2.0 Demo:

Now that a profile has been created, it must be configured with the appropriate Hotspot 2.0 network information: SSID & Network Type

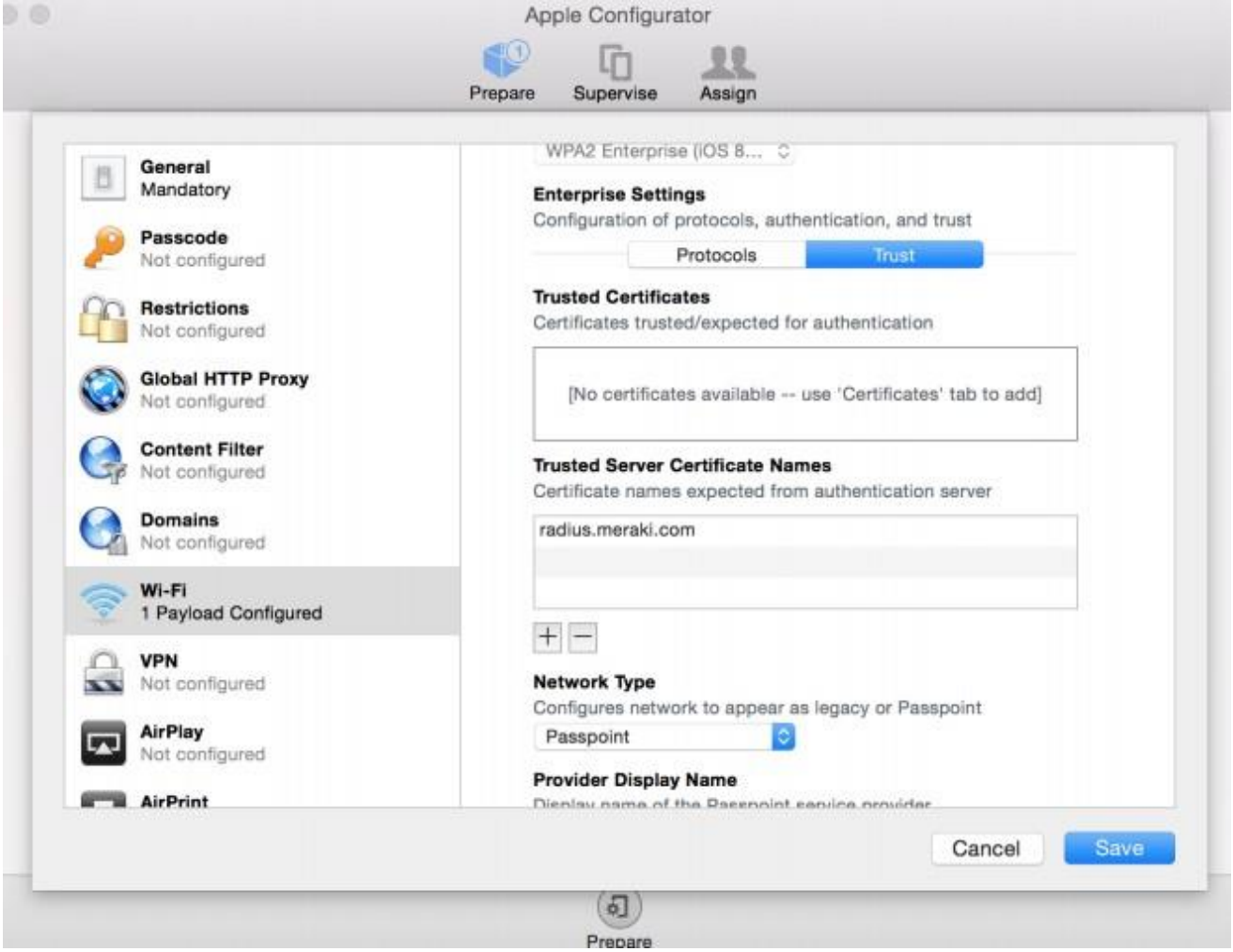
Leave the SSID blank and change the Network Type to Passpoint:

Select the Accepted EAP Types for your configuration. In this example, we are using TTLS because we are interfacing with the Meraki Hosted 802.1X RADIUS server.

Enter the Username and Password for the user that was created earlier:

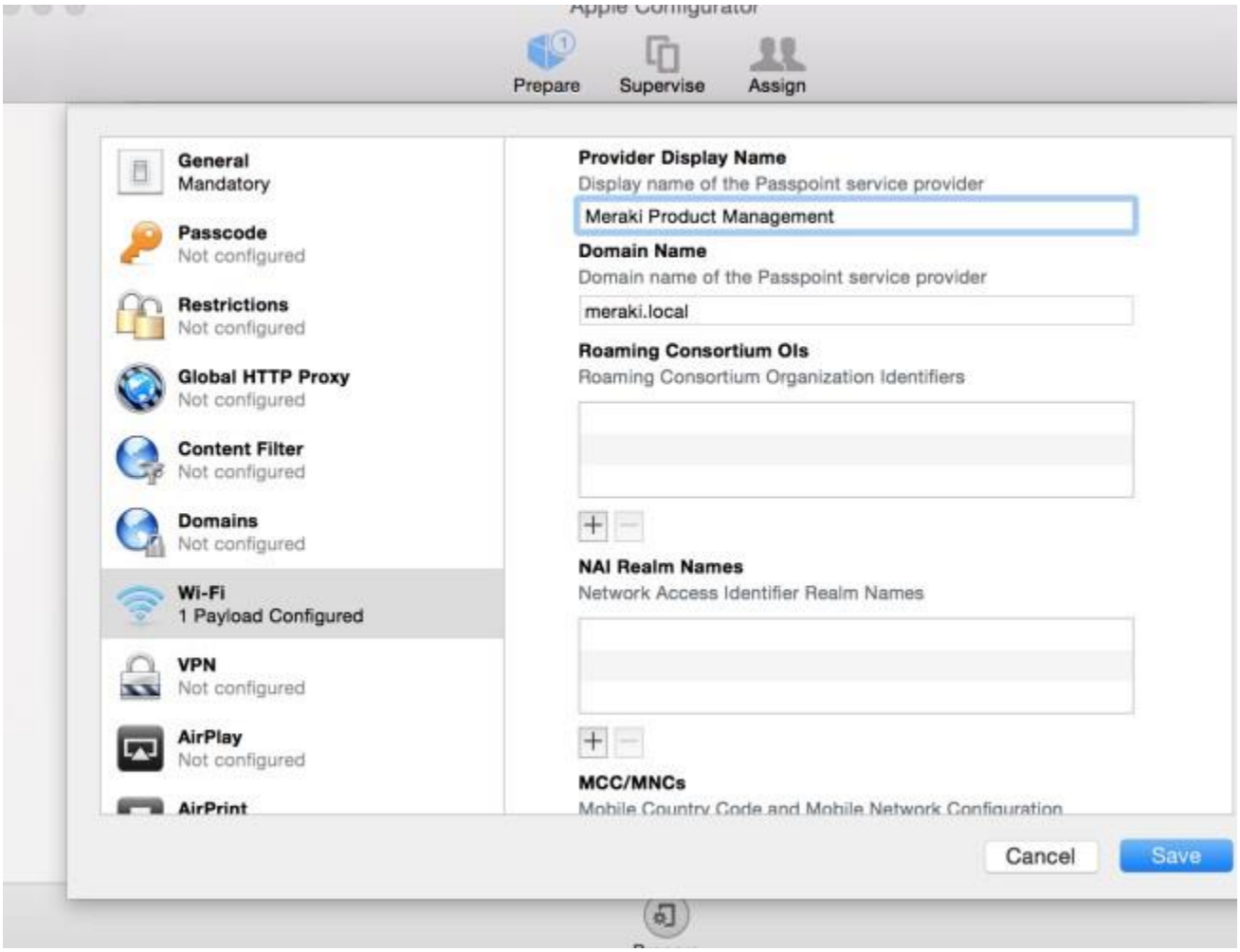


Under the Trust tab, enter radius.meraki.com as a Trusted Server Certificate Name.

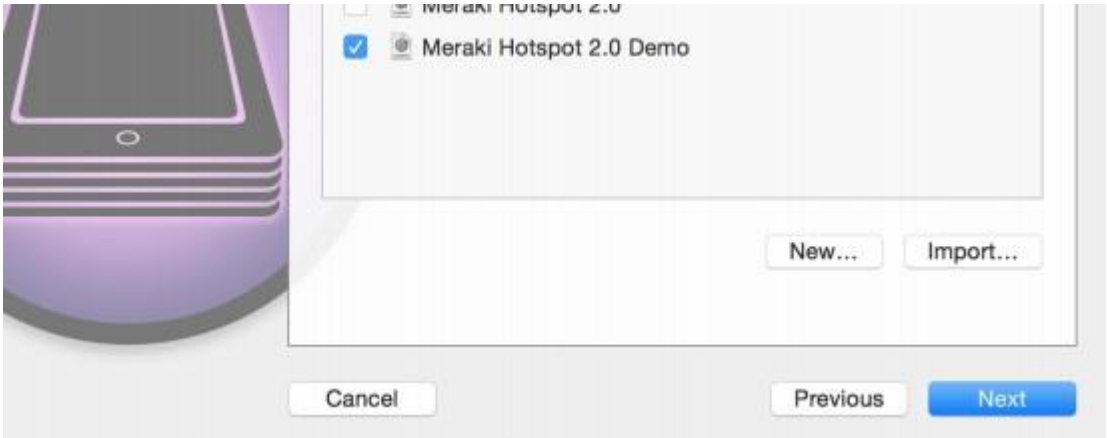


Enter the Passpoint service provider as the Provider Display Name. Additionally, add the Hotspot 2.0 Domain Name as configured in Dashboard.

This example uses Meraki Product Management as the service provider name and meraki.local as the Domain.

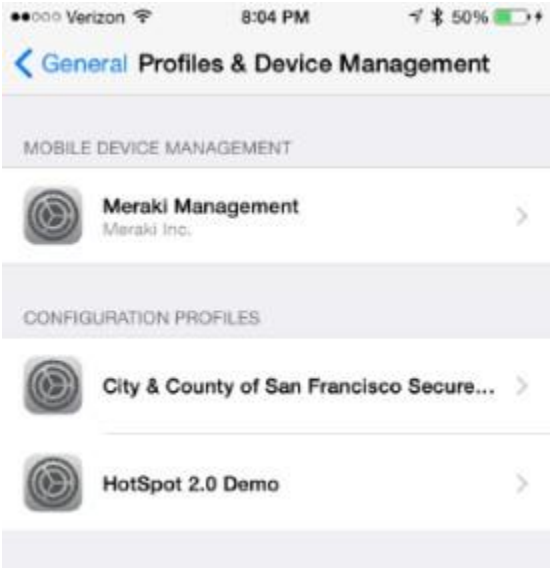


Click Save on the main configuration dialog box. Check the box next to the newly created proflle and click Next to apply it to the device.

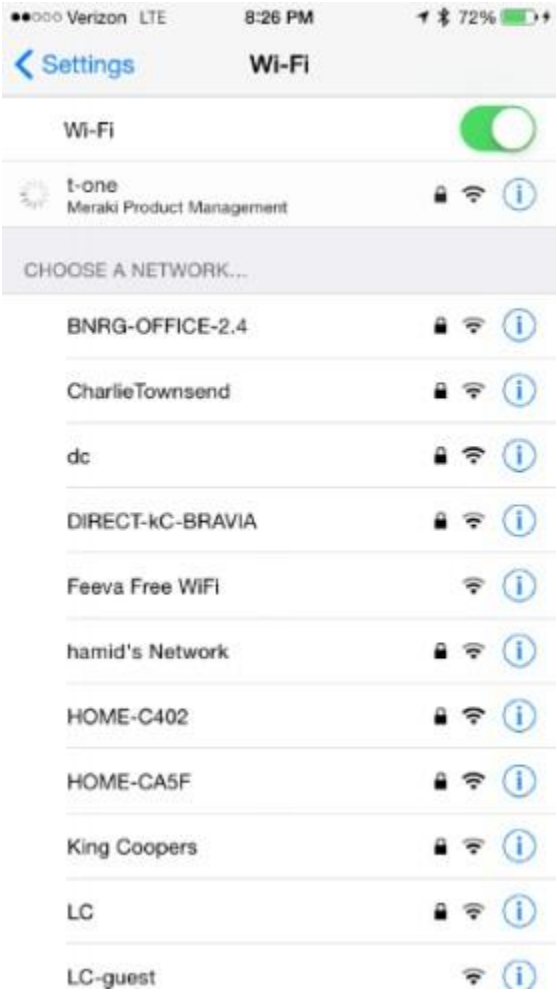


On the iOS device, follow the on-screen instructions to install the profile:

Ensure that the new profile is listed in the Profiles on the device. There may be multiple profiles on the device; in this example the device has two other profiles, including the Meraki MDM profile:



Ensure that there are no other preferred Wireless networks within range of the device. When the Hotspot 2.0 SSID is the only SSID within range, the iPhone will join the network automatically:



5.34.4 Attention

Only Enterprise WPA2_AES and Enterprise WPA3_AES256 support hotspot2.0.

The hotspot2.0 parameters on SSID must include the configuration on client.

5.35 IoT Device Profiling

5.35.1 Feature description

The proliferation of IoT, BYOD, mobile devices require that the network administration evolve the way they manage from traditional connected devices. As network engineers are challenged to support large numbers of smartphones and tablets in addition to laptops and desktops, there is a need for reliably and dynamically identifying devices, make sure these devices are compliant and to enforce required polices on these devices.

Gaining visibility into IoT device types is essential for network engineers to build granular access policies for security and quality of service (QoS) for critical enterprise applications. It is becoming increasingly imperative for the network administrators to do the following things

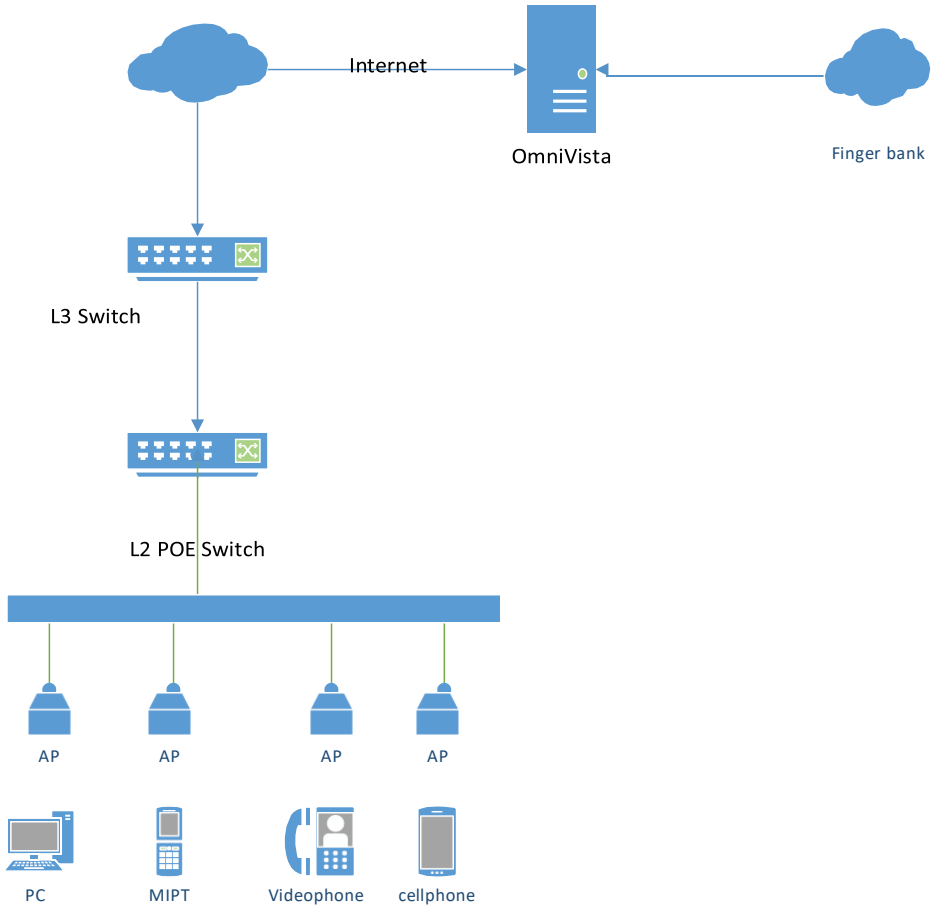
To be able to view, identify & catalog the various IoT devices connecting to the network

To authenticate the devices and tracking authentication status

On-board or profile the device in a category for uniform application of policies

It is required that Switch/AP collect profiling information by snooping the network packets that acts as a fingerprint to uniquely identify the device and sent to network management for identifying and categorizing the device. Fingerprinting information include dhcp fingerprints, dhcp vendor, http user-agents, dns hostnames etc.

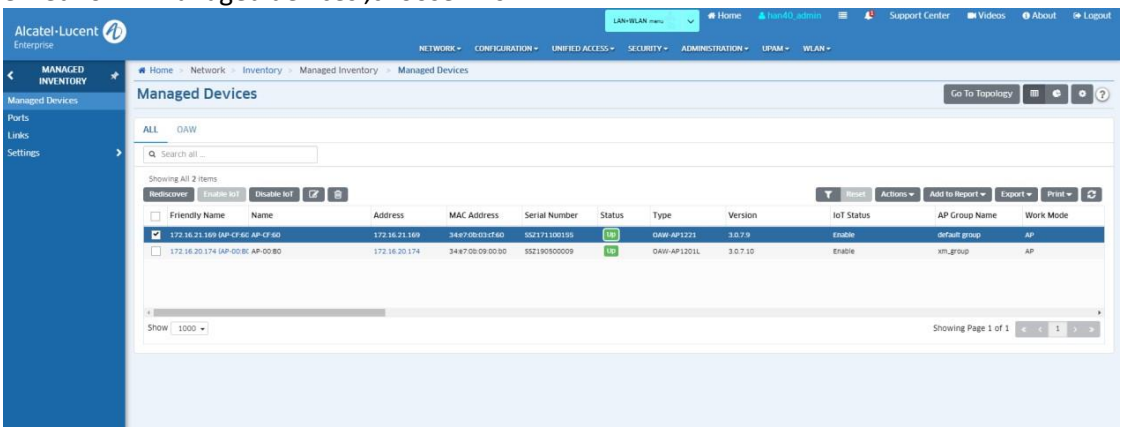
5.35.2 Topology



5.35.3 Configuration

Switch of IoT

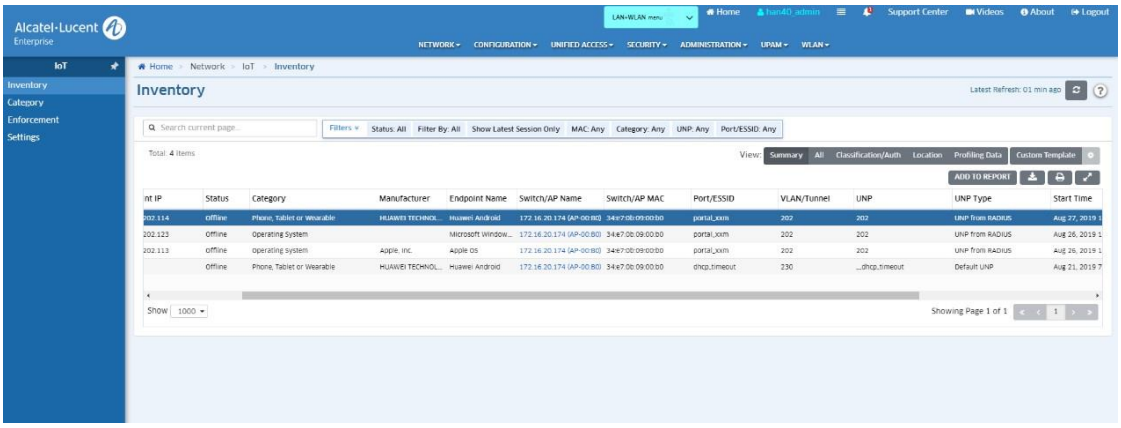
Open the Network->Managed devices ,choose APs



Pic 3.1 Enable/Disable IoT

Inventory

Open the Network->IoT->Inventory ,check information



Pic 3.2 IoT inventory

Information Type

No	Parameter	Description	Values
1	deviceMac	MAC address of Switch/AP	
2	ip	Endpoint IP address	
3	opt55	DHCP Option 55	
4	opt60	DHCP Option 60	
5	userAgents	HTTP user-agents	
6	hosts	DNS hostnames	
7	port	Port number /ESSID	
8	portType	Type of the port where the endpoint is connected	Wired UNP
			Wireless
9	portDesc	Port Alias/ WLAN service	
10	vlan	VLAN number	
11	unp	UNP profile name	
12	unpType	This identifies how the UNP profile got assigned by the Switch/AP	Default UNP
			UNP from classification
			UNP from RADIUS
13	authType	Authentication type.	1: None
			2: 802.1X
			3: MAC
14	authStatus	Authentication status	1: Passed
			2: Failed
			3: Server Unreachable
15	connError	This identifies the reason why the endpoint failed to connect to the nework.	1: 802.1x authentication failure – invalid certificate
			2: 802.1x authentication failure – invalid credentials
			3: 802.1x authentication timeout
			4: MAC Authentication failure
			5: MAC Authentication timeout
			10: DHCP Timeout
			33: PSK authentication failure

5.36 Security Issues for AP Software

5.36.1 Feature description

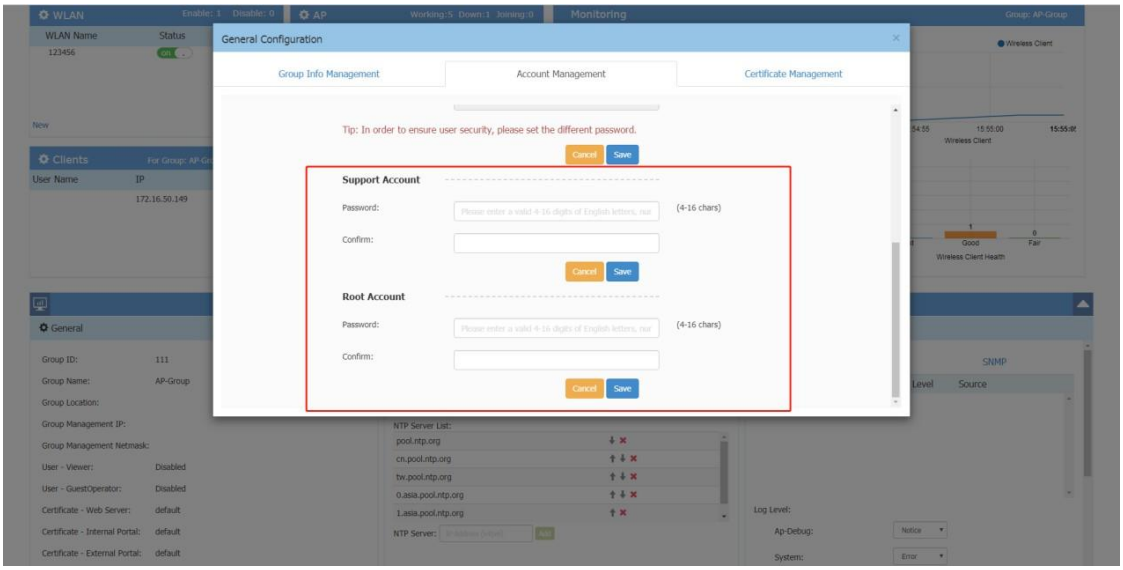
Support Access default password change in Express mode. “Privilege Technical Access” key definition on AP, helps derives root password. Should be modifiable. Factory reset of AP sets it to default value.

5.36.2 Topology

Same topology as in section 5.14.2.

5.36.3 Configuration

1) Cluster Main page-> System-> General-> General Configuration->Account Management,you can configure Support Account and Root Account:

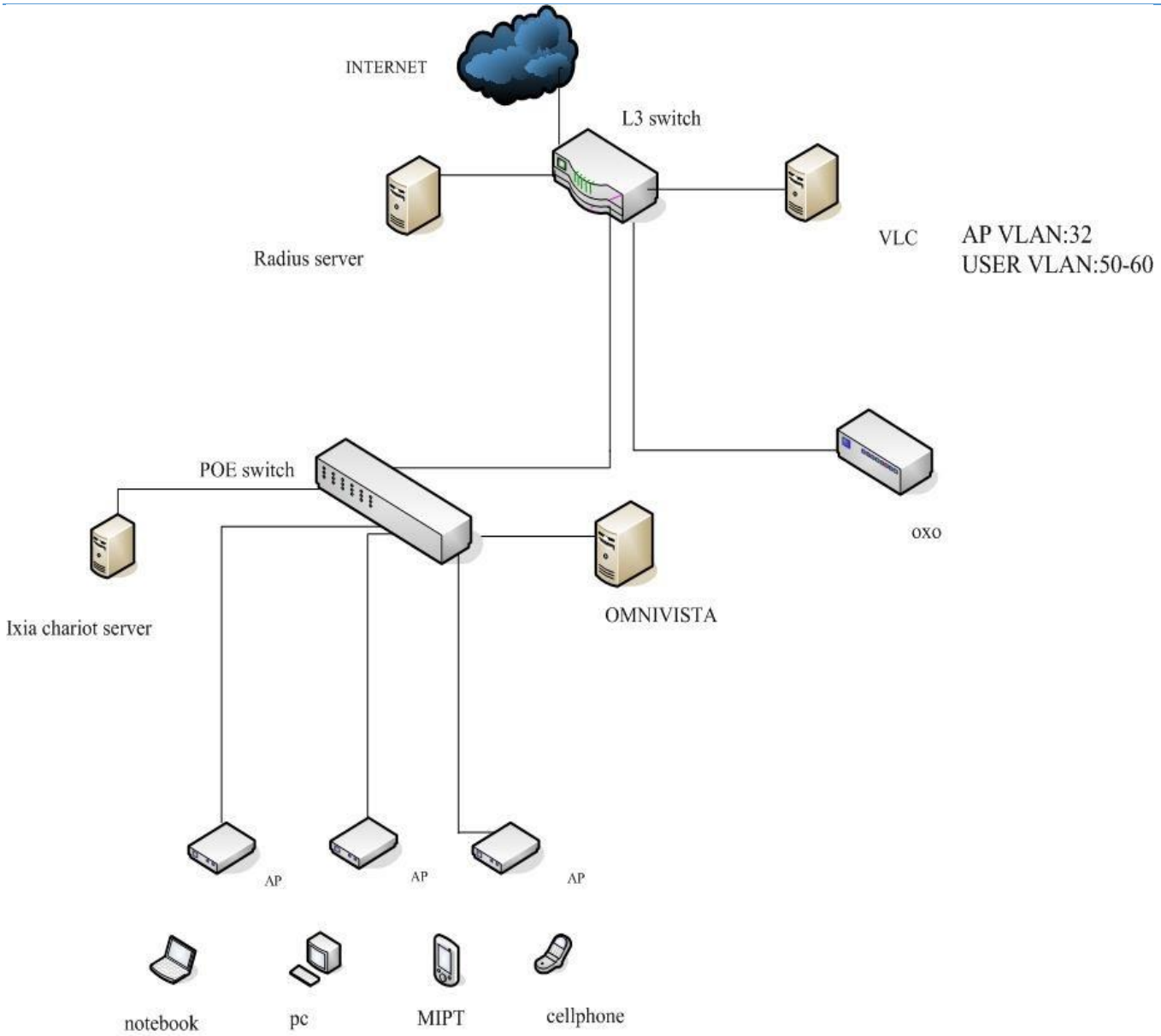


5.37 Show client username for 802.1x clients(Cluster)

5.37.1 Feature description

AP has already supported show the client authenticating portal username in Stellar UI. However for 802.1x clients authenticating using EAP-PEAP, the client username is empty. We should display Radius username attribute in all Radius authentication modes.

5.37.2 Topology



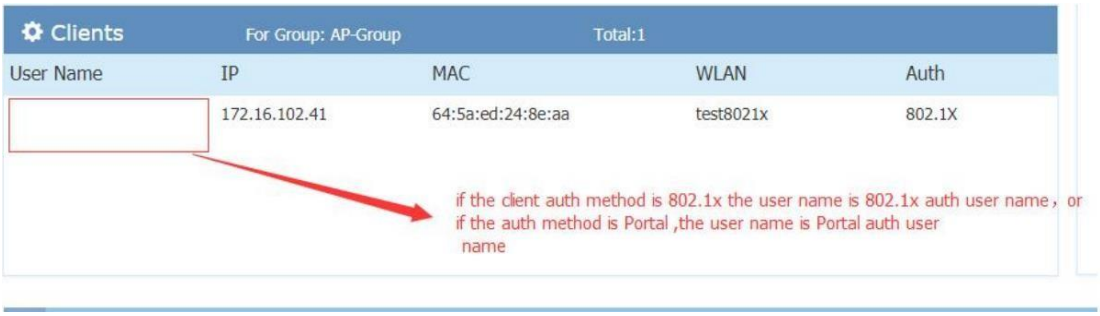
5.37.3 Configuration

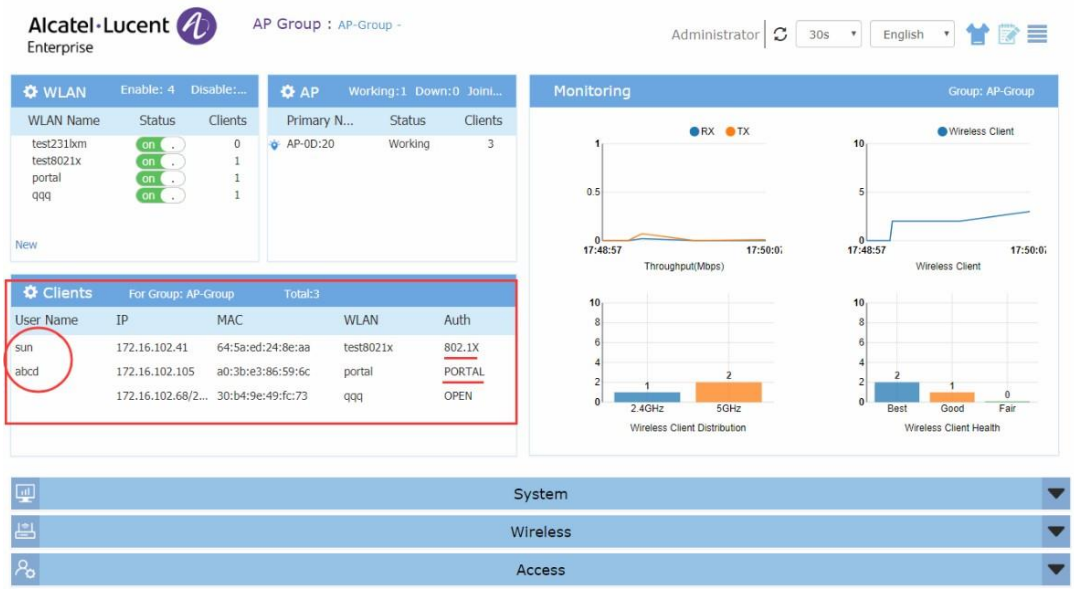
User name display under different authentication modes:

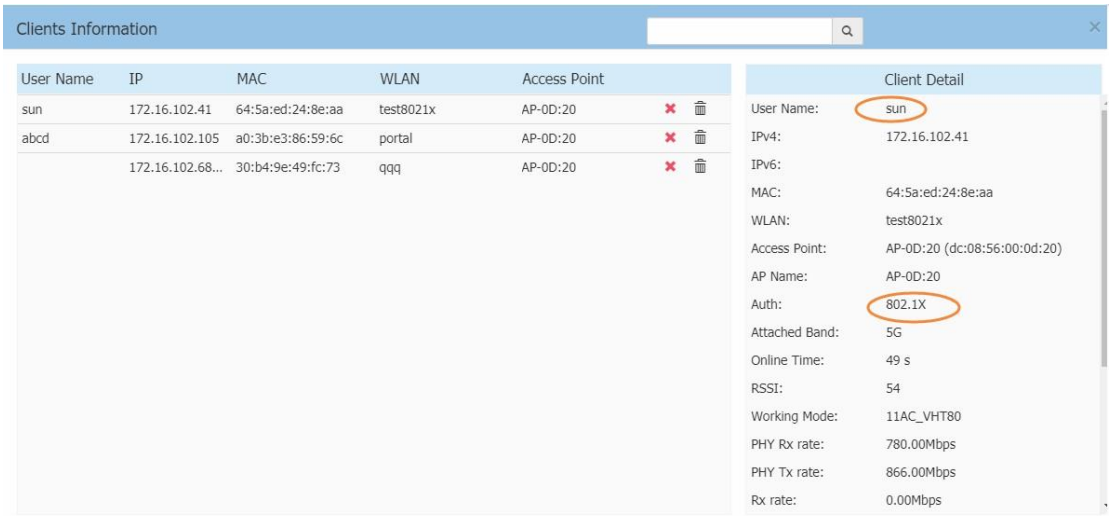
Portal mode authentication user, the user name is the portal name;

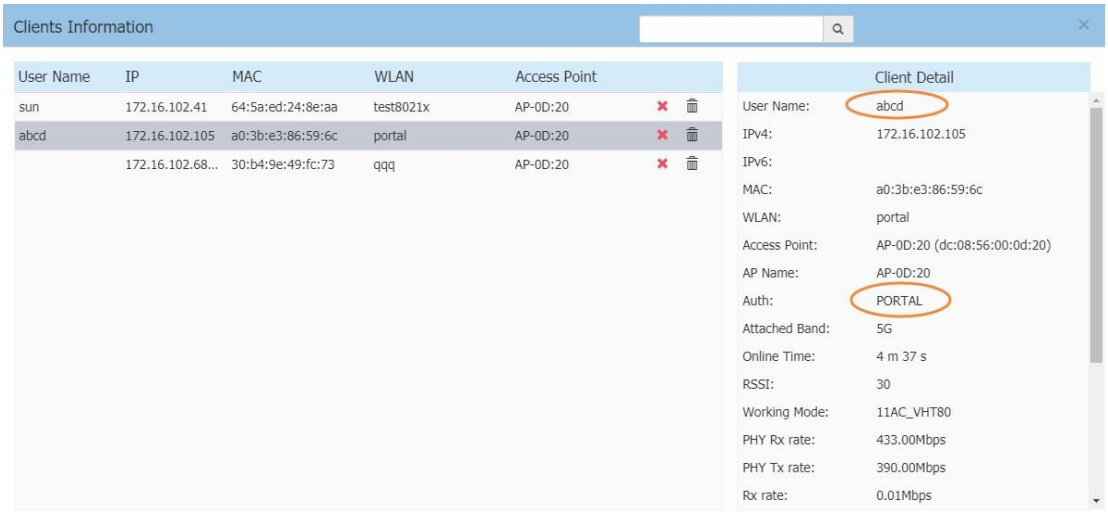
802.1x authenticated user, the username is the associated 802.1x name;

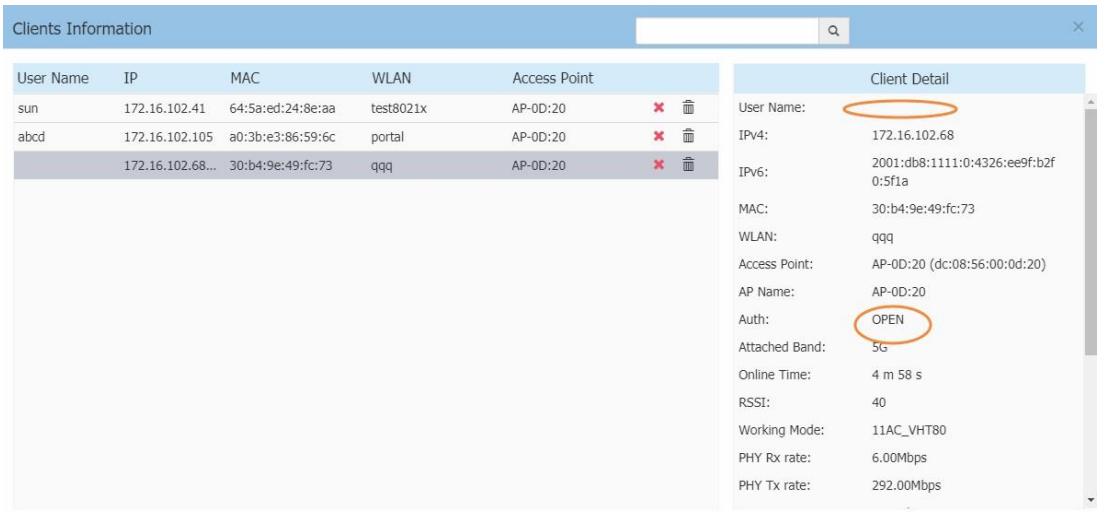
Authentication of other WLAN modes, including open, and the username is empty.




Alcatel·Lucent Enterprise
AP Group : AP-Group
Administrator
30s
English
WLAN Enable: 4 Disable:...
WLAN Name Status Clients
test231bxm on 0
test8021x on 1
portal on 1
qqq on 1
New
AP Working:1 Down:0 Joini...
Primary N... Status Clients
AP-0D:20 Working 3
Monitoring Group: AP-Group
RX TX
Throughput(Mbps)
Wireless Client
Wireless Client Distribution
Wireless Client Health
Clients For Group: AP-Group Total:3
User Name IP MAC WLAN Auth
sun 172.16.102.41 64:5a:ed:24:8e:aa test8021x 802.1X
abcd 172.16.102.105 a0:3b:e3:86:59:6c portal PORTAL
172.16.102.68/2... 30:b4:9e:49:fc:73 qqq OPEN
System
Wireless
Access


Clients Information
User Name IP MAC WLAN Access Point
sun 172.16.102.41 64:5a:ed:24:8e:aa test8021x AP-0D:20
abcd 172.16.102.105 a0:3b:e3:86:59:6c portal AP-0D:20
172.16.102.68... 30:b4:9e:49:fc:73 qqq AP-0D:20
Client Detail
User Name: sun
IPv4: 172.16.102.41
IPv6:
MAC: 64:5a:ed:24:8e:aa
WLAN: test8021x
Access Point: AP-0D:20 (dc:08:56:00:0d:20)
AP Name: AP-0D:20
Auth: 802.1X
Attached Band: 5G
Online Time: 49 s
RSSI: 54
Working Mode: 11AC_VHT80
PHY Rx rate: 780.00Mbps
PHY Tx rate: 866.00Mbps
Rx rate: 0.00Mbps


Clients Information
User Name IP MAC WLAN Access Point
sun 172.16.102.41 64:5a:ed:24:8e:aa test8021x AP-0D:20
abcd 172.16.102.105 a0:3b:e3:86:59:6c portal AP-0D:20
172.16.102.68... 30:b4:9e:49:fc:73 qqq AP-0D:20
Client Detail
User Name: abcd
IPv4: 172.16.102.105
IPv6:
MAC: a0:3b:e3:86:59:6c
WLAN: portal
Access Point: AP-0D:20 (dc:08:56:00:0d:20)
AP Name: AP-0D:20
Auth: PORTAL
Attached Band: 5G
Online Time: 4 m 37 s
RSSI: 30
Working Mode: 11AC_VHT80
PHY Rx rate: 433.00Mbps
PHY Tx rate: 390.00Mbps
Rx rate: 0.01Mbps



5.37.4 Attention

If the username is not displayed, please check the following:

Check the authentication mode: Only the portal authentication and 802.1x authentication will display the username. The other authentication methods are empty.

This field is empty when the client authenticate failed.

5.38 Social login wechat

5.38.1 Feature description

In the previous social login, we added the authentication method of wechat, which supports mobile terminal and PC. The mobile terminal will jump to the application, and the PC will generate a QR code and scan the code with the mobile terminal.

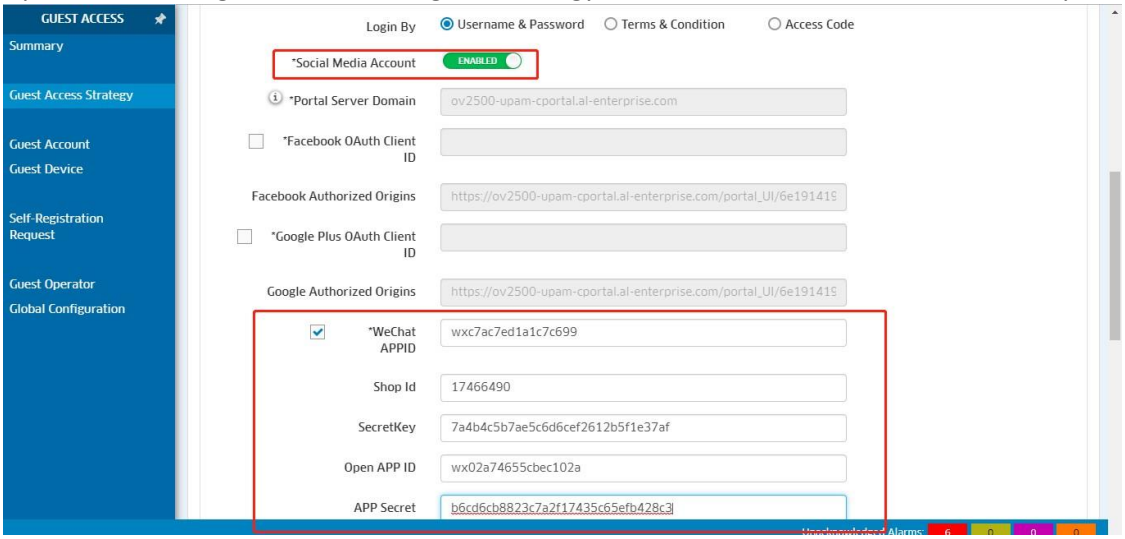
5.38.2 Configuration

Pre-configured WeChat authentication

Please refer to appendix 8.1

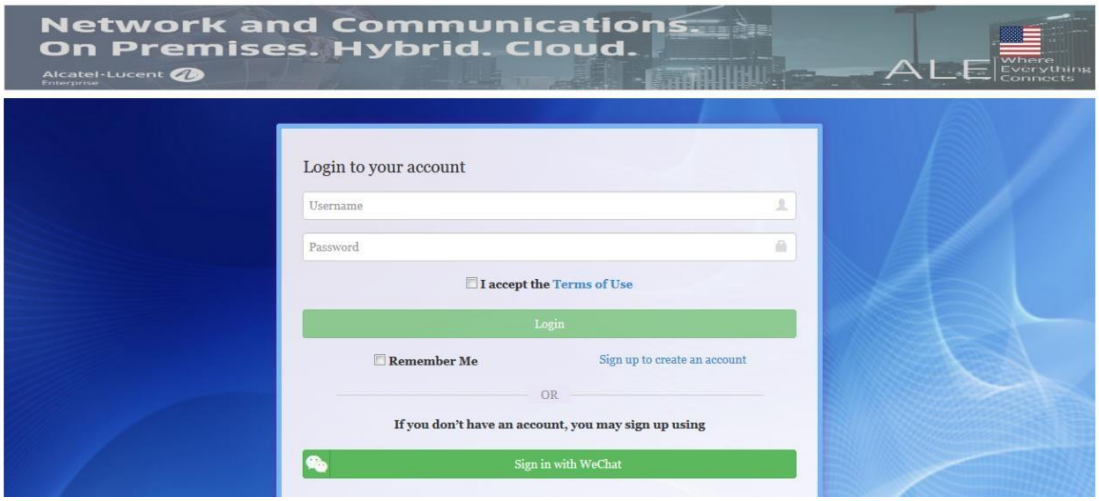
Create portal WLAN

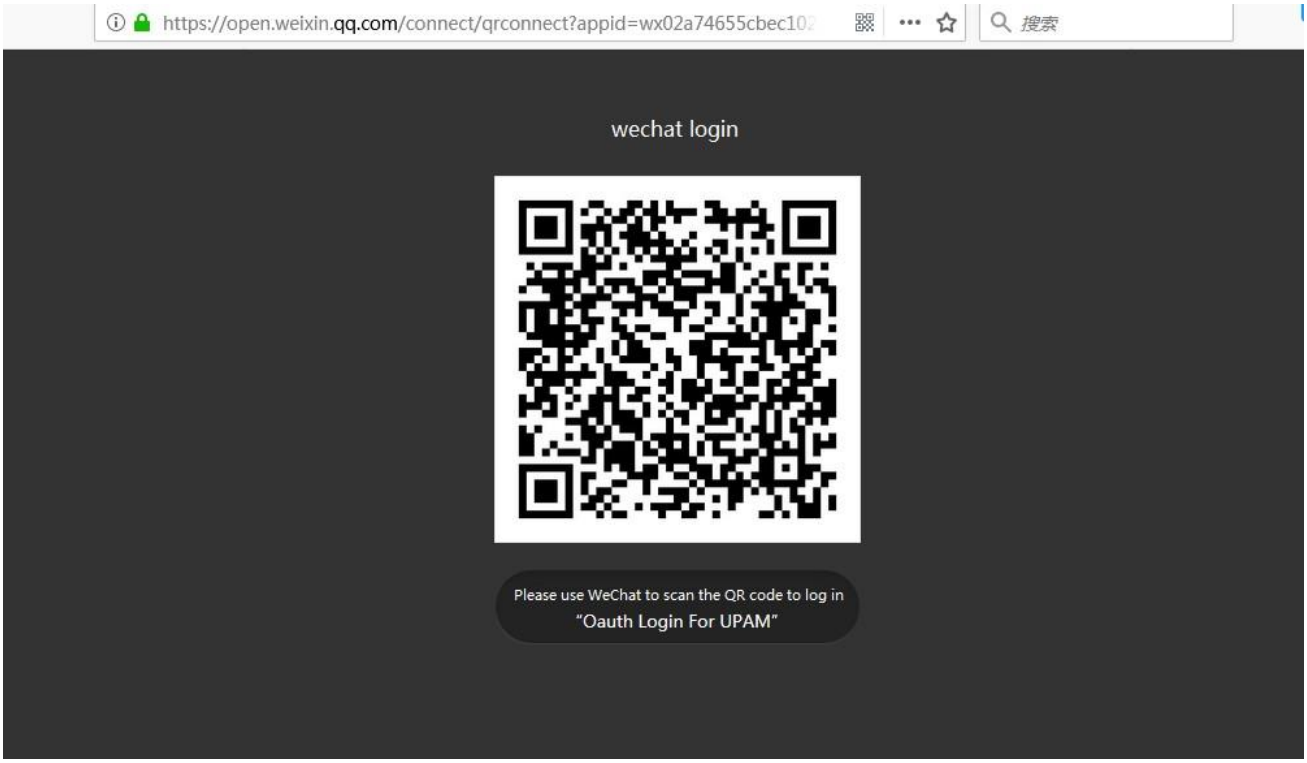
Open the social login module in the guest strategy, select WeChat, and fill in the relevant parameters.

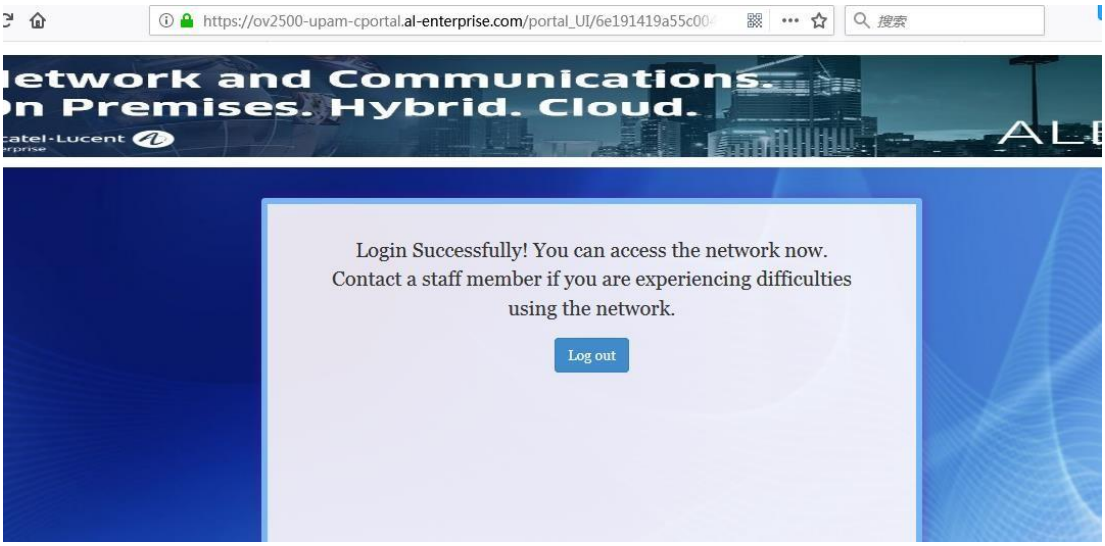


Terminal authentication

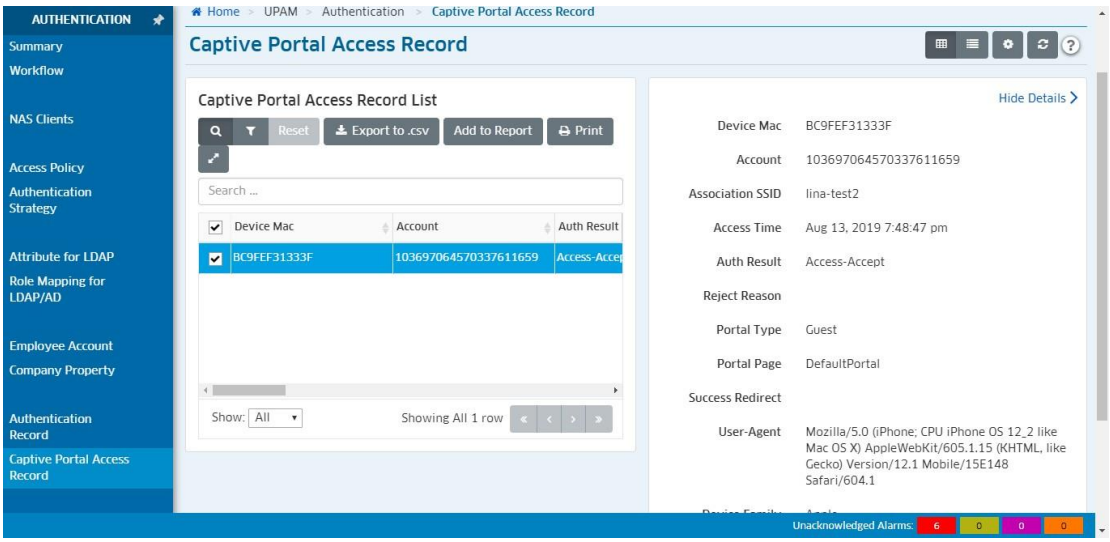
PC

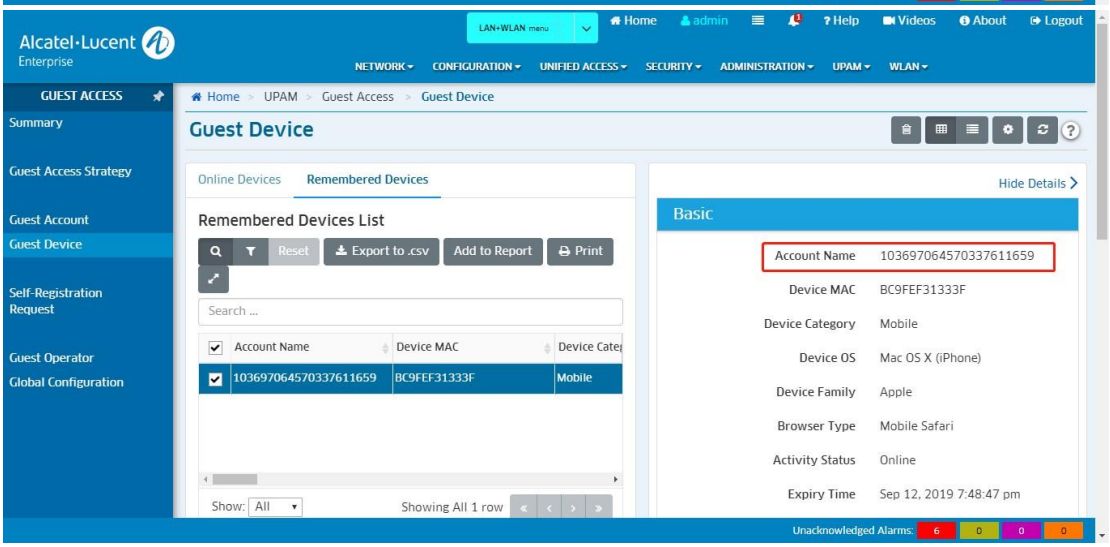

Network and Communications.
On Premises. Hybrid. Cloud.
Alcatel·Lucent
ALE
Where Everything Connects
Login to your account
Username
Password
I accept the Terms of Use
Login
Remember Me
Sign up to create an account
OR
If you don't have an account, you may sign up using
Sign in with WeChat


https://open.weixin.qq.com/connect/qrconnect?appid=wx02a74655cbec10
搜索
wechat login
Please use WeChat to scan the QR code to log in
"Oauth Login For UPAM"



Also visible in the certification record and online





Note

(1) authentication timeout

If the login account information expires for about 1 minute, the terminal prompts on WeChat, the connection fails, please check your network settings, you need to open the portal page again in the browser, jump to WeChat, re-login

If on the PC side, the time of popping up the QR code exceeds the release time (about 2 minutes), and then use the mobile phone to scan and agree. The PC will not respond. You need to re-select the WeChat in the portal page. Authentication, generate QR code again, scan at the terminal

(2) The same WeChat account, login with a different phone or pad is the same guest account1, on another PC will be another account2, different PC are same account2.

5.39 Support static-wep in the cluster

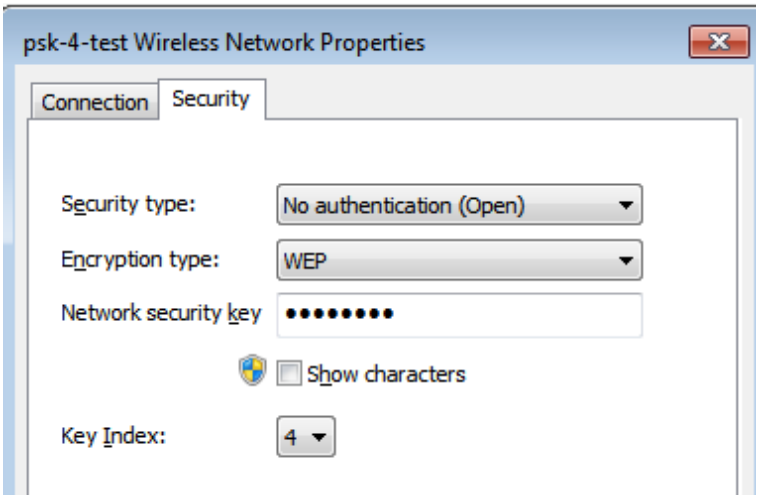
5.39.1 Feature description

This is the new encryption of PSK .When you select the static wep,then the key index of the client-side should be the same as the AP.

5.39.2 Configuration

WLAN configuration page

The client-side:



5.40 UPAM Guest Strategy Enhancement function

5.40.1 Feature description

In some hospitality environments where free WIFI is provided they just want to collect user information as part of the self-registration and allow access by T&C check. They don’t want to provide users with any credentials for access, so we add Custom Attributions function in Guest Access Strategy.

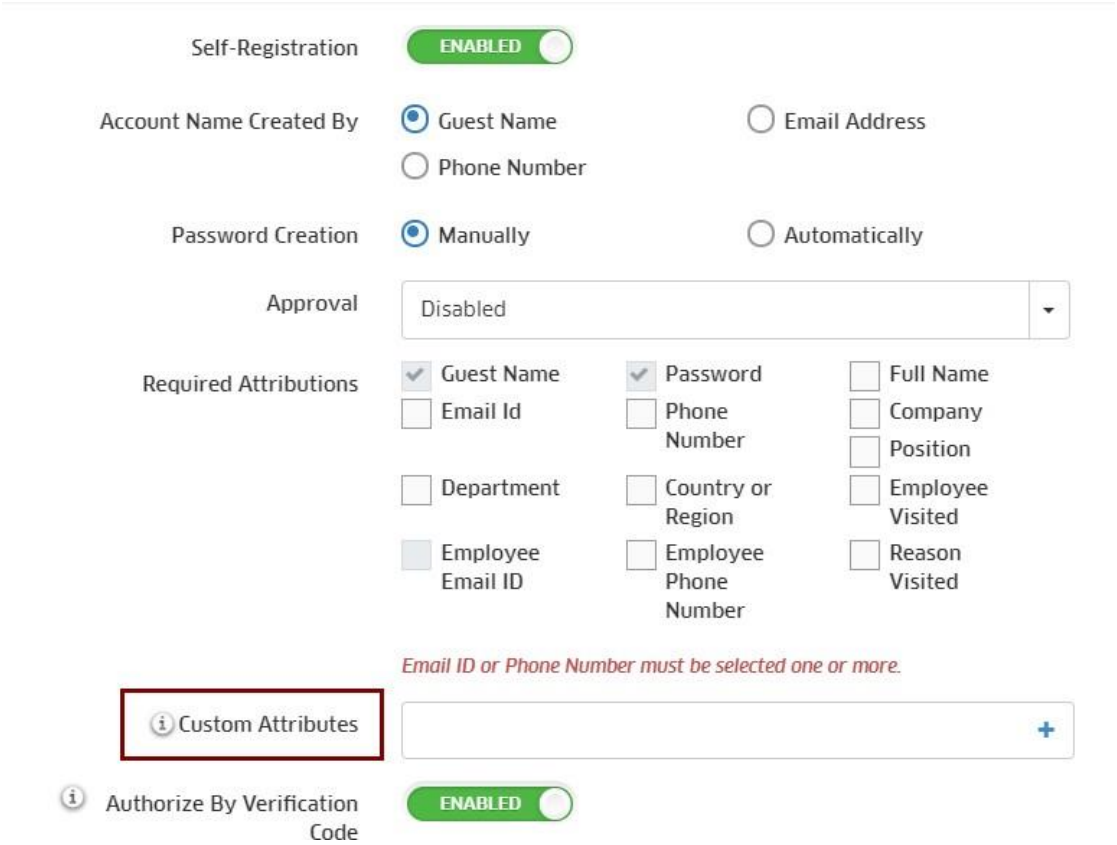
5.40.2 Topology

Same topology as in section 5.14.2.

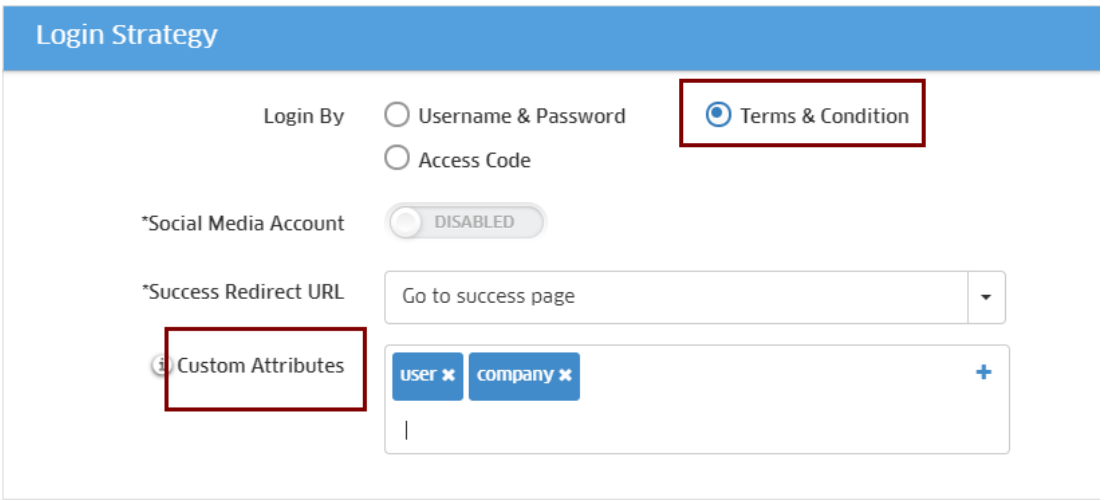
5.40.3 Configuration

The following is how to use this function:

When use select login by Username & Password, user should enable Self-Registration and input what information is wanted as Custom Attributes;



When use select login by Terms & Condition, user can set Custom Attributes in Login Strategy. Shown as the following picture



5.41 VLAN Pooling

5.41.1 Feature description

Add VLAN Pool support based on the original VLAN function, when selecting Mapping Method = Map to VLAN Allows you to specify one or more VLANs, including a specified range (eg, 10-20) or a separate multiple VLAN (eg, 21, 23, 25) or a mixture of the two (eg, 10-20, 21, 23, 25). When a client accesses, the AP selects a VLAN in the VLAN Pool. When multiple users access the network, the number of clients connected to each VLAN in the VLAN Pool is relatively balanced.

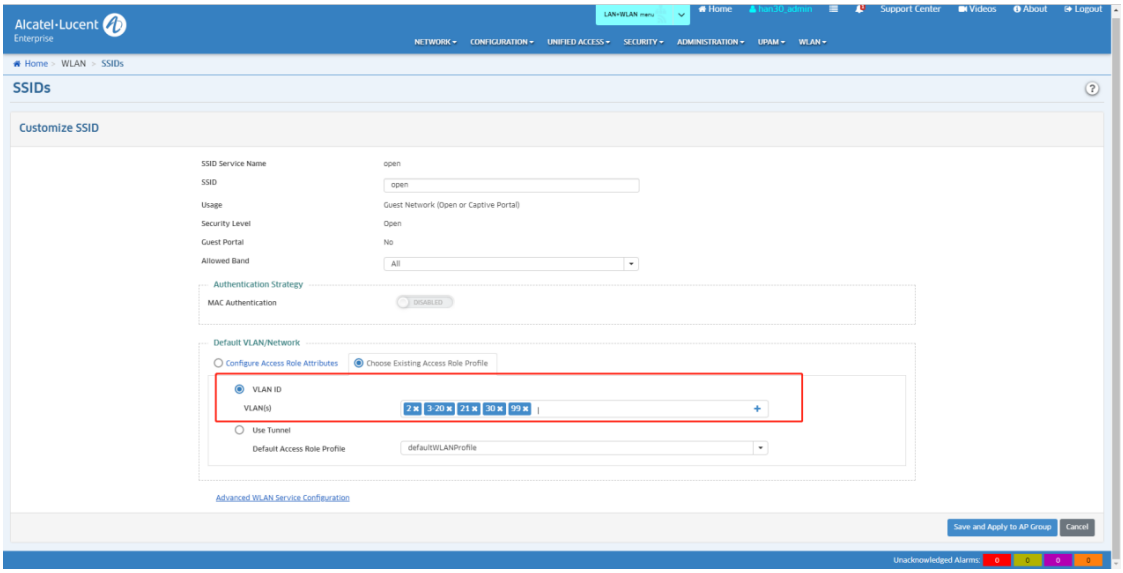
5.41.2 Topology

Same topology as in section 5.14.2

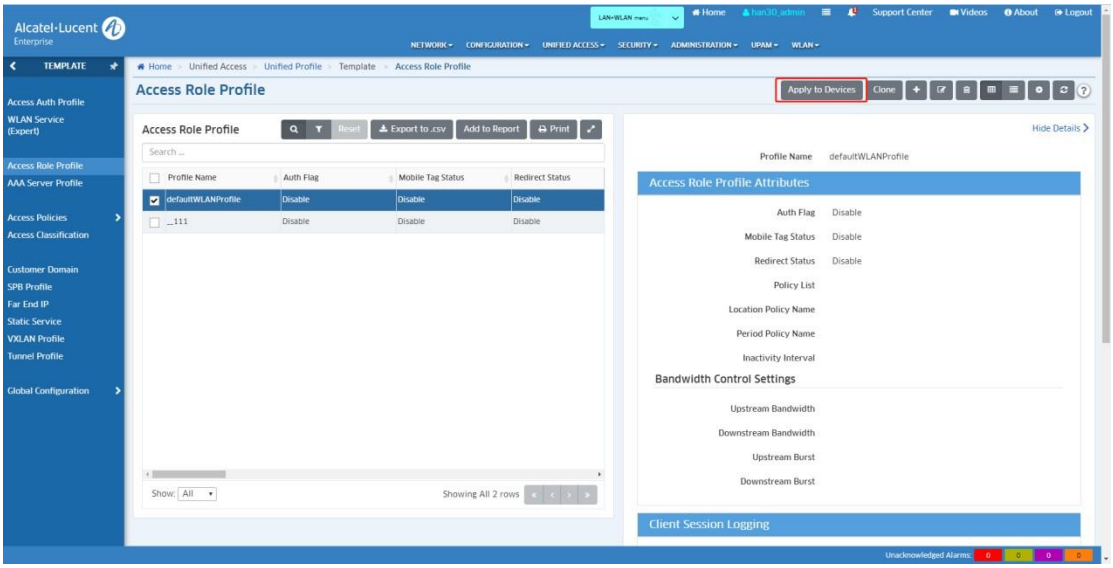
5.41.3 Configuration

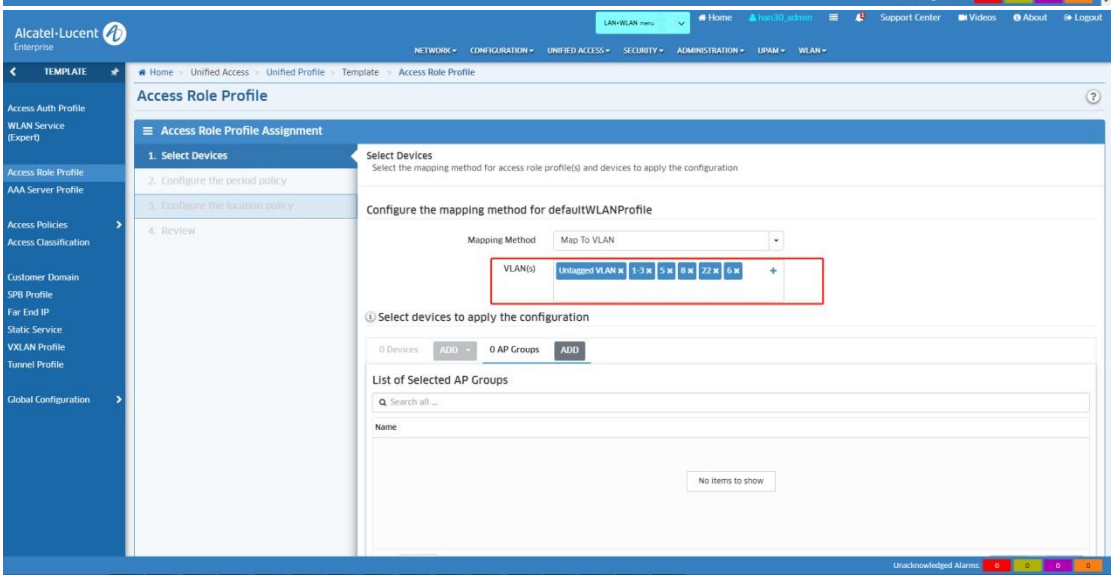
1) Home->WLAN->SSIDs, create/modify SSID:

You can input multiple VLAN IDs.



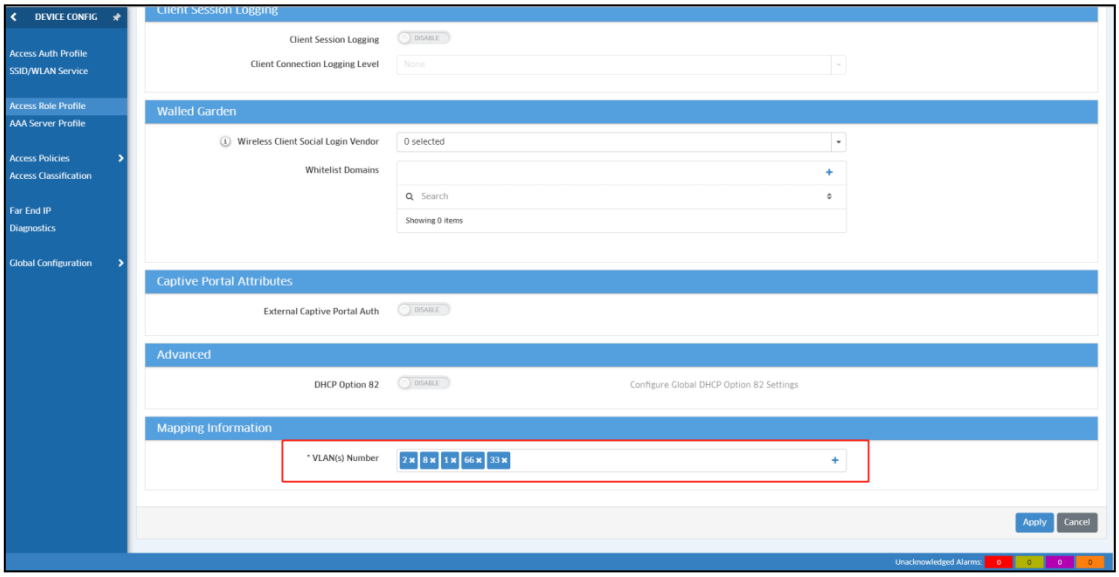
2) Home->Unified Access->Unified Profile->Template->Access Role Profile, choice an Access Role Profile to Apply to Device:





Then you can input multiple VLAN IDs in VLAN(s).

3) Home->Unified Access->Unified Profile-> Device Config-> Access Role Profile->Add Group, choice an Access Role Profile and click Edit:



You can modify VLAN(s) Number with multiple VLAN IDs.

5.41.4 Attention

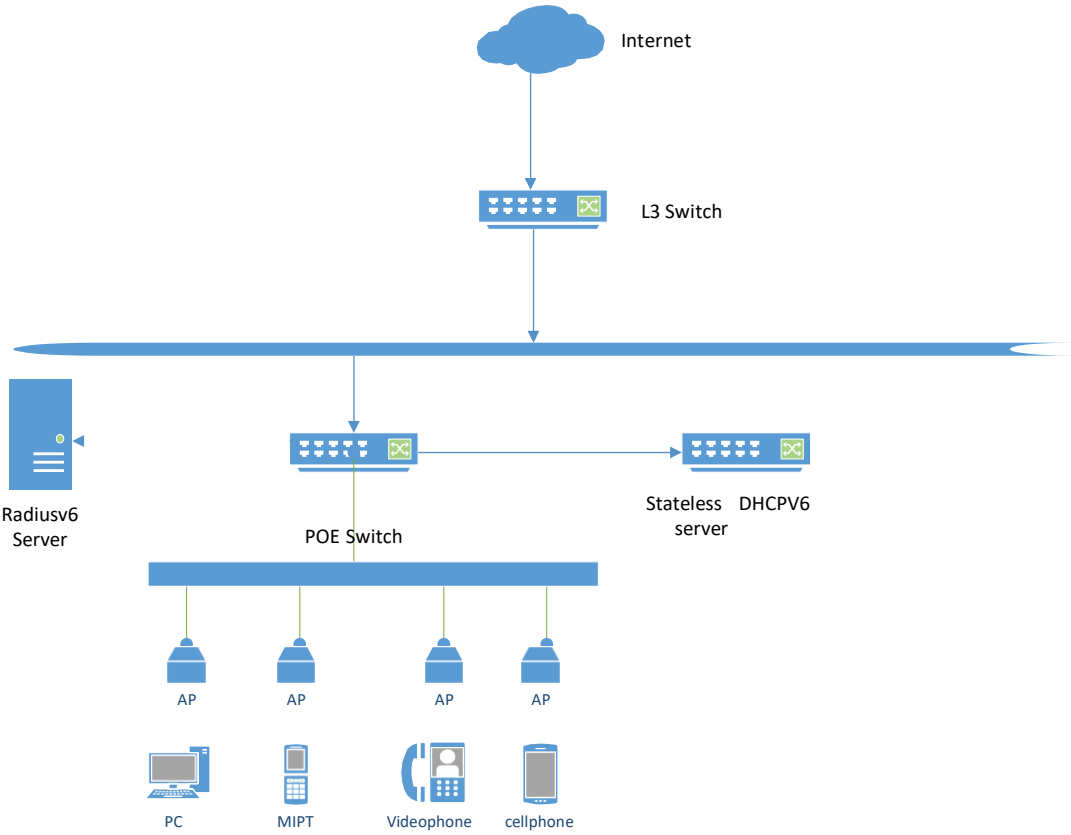
Only 65 VLAN interface can be created on an AP, the multiple Access Role Profiles with multiple VLANs should less than 65 to make sure your every VLAN is useful.

5.42 IPv6 Phase 2(Cluster)

5.42.1 Feature description

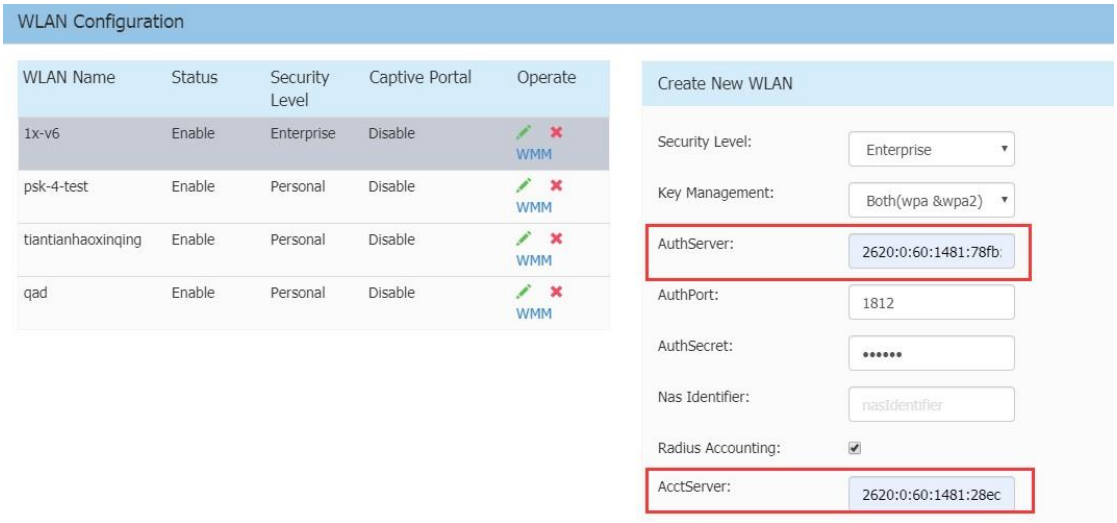
The AP can get IPv6 address through stateless automatic configuration on the cluster mode.On the Stellar UI page,the following functions can work through IPv6: 802.1x authention、group info management、syslog remote server、AP log collection、Ping、Traceroute、TFTP server、Upgrade through IPv6 URL、Trap server、NTP server

5.42.2 Topology

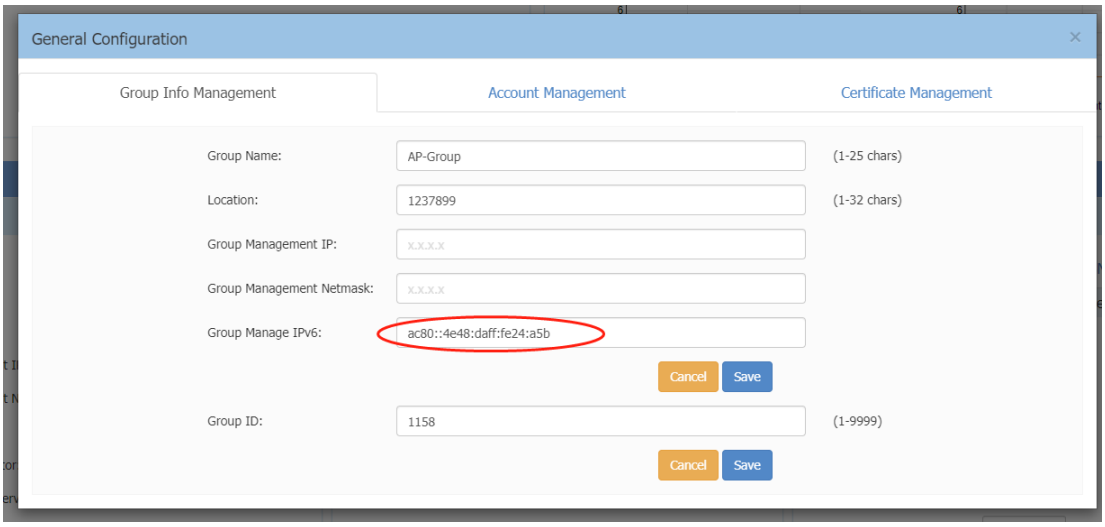


5.42.3 Configuration

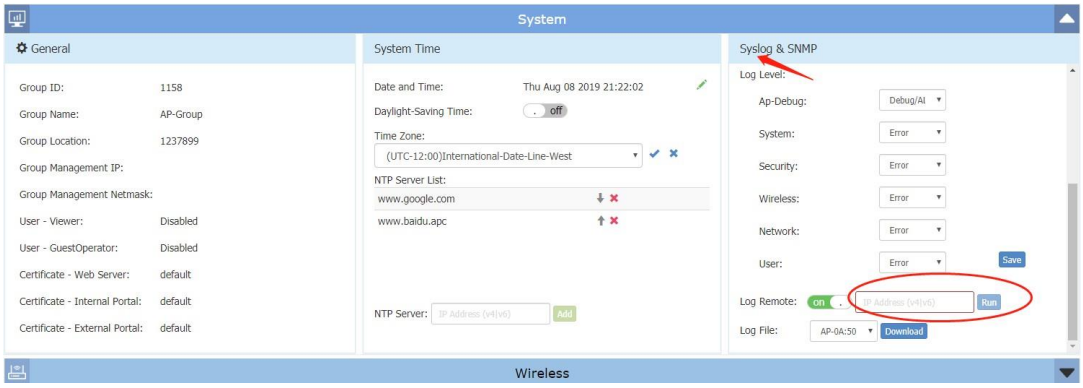
1. The 802.1x authention:



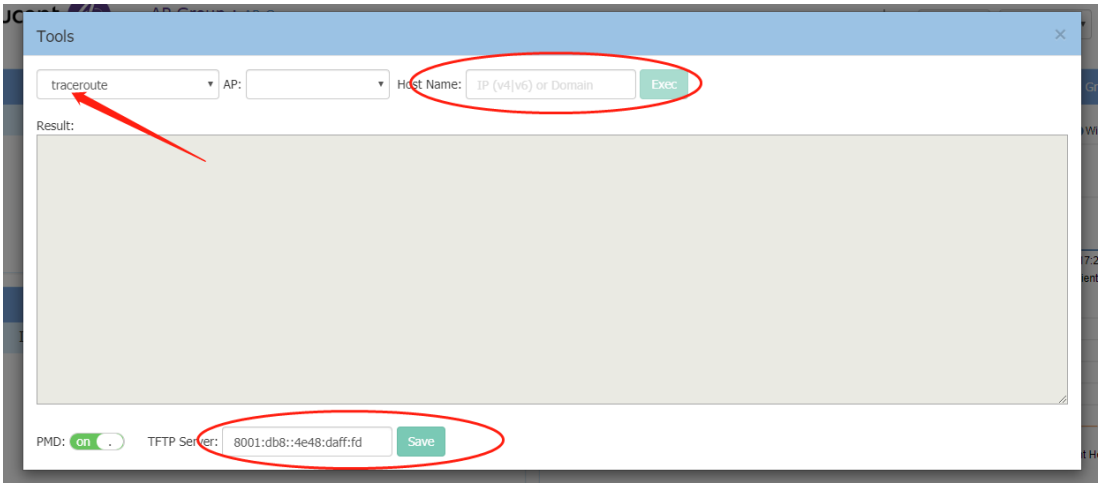
2. Group info mgmtsupport IPV6（v4 |v6）

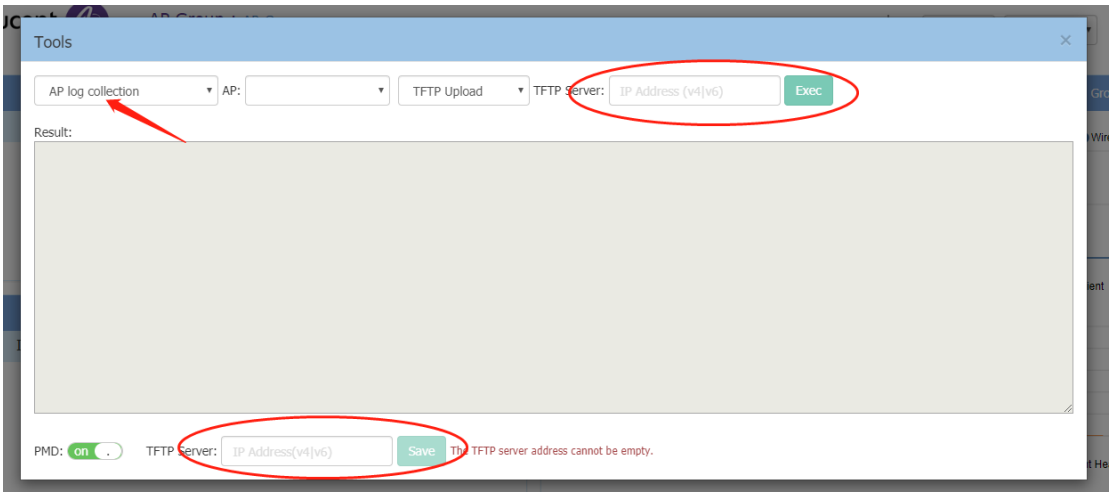


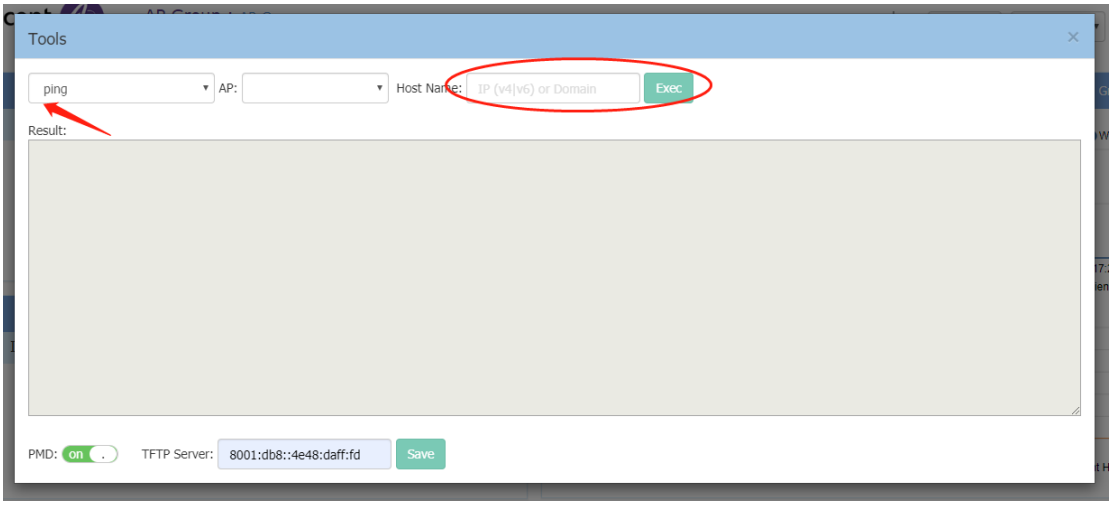
3. Syslog Remote address support IPV6



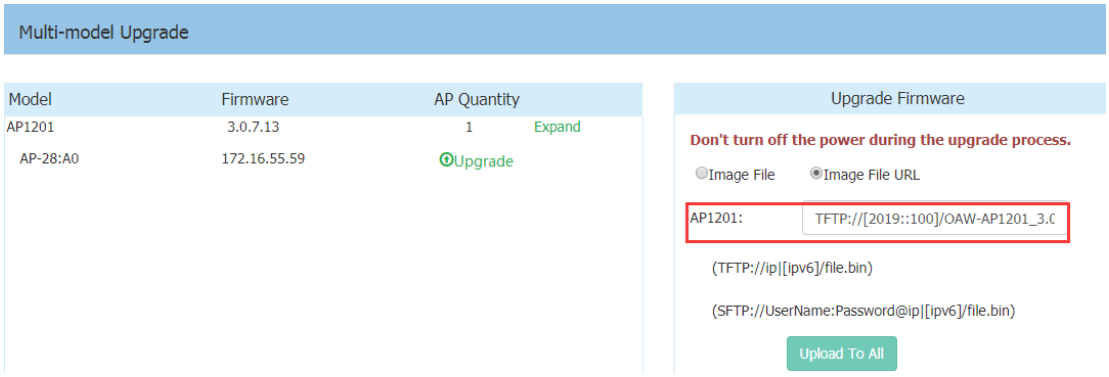
4. AP log collection、traceroute、ping and Tftp Server of PMD：



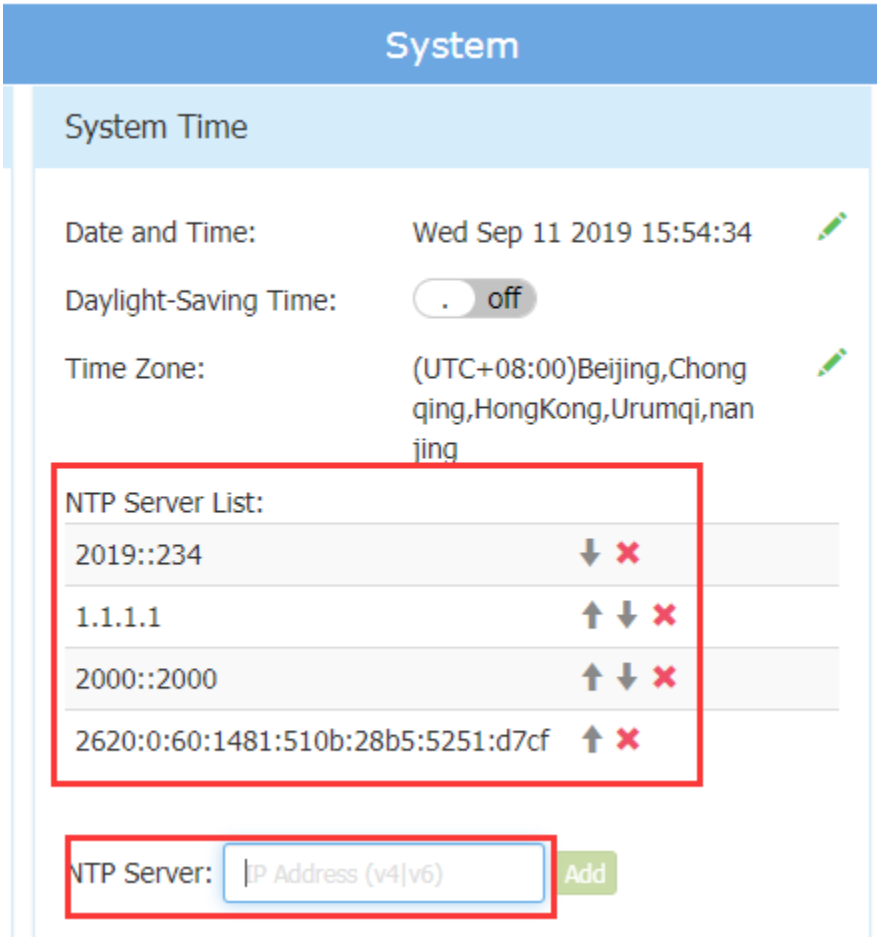




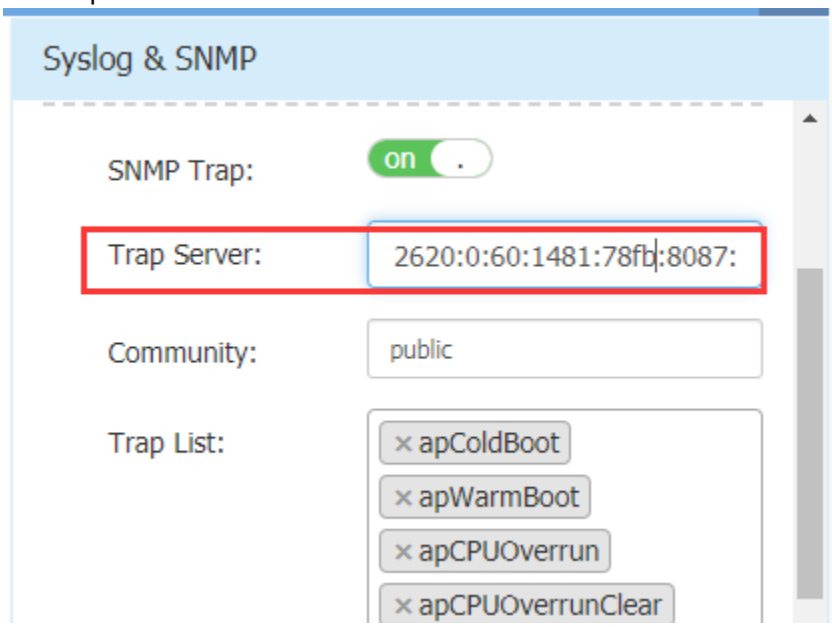
5. Upgrade through URL



6. NTP server



7. Trap server



5.43 WLAN Blacklist Client enhancements (OVE&OVC)

5.43.1 Feature description

Today we allow manual addition of a MAC address into the Client Blacklist; The default expiry period is 24 Hrs from creation and the Reason field is fixed to “Manual add”. Request is to provide optional fields “Expiry Date” and “Reason”. The defaults will remain the same. The “Expiry Date” can be 1 to 365 days out. The “Reason” field is a textual string. Mainly the following:

(1) The blacklisting duration should be configurable to more than 24 hours. This has to be done in both cases when the MAC address is manually added, or when an existing connected client is selected for blacklisting.

(2) They need more scalability beyond the maximum of 128 MAC address limitation present today. (to support 256 MACs).

5.43.2 Topology

Same topology as in section 5.14.2.

5.43.3 Configuration

On both OVC and OVE mode, go to "Home-->WLAN-->Client-->Client Blacklist" page and add client blacklist.

There will be two new fields now: “Expiry Date”, “Reason”. User can custom every client’s “Expiry Date” and “Reason”. If the user didn’t change the “Expiry Date”, the date would same with the aging time of Client Blacklist Policy in WIPS. The “Expiry Date” can be 1 to 365 days out. The “Reason” field is a textual string, and the default value is “Manual add”

5.43.4 Attention

(1) Modify "Aging Time" :

As long as the validity period is modified, the start and end time of the validity period will be counted from the time of the update.

For example, the previous start and end time is calculated from 3:00, and at 4 o'clock, the Aging Time is modified. The start and end time will be calculated from 4 o'clock.

(2) Modify only "Reason" without modifying "Aging Time":

If only the reason is changed, the validity period will not change.

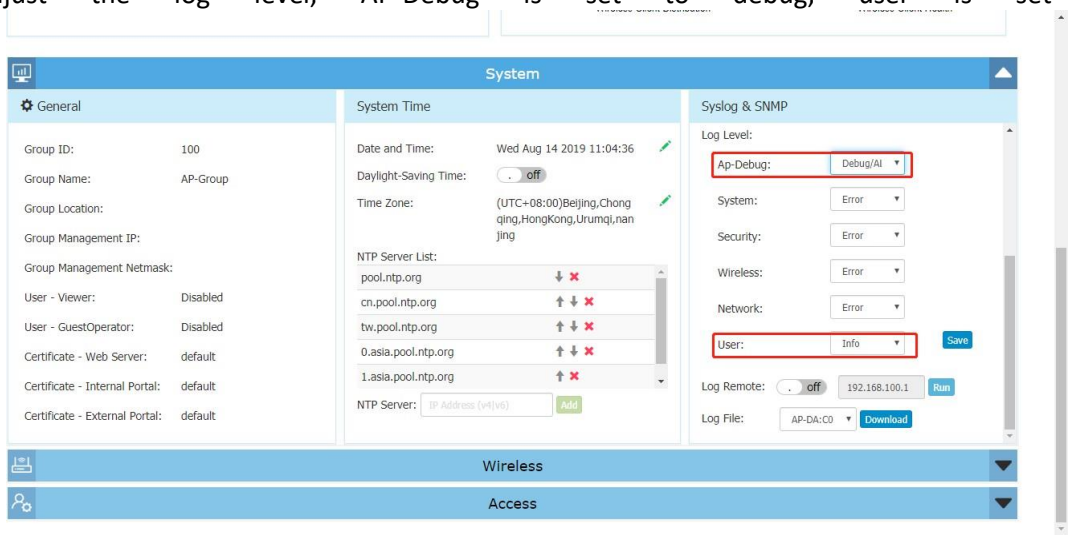
5.44 wmm awareness logging

5.44.1 Feature description

Function output log for voice and video awareness. The log level is info. The Syslog server, the download log, both have output.

5.44.2 Configuration

Adjust the log level, AP-Debug is set to debug, user is set to info, click save



Enable voice and video awareness

Check the log contents in the download log

(1) Background is enabled, voice and video awareness is enabled, voice and video streams are detected, the background will be paused, and no voice and video streams will be restored.

```
2019-07-30 14:33:30 User um[1819] <INFO> [AP 34:E7:0B:03:DA:C0@172.16.25.101] : Detect client: 172.16.25.108 has voice/Video
stream ,Need  pause scanning  so run the command  bg-s -x pause_scanning=1
2019-07-30 14:37:31 User um[1819] <INFO> [AP 34:E7:0B:03:DA:C0@172.16.25.101] : no client  has voice/Video stream, and
backgroundScanning  is  pause status, so  restart backgroundScanning, run the command bg-s -x pause_scanning=0&
```

(2) Background is off, voice and video awareness is off, when detecting or receiving a voice stream, since the background is off, no action is taken

```
stream ,Need  pause scanning, run the cmd bg-s -x pause_scanning=1
2019-07-30 14:49:03 User um[1819] <INFO> [AP 34:E7:0B:03:DA:C0@172.16.25.101] : Detect client: 172.16.25.108 has voice/Video
stream , but the backgroundScanning is off, so do noting
2019-07-30 14:49:07 User um[1819] <INFO> [AP 34:E7:0B:03:DA:C0@172.16.25.101] : Recv the user 172.16.25.108 has voice/Video
stream ,but the Background Scanning  is off,so do noting
```

(3) Voice and video awareness is off, no operation

```
2019-07-30 14:50:34 User um[1819] <INFO> [AP 34:E7:0B:03:DA:C0@172.16.25.101] : Beause the  Voice and Video Awareness switch
is close,and backgroundScanning  config is enable, now the backgroundScanning  is  pause  status ,Now need  restart the
backgroundScanning
2019-07-30 14:53:10 User um[1819] <INFO> [AP 34:E7:0B:03:DA:C0@172.16.25.101] : Recv the user 172.16.25.108 has  voice/Video
stream  but Voice and Video Awareness switch  is off ,so do nothing
```

5.44.3 Attention

The log save time is the same as the keep time of the keys syslog. It may be overwritten by other content for ten or twenty minutes.

5.45 802.11w support for wpa2

5.45.1 Feature description

The 802.11w protocol is mainly based on the existing encryption form of data packets and similarly encrypts management frames. Management frames that 802.11w needs to encrypt include disassociation frames, deauthentication frames, and strong Action frames.

The management frame encryption function is optional and requires mutual negotiation between the two parties. Negotiation is identified by the 6 and 7 bits of RSN Capabilities. The 6th bit is Management Frame Protection Required (MFPR), and the 7th bit is Management Frame Protection Capable (MFPC). MFPR represents whether it is mandatory to support management frame encryption, and MFPC represents whether it supports management frame encryption. When negotiating, if one party requires mandatory support for 802.11w (MFPR is set to 1) and the other party does not support 802.11w (MFPR is set to 0), the negotiation cannot be successful; everything else is OK.

You can configure the 802.11w switch status in the AP wlan configuration parameters: Disabled / Optional / Required.

When the 802.11w switch status is: Disabled (MFPR = 0, MFPC = 0), it means that management frame encryption is not supported;

When the 802.11w switch status is: Optional, MFPR = 0 and MFPC = 1, it indicates that management frame encryption is supported

When the 802.11w switch status is: Required, MFPR = 1 and MFPC = 1, which means that management frame encryption is mandatory;

5.45.2 Topology

Same topology as in section 5.14.2.

5.45.3 Attention

Negotiation principles between AP and client:

AP MFPC	AP MFPR	STA MFPC	STA MFPR	AP Action	STA Action	Whether management frames are encrypted
0	0	0	0	Associated with terminal	Associated with AP	No
0	0	1	0	Associated with terminal	Associated with AP	No
0	0	1	1	None	Refused to associate with AP	-
1	0	0	0	Associated with terminal	Associated with AP	No
1	0	1	0	Associated with terminal	Associated with AP	Yes

WLAN configuration PMF parameter support:

	Security Level	Key Management/ Encryption Type	Default Value	Range	Status
Cluster	Personal	Both(wpa&wpa2)	Disabled	Disabled Optional Required	Can be modified
		wpa2-personal	Disabled	Disabled Optional Required	Can be modified
		Both(wpa2&wpa3)	Optional	Optional/Required	Only display cannot be
		wpa3-personal	Required	Required	Only display cannot be
		Static-wep	-	-	Do not show
	Enterprise	Both(wpa&wpa2)	Disabled	Disabled Optional Required	Can be modified
		wpa2-enterprise	Disabled	Disabled Optional Required	Can be modified
		wpa3-enterprise(CNSA disable)	Optional	Optional/Required	Only display cannot be
		wpa3-enterprise(CNSA enable)	Required	Required	Only display cannot be
OV	Personal	WPA2_PSK_AES	Disabled	Disabled Optional Required	Can be modified
		WPA3_PSK_SAE_AES	Optional	Optional/Required	Only display cannot be
		WPA3_SAE_AES	Required	Required	Only display cannot be
	Enterprise	WPA2_AES	Disabled	Disabled Optional Required	Can be modified
		WPA3_AES	Optional	Optional/Required	Only display cannot be
		WPA3_AES256	Required	Required	Only display cannot be

5.46 Authenticated Switch Access using UPAM

5.46.1 Feature description

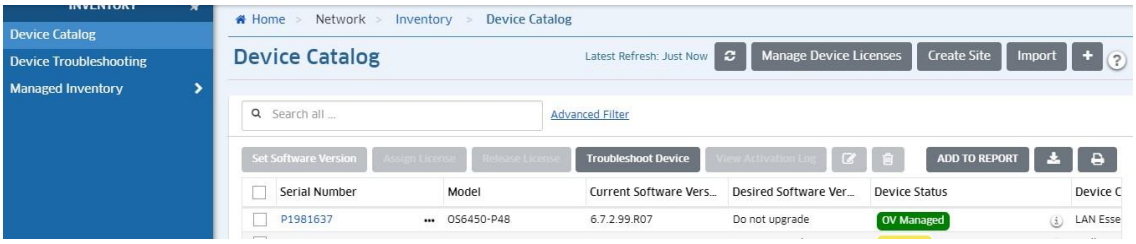
Customers can use UPAM for Unified Access but are forced to rely on 3rd party Radius server for switch access authentication. Many of our mid to large customers centrally secure network access through ASA.Request is for adding support for VSA 26 subtype 9 (Alcatel-Asa-Access) and subtypes 39-42, as well as GUI front end to configure switch access levels. Within OV/UPAM allow configuration and monitoring of all switch access.

5.46.2 Topology

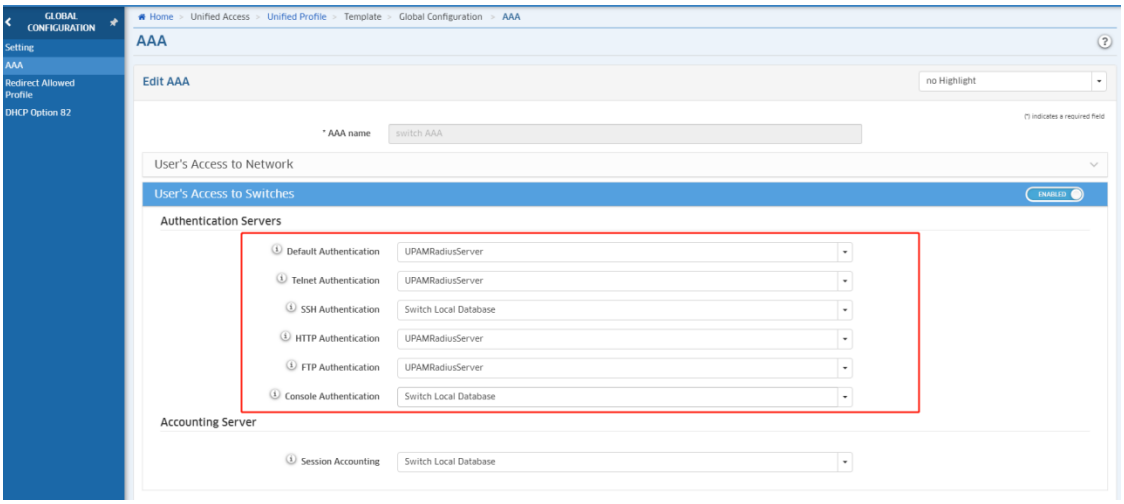
Same topology as in section 5.14.2.

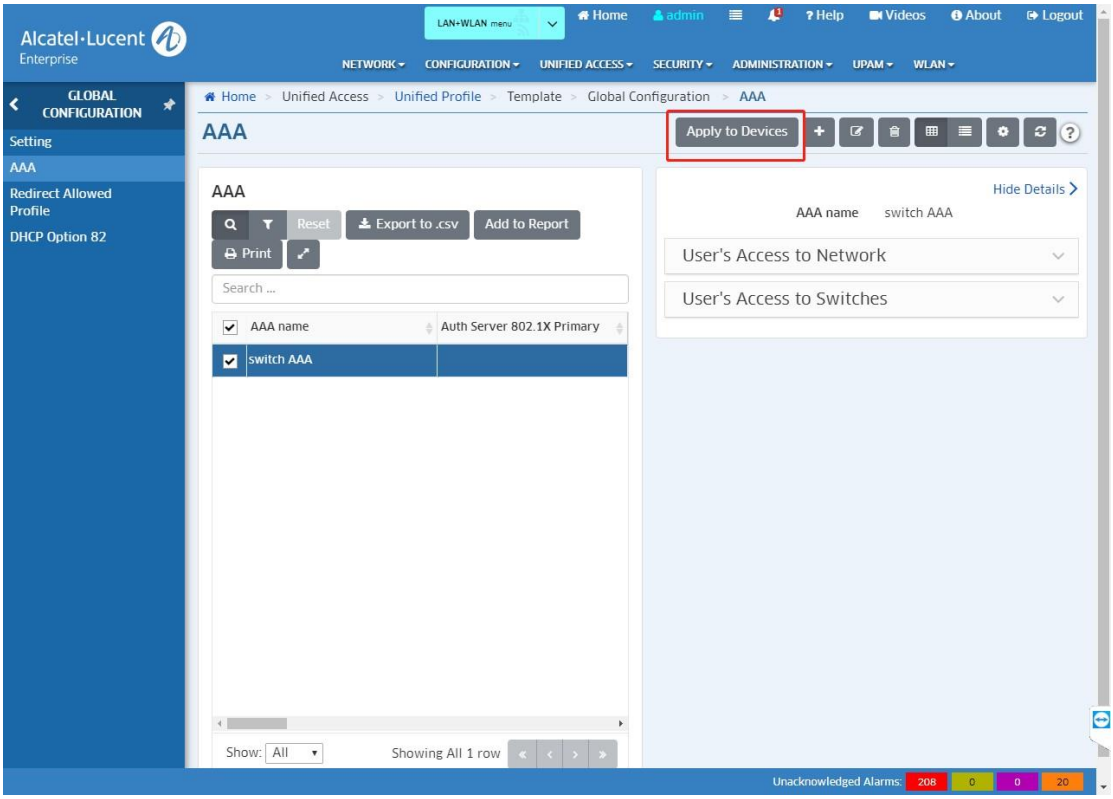
5.46.3 Configuration

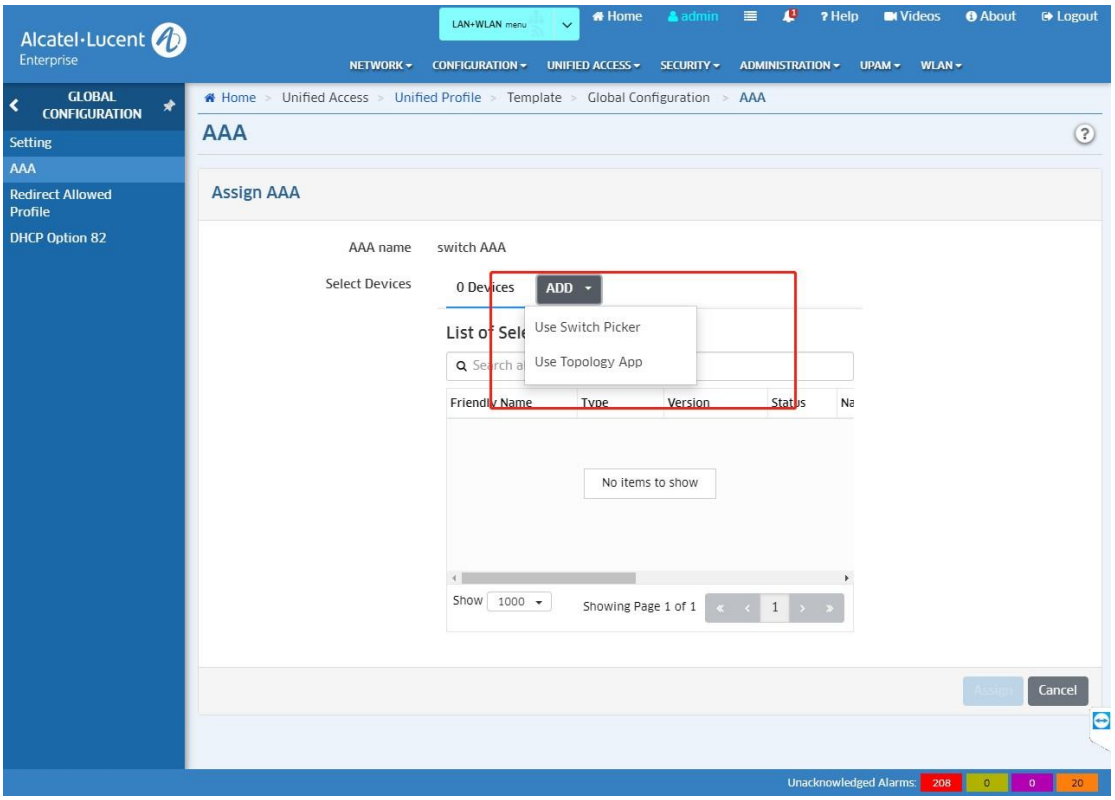
Make sure your switch managed by OVE or OVC

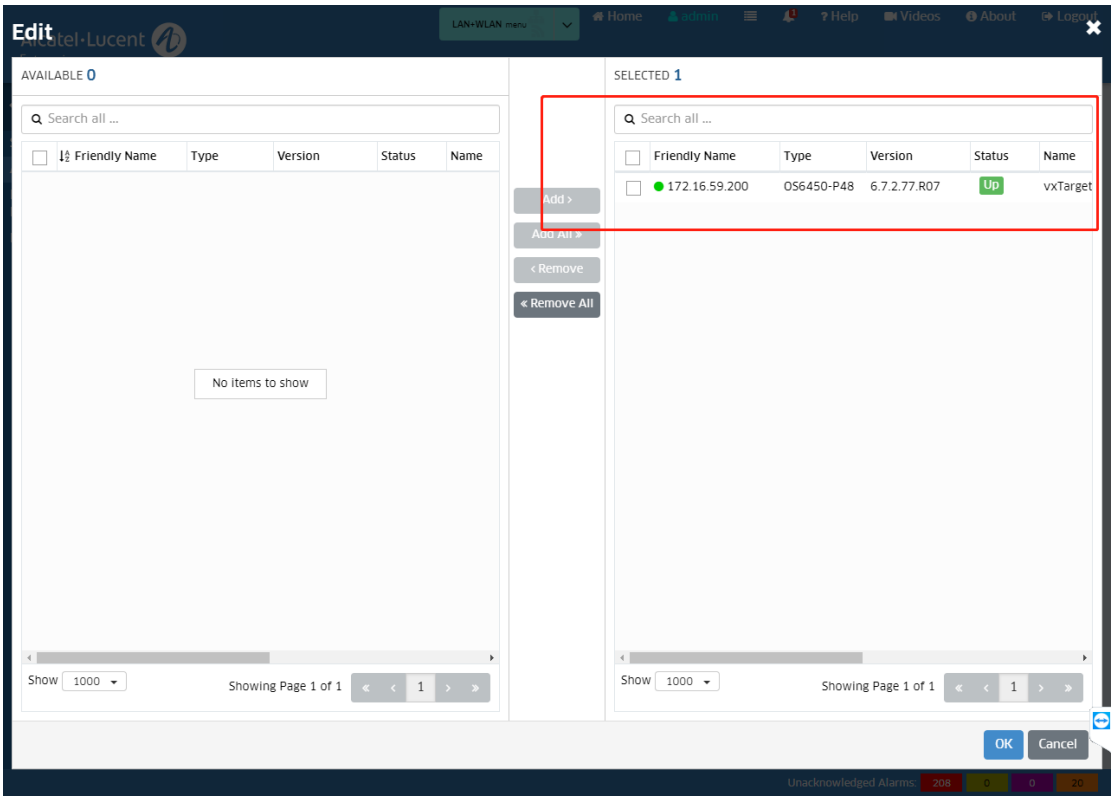


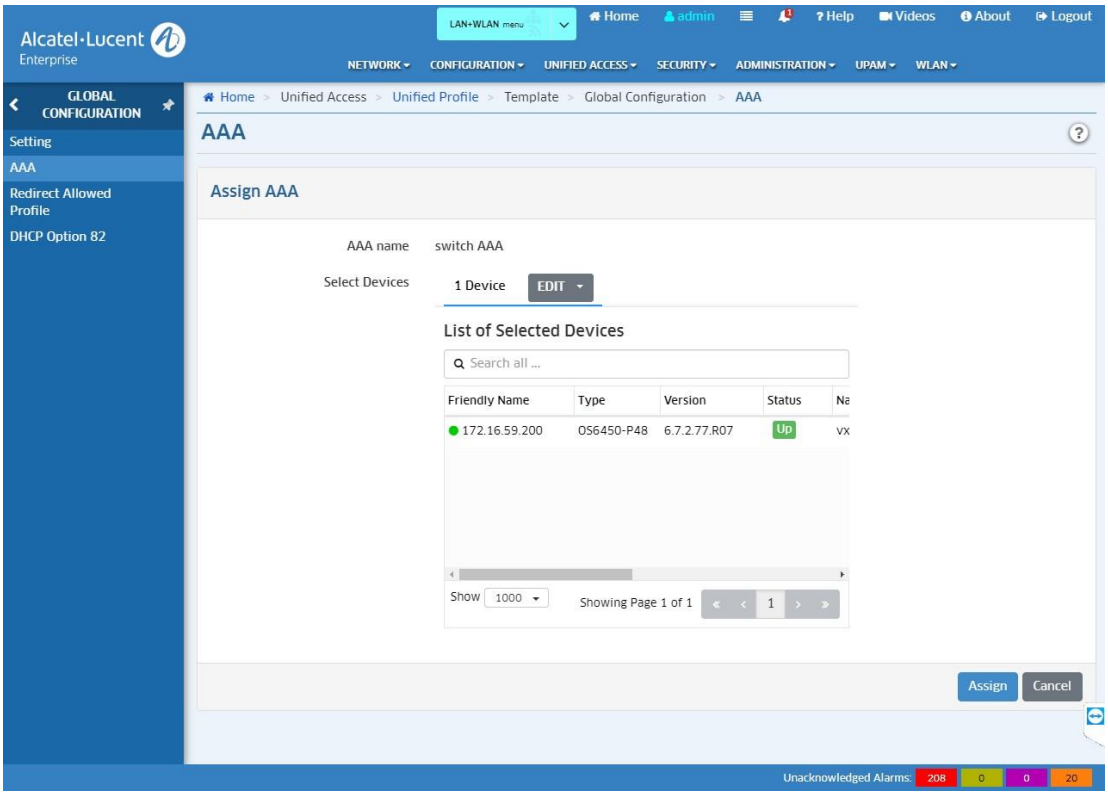
Add AAA for switch, and select UPAMRadiusServer as Authentication Servers. Then apply your AAA on your switch:



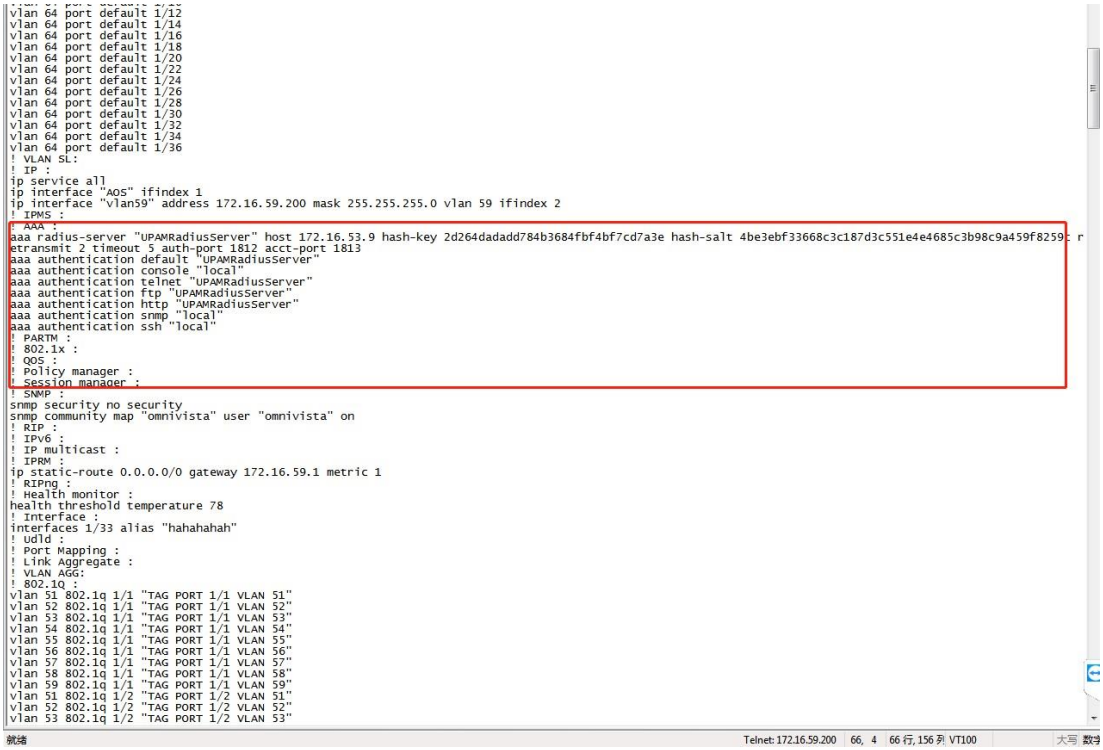



Alcatel·Lucent Enterprise
LAN+WLAN menu
Home
admin
Help
Videos
About
Logout
NETWORK
CONFIGURATION
UNIFIED ACCESS
SECURITY
ADMINISTRATION
UPAM
WLAN
GLOBAL CONFIGURATION
Setting
AAA
Redirect Allowed Profile
DHCP Option 82
Home > Unified Access > Unified Profile > Template > Global Configuration > AAA
AAA
Assign AAA
AAA name
switch AAA
Select Devices
0 Devices
ADD
Use Switch Picker
Use Topology App
Friendly Name
Type
Version
Status
No items to show
Show 1000
Showing Page 1 of 1
Assign
Cancel
Unacknowledged Alarms: 208 0 0 20


Edit
AVAILABLE 0
Search all ...
Friendly Name
Type
Version
Status
Name
No items to show
Show 1000
Showing Page 1 of 1
Add >
Add All >
< Remove
« Remove All
SELECTED 1
172.16.59.200
OS6450-P48
6.7.2.77.R07
Up
vxTarget
OK
Cancel

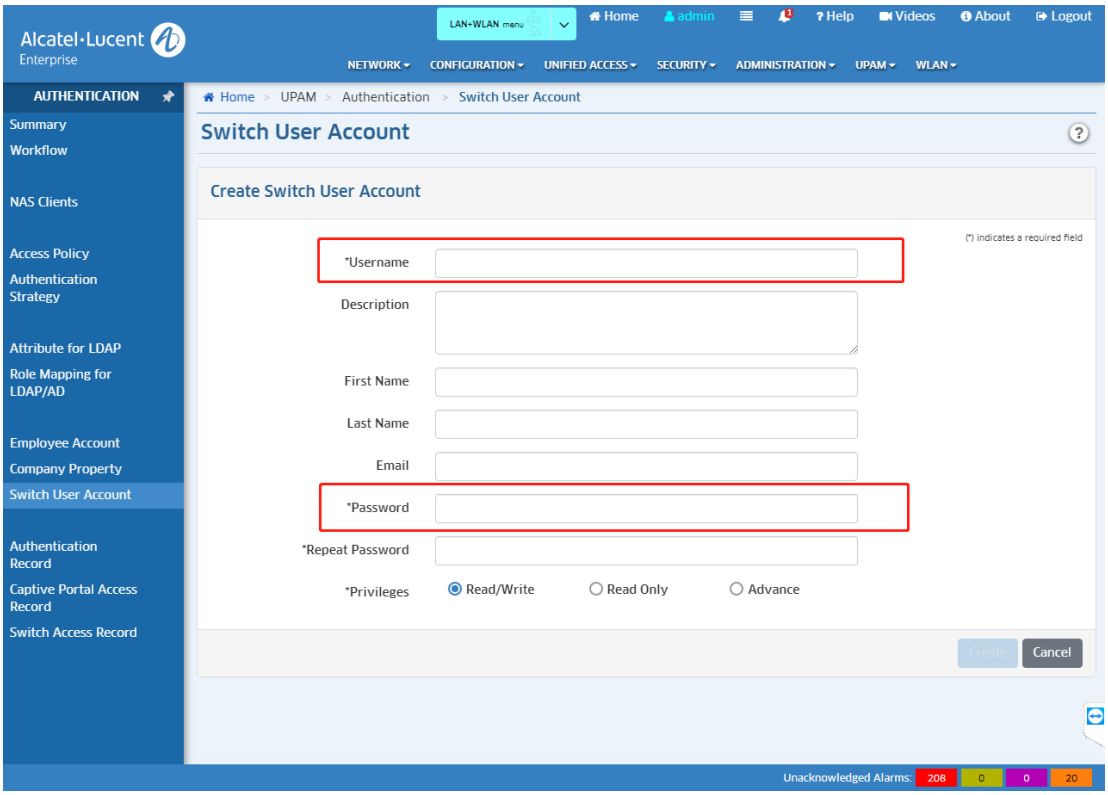


Then you can get configuration on your switch:

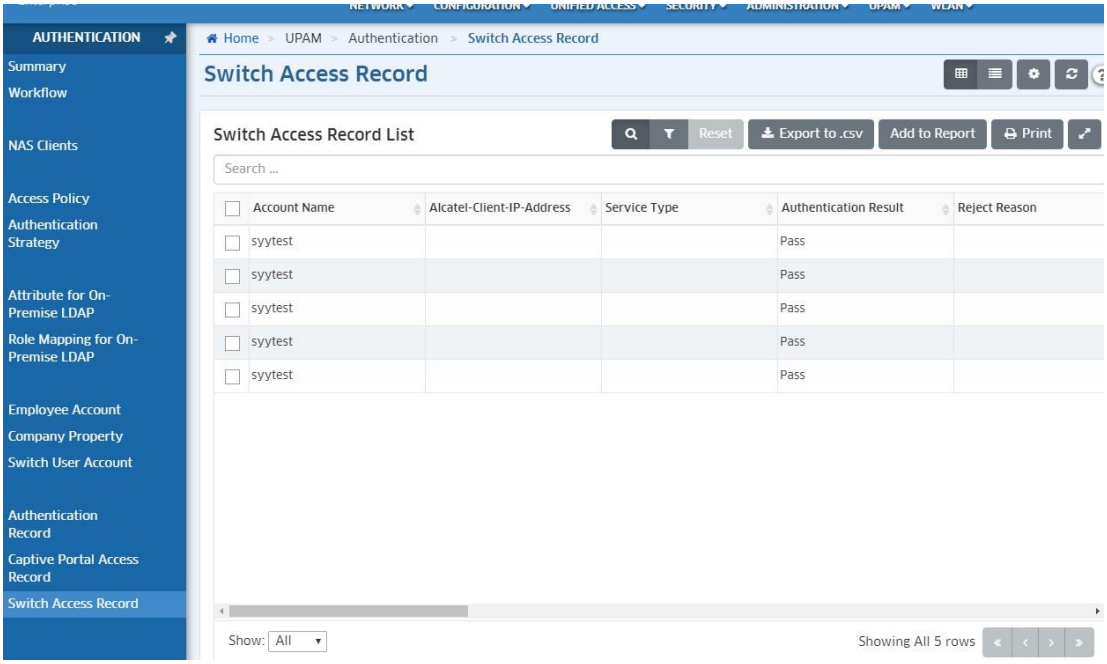


```
vlan 64 port default 1/12
vlan 64 port default 1/14
vlan 64 port default 1/16
vlan 64 port default 1/18
vlan 64 port default 1/20
vlan 64 port default 1/22
vlan 64 port default 1/24
vlan 64 port default 1/26
vlan 64 port default 1/28
vlan 64 port default 1/30
vlan 64 port default 1/32
vlan 64 port default 1/34
vlan 64 port default 1/36
! VLAN SL:
! IP :
ip service all
ip interface "AOS" ifindex 1
ip interface "vlan59" address 172.16.59.200 mask 255.255.255.0 vlan 59 ifindex 2
! IPMS :
! AAA :
aaa radius-server "UPAMRadiusServer" host 172.16.53.9 hash-key 2d264dadadd784b3684fbf4bf7cd7a3e hash-salt 4be3ebf33668c3c187d3c551e4e4685c3b98c9a459f8259: r
etransmit 2 timeout 5 auth-port 1812 acct-port 1813
aaa authentication default "UPAMRadiusServer"
aaa authentication console "local"
aaa authentication telnet "UPAMRadiusServer"
aaa authentication ftp "UPAMRadiusServer"
aaa authentication http "UPAMRadiusServer"
aaa authentication snmp "local"
aaa authentication ssh "local"
! PARTM :
! 802.1x :
! QOS :
! Policy manager :
! Session manager :
! SNMP :
snmp security no security
snmp community map "omnivista" user "omnivista" on
! RIP :
! IPv6 :
! IP multicast :
! IPRM :
ip static-route 0.0.0.0/0 gateway 172.16.59.1 metric 1
! RIPng :
! Health monitor :
health threshold temperature 78
! Interface :
interfaces 1/33 alias "hahahahah"
! Udld :
! Port Mapping :
! Link Aggregate :
! VLAN AGG:
! 802.1Q :
vlan 51 802.1q 1/1 "TAG PORT 1/1 VLAN 51"
vlan 52 802.1q 1/1 "TAG PORT 1/1 VLAN 52"
vlan 53 802.1q 1/1 "TAG PORT 1/1 VLAN 53"
vlan 54 802.1q 1/1 "TAG PORT 1/1 VLAN 54"
vlan 55 802.1q 1/1 "TAG PORT 1/1 VLAN 55"
vlan 56 802.1q 1/1 "TAG PORT 1/1 VLAN 56"
vlan 57 802.1q 1/1 "TAG PORT 1/1 VLAN 57"
vlan 58 802.1q 1/1 "TAG PORT 1/1 VLAN 58"
vlan 59 802.1q 1/1 "TAG PORT 1/1 VLAN 59"
vlan 51 802.1q 1/2 "TAG PORT 1/2 VLAN 51"
vlan 52 802.1q 1/2 "TAG PORT 1/2 VLAN 52"
vlan 53 802.1q 1/2 "TAG PORT 1/2 VLAN 53"
就绪
Telnet: 172.16.59.200 66, 4 66 行, 156 列 VT100
大写 数字
```

3. Add switch user account on UPAM, Home->UPAM->Authentication ->Switch User Account, add switch account , you can set account Privileges with Read/Write or Read Only or Advance:



4.Then you can get your record on Switch Access Record list:



5.46.4 Attention

1. If your switch is not be managed on OVE and you want to use UPAM switch account, you must configure UPAM radius server on your switch with CLI.
2. If we ignore the ASA => OV won't touch the current configuration of the device
3. If we enable ASA:

- We can specify server name for each interface
- We can keep the current configuration of an interface (**Keep Existing Config** option)
- We can deny the authentication of an interface (**Deny Access** option)
- We can remove accounting session (**None** option)

4. The authentication server is still UPAM on switch after I ignore the AAA

To remove the UPAM authentication of an interface, you can:

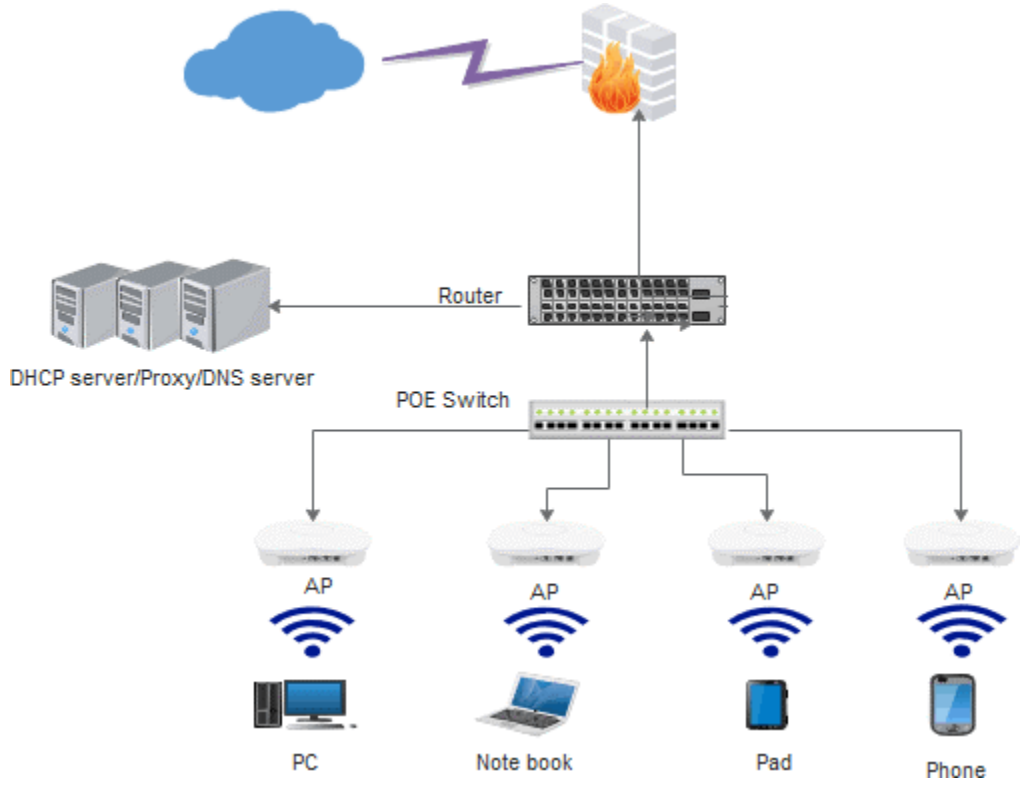
- use local database (select **Switch Local Database** option)
- deny access (select **Deny Access** option)

5.47 Device Specific PSK

5.47.1 Feature description

The Device Specific PSK is the security upgrade for the commom psk.Every device has its own unique Device Specific PSK that is valid for that device only. Each Device Specific PSK is bound to the MAC address of an authorized device - even if that PSK is shared with another user, it will not work for any other machine.

5.47.2 Topology



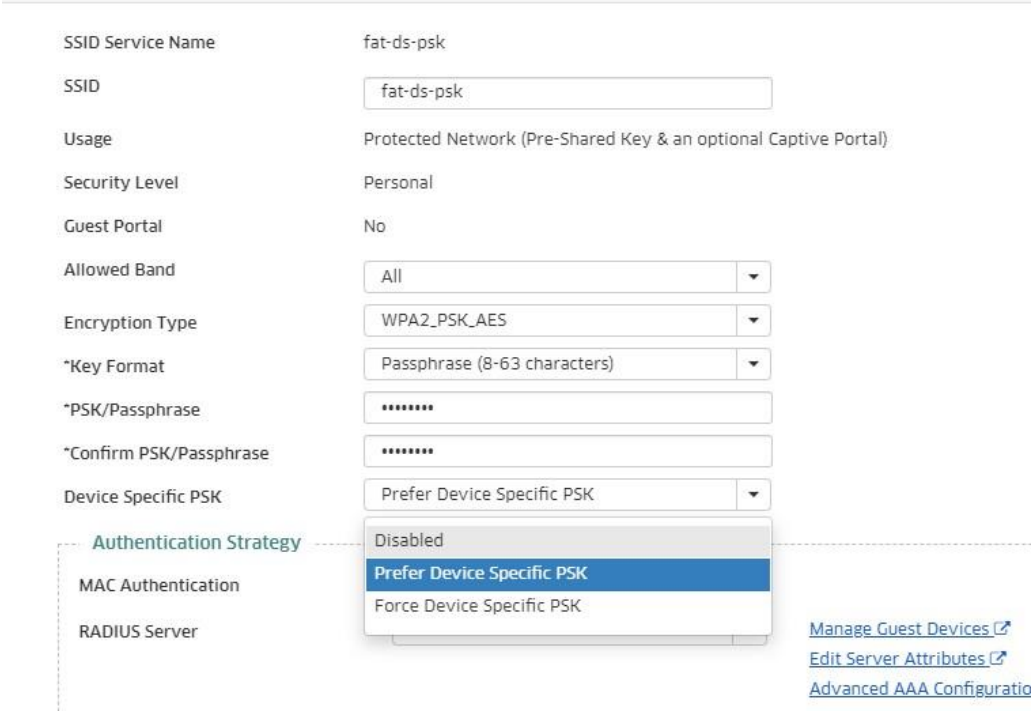
5.47.3 Configuration

1. Link: Home->WLAN->SSIDs ,Create the psk wlan and select the ds-psk mode

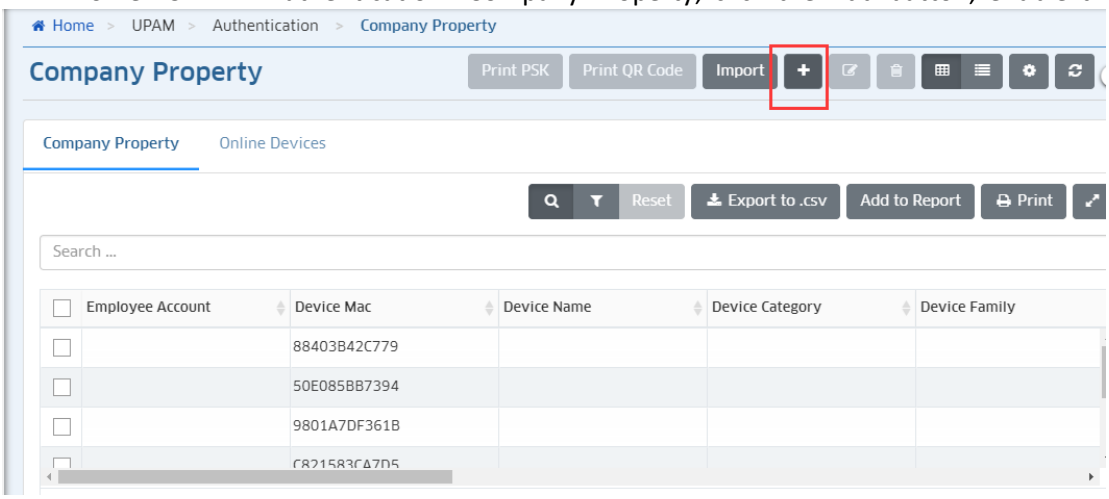
Disabled – Use SSID PSK only

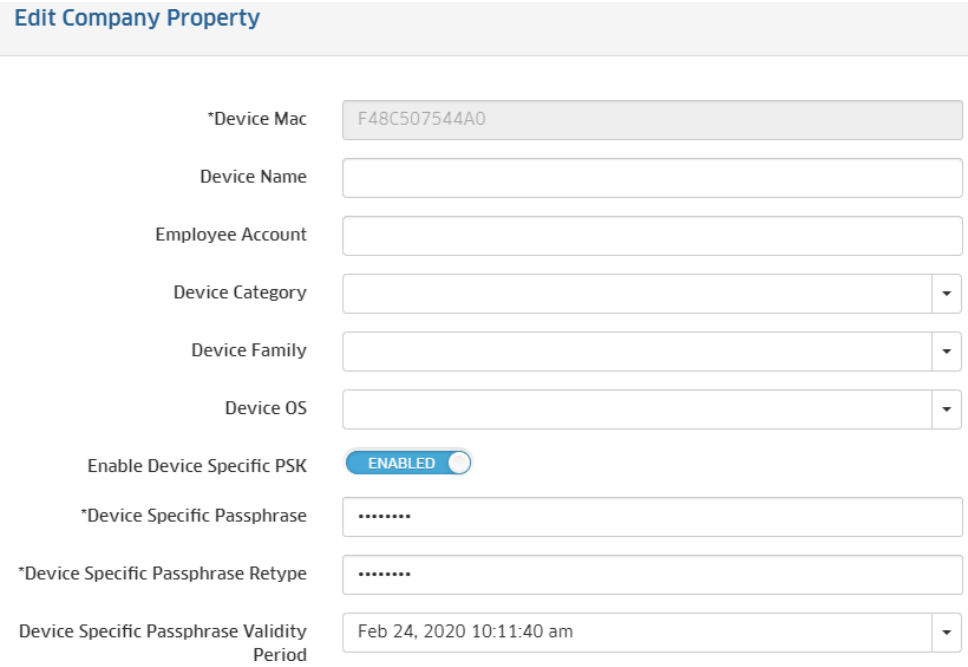
Prefer Device Specific PSK – Fallback to SSID PSK if Device Specific PSK is not sent by Radius via MAC Auth. Device will be failed to associate if any PSK check failed.

Force Device Specific PSK – Device will be failed to associate if Device Specific PSK is not sent by Radius via MAC Auth.

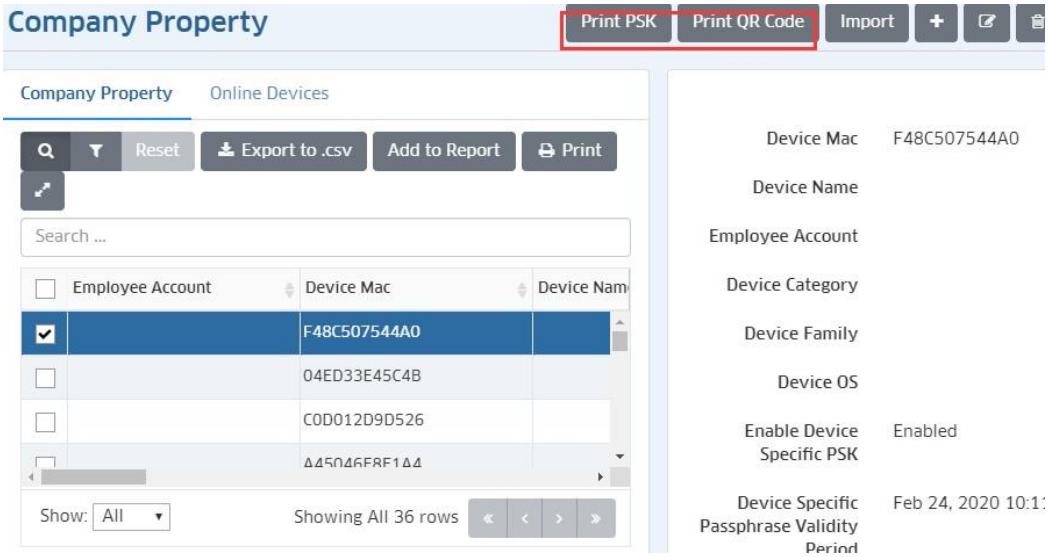


2. Link: Home->UPAM->Authentication->Company Property, click the Add button, enable the DSPSK of the client.

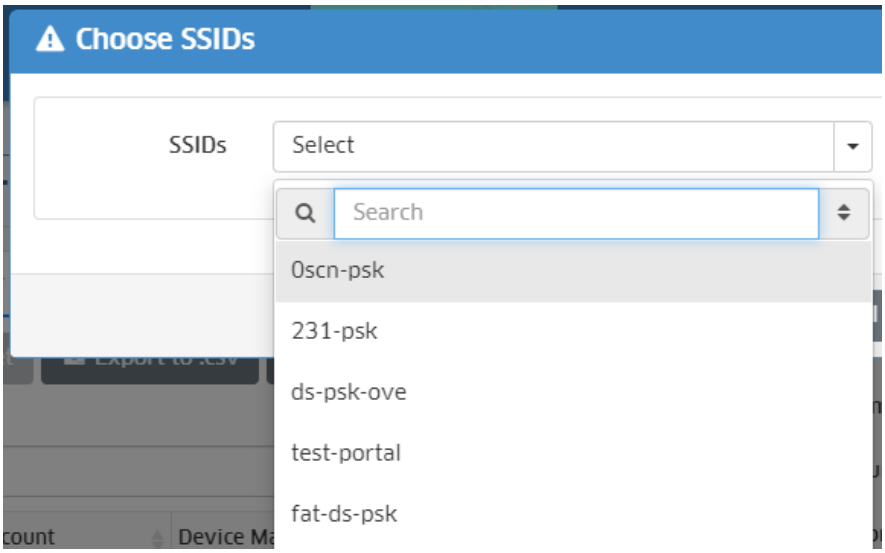




In Company Property List UI, the PSK can be printed

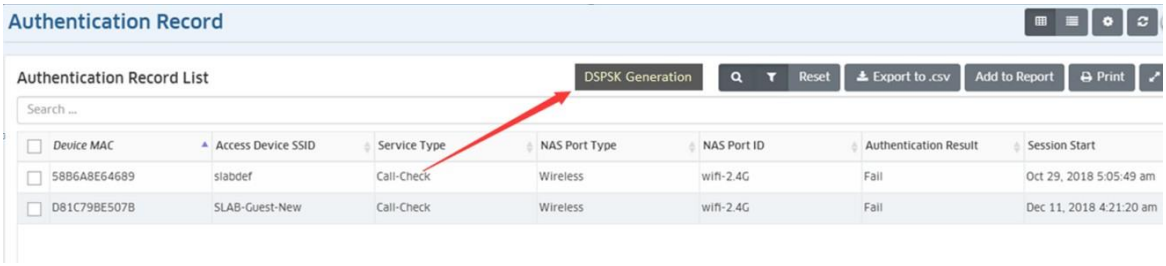


When click the button ‘Print QR Code Of DSPSK’， user should choose an existing SSID to print



3. Generating DSPSK from Authentication Records

In UPAM Authentication Record, the admins can choose a few records to batch generate the DSPSK.(Home->UPAM->Authentication-> Authentication Record)



5.48 IPv6 application in Stellar AP

IPv6 protocol enables next generation large-scale IP networks by supporting addresses that are 128 bits long. This allows 2^{128} possible addresses (compared to 2^{32} possible IPv4 addresses). Most government and large university RFPs request support for IPv6 managed infrastructure. According to the requirements of the customers and the products development needs, Stellar AP now supports more and more applications of Ipv6 as described below.

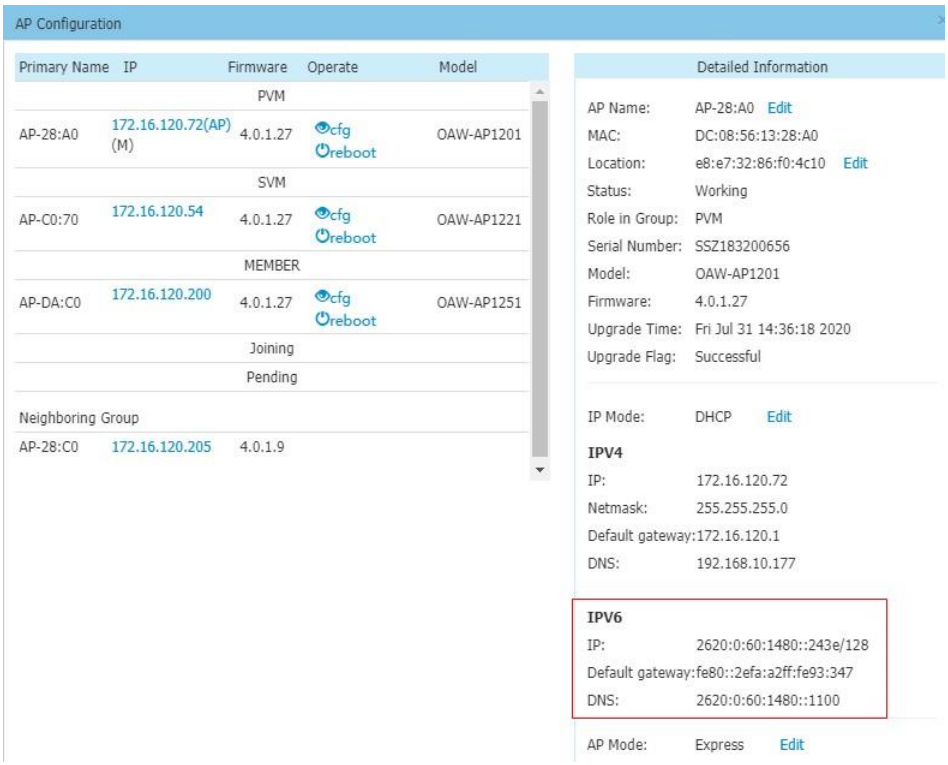
5.48.1 Stellar AP supports IPv4/IPv6 dual stack.

Ipv4 and Ipv6 address can be shown with the command "ifconfig br-wan" in CLI. Stellar AP can be fully managed over Ipv6 interface.

```
support@AP-DA:C0:~$ ifconfig br-wan
br-wan    Link encap:Ethernet  HWaddr 34:E7:0B:03:DA:C0
          inet addr:172.16.120.200  Bcast:172.16.120.255  Mask:255.255.255.0
          inet6 addr: 2620:0:60:1480:36e7:bff:fe03:dac0/64 Scope:Global
          inet6 addr: fe80::36e7:bff:fe03:dac0/64 Scope:Link
          inet6 addr: 2620:0:60:1480::20f1/128 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:40815 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4918 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3955436 (3.7 MiB)  TX bytes:1322653 (1.2 MiB)
```

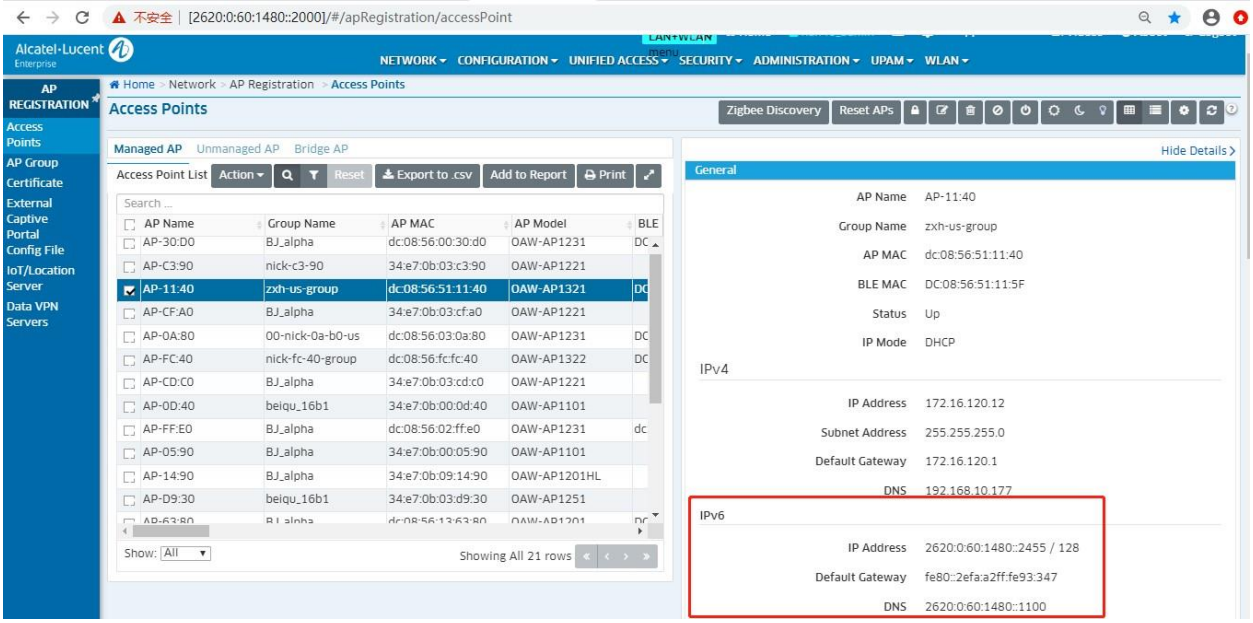
5.48.1.1 IPv6 display on cluster web UI.

Login the cluster, click the AP module, and it's seen in the Detailed Information of AP Configuration.



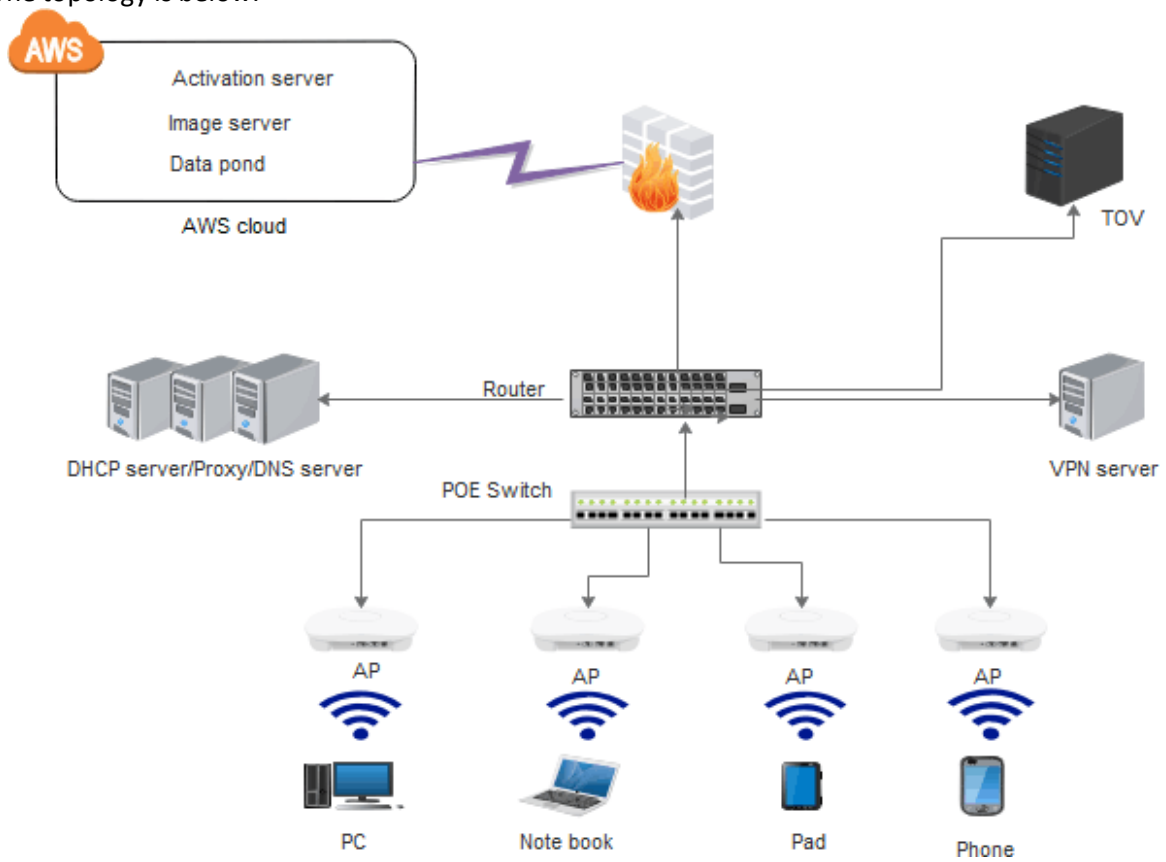
5.48.1.2 IPv6 display on OVC/OVE web UI.

Check Path: Home→Network →Access Points, select one AP and it is seen in the Details right.



5.48.2 Registering to OVC over IPv6.

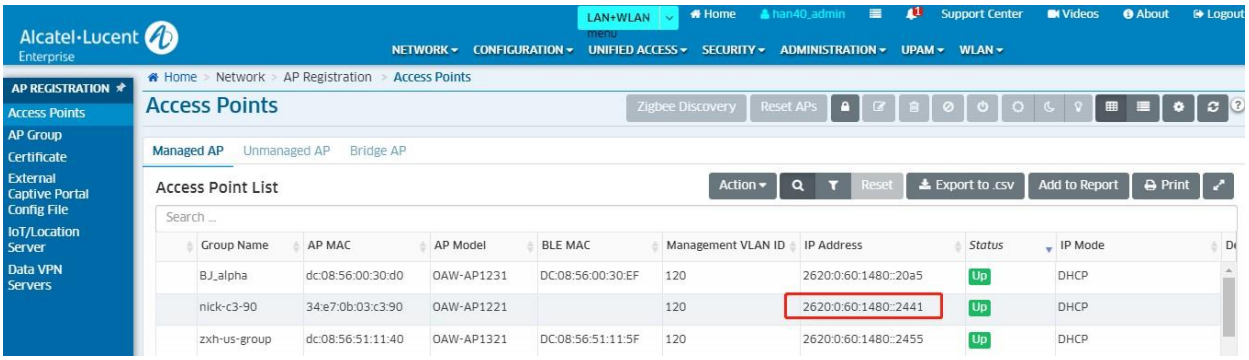
The topology is below:



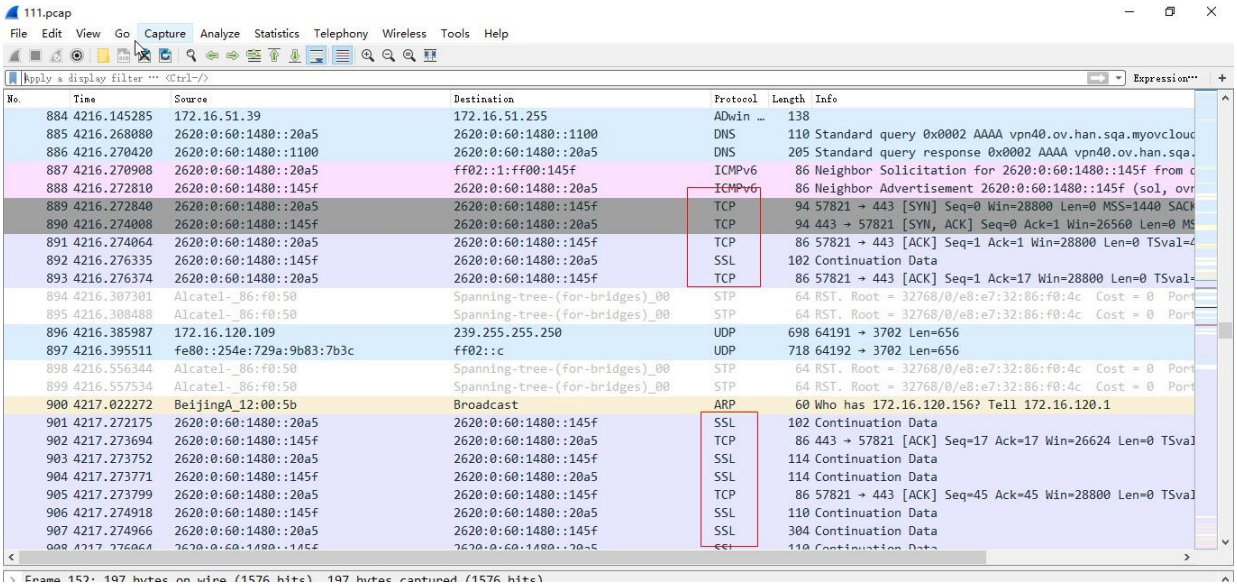
Stellar APs of all models can register to OVC over IPv6. And only AP1201BG does not consume the license.

Stellar AP shall register to OVC over IPv6 first under dual stack. And it shall use IPv4 to register to OVC when IPv6 is not available under dual stack.

If the registering to OVC is over IPv6, the IP Address displayed in the Access Points list shall be IPv6 as shown in below screenshot. Otherwise, it shall be over IPv4.



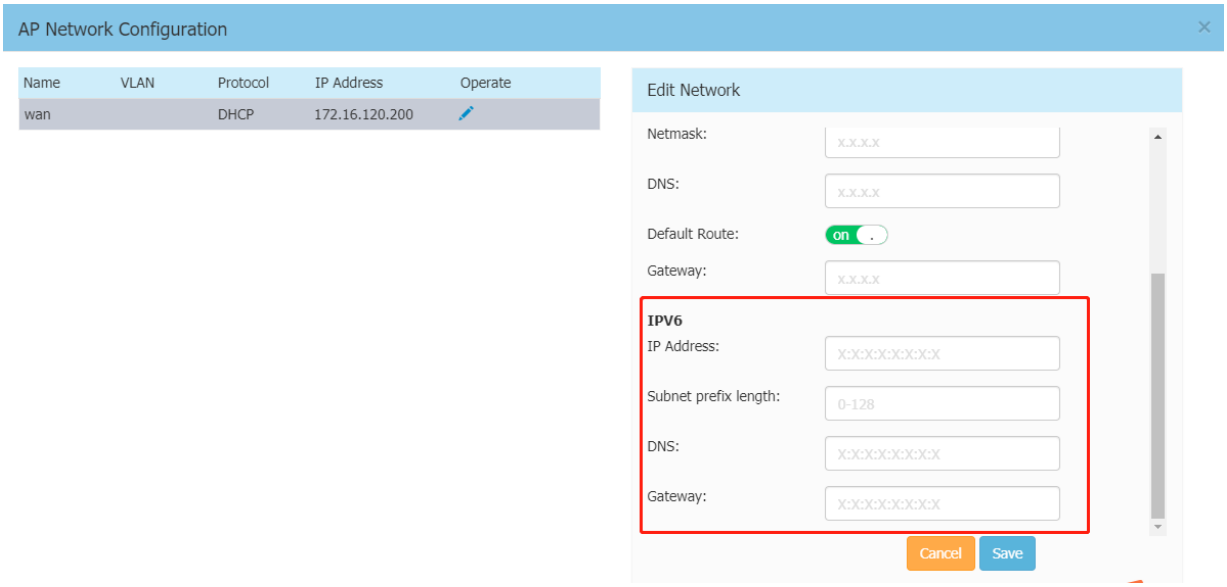
Also it can be checked whether it is over IPv6 to register to OVC through the capture.



5.48.3 Set static IPv6 address.

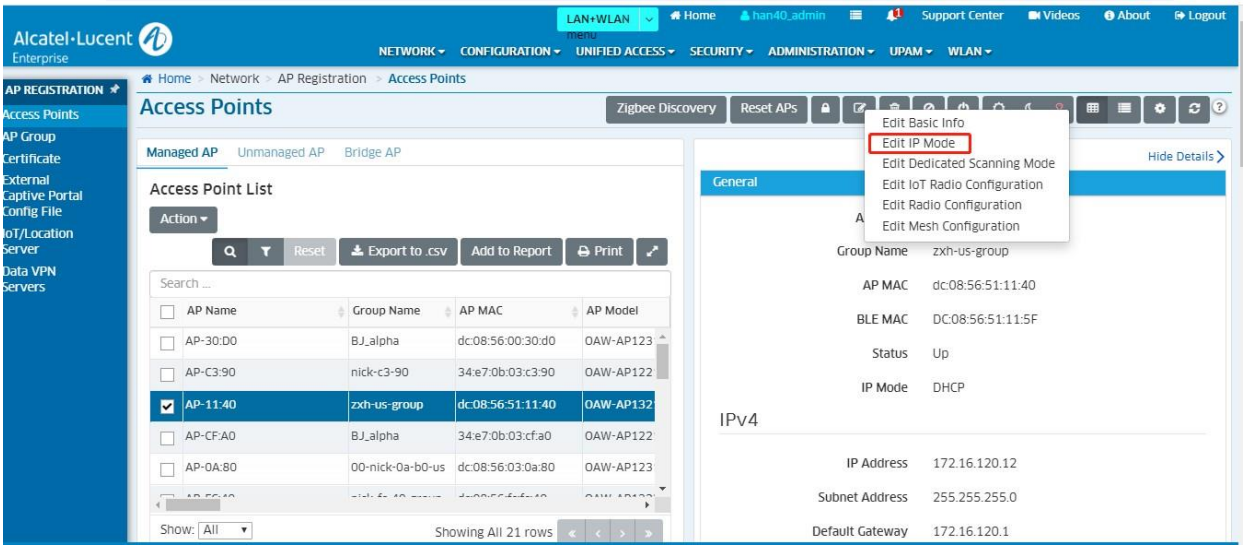
5.48.3.1 Static IPv6 address set on cluster web UI

First login the cluster, click the AP module and select on AP and enter its AP UI, then edit the AP Network Configuration, choose the protocol to be static.

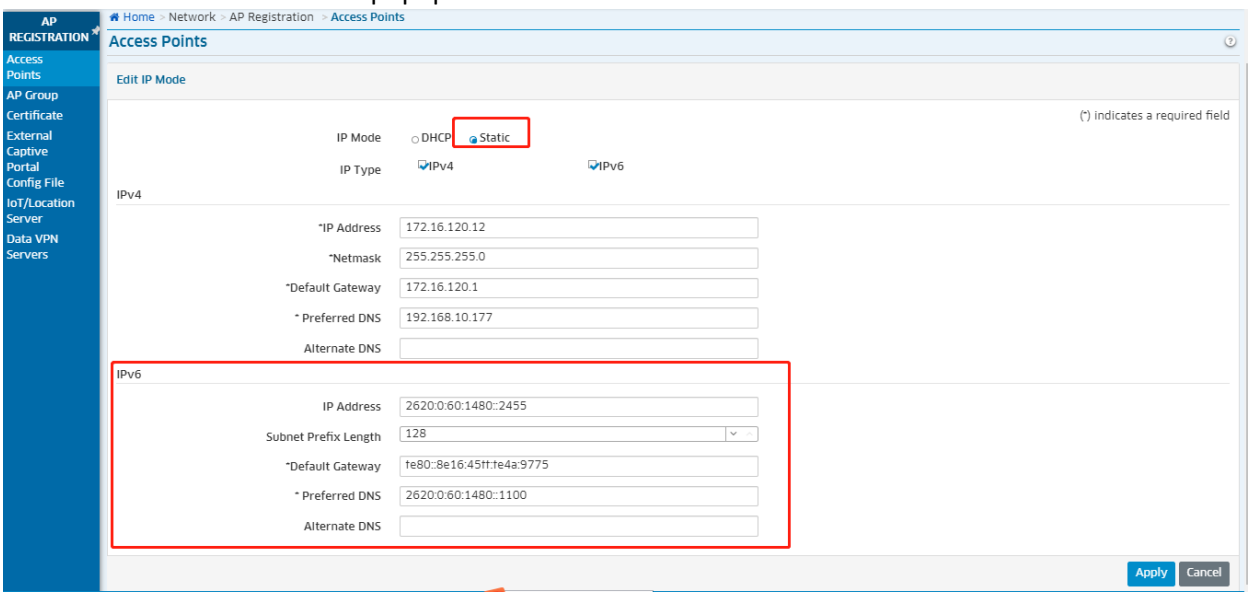


5.48.3.2 Static IPv6 address set on OVC web UI

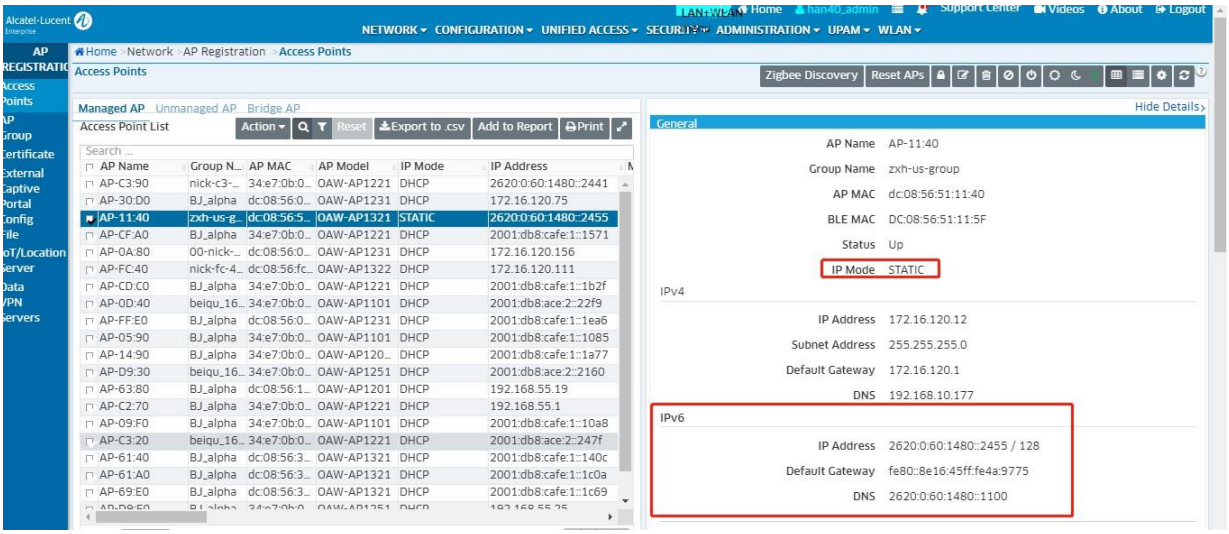
Navigate to Home>Network>Access Points, select one AP and click on Edit button, then click “edit IP Mode”.



Select the “static” mode in the popup window.



After finishing the setting, static IPv6 can be displayed as below:



5.48.4 Support authentication IPv6 client with external Radius Server and external captive portal server hosted with IPv6 address

The related test cases are tested by TMA team because UPAM supporting IPv6 is not required in this release.

5.48.4.1 Authentication IPv6 client with external Radius Server

5.48.4.2 Authentication IPv6 client with external captive portal

This feature is mainly to increase the support of the captive portal ipv6 protocol stack. When the client is in the ipv6 network environment, the AP can perform ipv6 redirection and perform portal authentication. Current Captive Portal supports dual stacks.

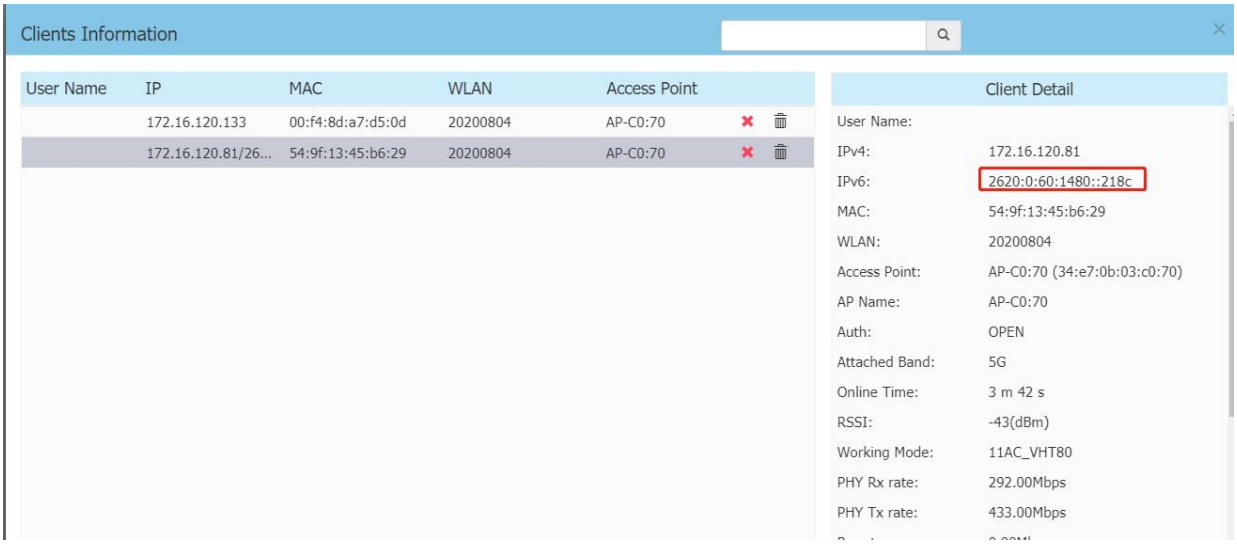
5.48.5 IPv6 clients' display on cluster/OVC web UI.

Only the stateful IPv6 address can be displayed for IPv6 client now as shown in below screenshots. The stateless IPv6 address for the IPv6 client won't be displayed.

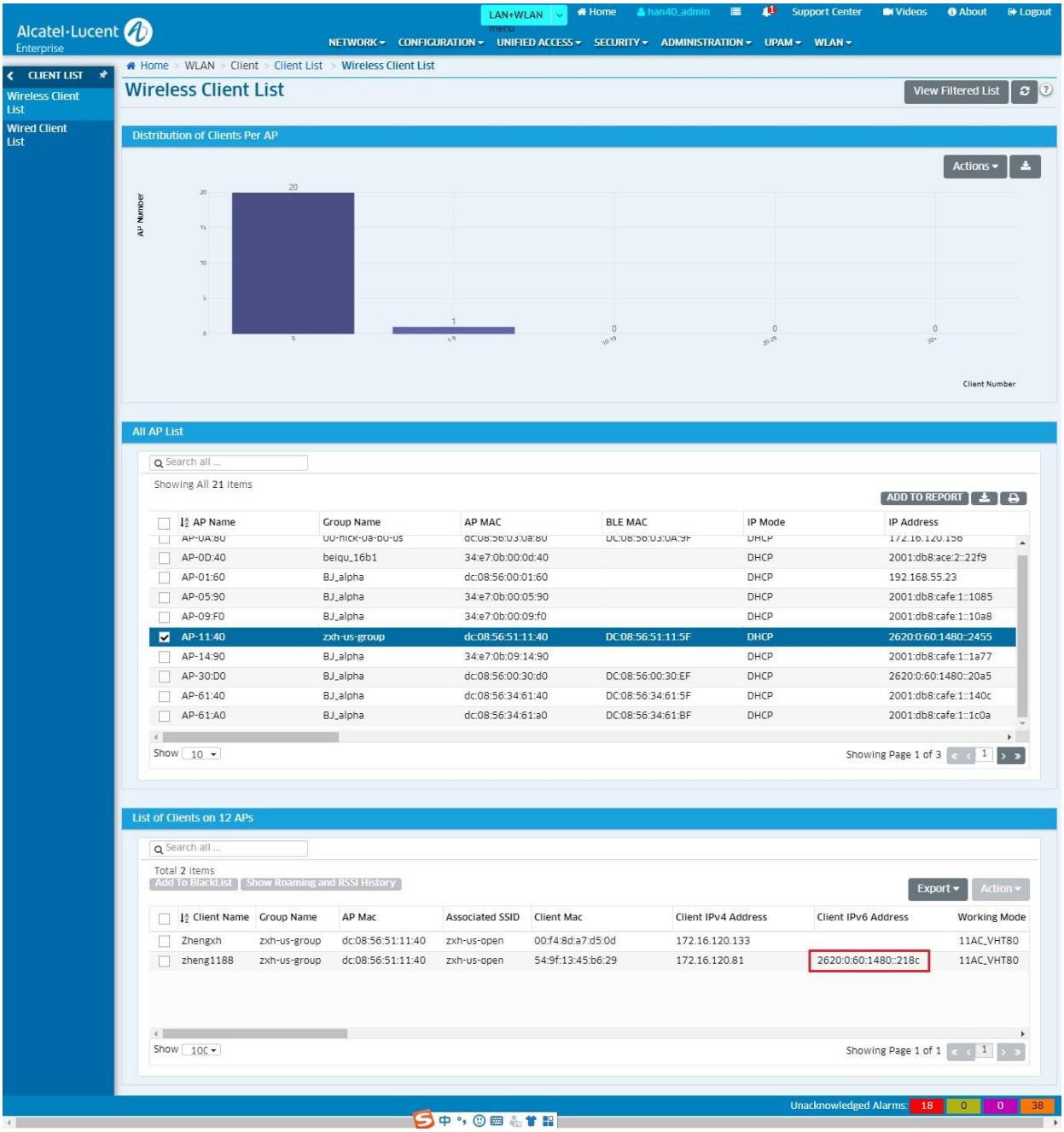
The result of sta_list:

```
support@AP-C0:70:~$ ssudo sta_list
SSID:20200804
STA_MAC              IPv4          IPv6                  OnlineTime      RX      TX          FREQ    AUTH    Final_role                VLANID  TUNNE
LID  FARENDIP
SSID:20200804
STA_MAC              IPv4          IPv6                  OnlineTime      RX      TX          FREQ    AUTH    Final_role                VLANID  TUNNE
LID  FARENDIP
00:f4:8d:a7:d5:0d  172.16.120.133                          27            171088        9862      5GHz OPEN    1596511743649arp          0     0
54:9f:13:45:b6:29  172.16.120.81     2620:0:60:1480::218c   929           90070         42860     5GHz OPEN    1596511743649arp          0     0
support@AP-C0:70:~$
support@AP-C0:70:~$
```

Clients Information on cluster web UI.



Clients Information on OVC web UI.



Note:

When the IPv6 clients are Windows type, its stateful IPv6 address cannot be displayed now though they have obtained both stateful and stateless IPv6 address.

Andriod clients cannot obtain the stateful IPv6 address. Stateless IPv6 address is OK.

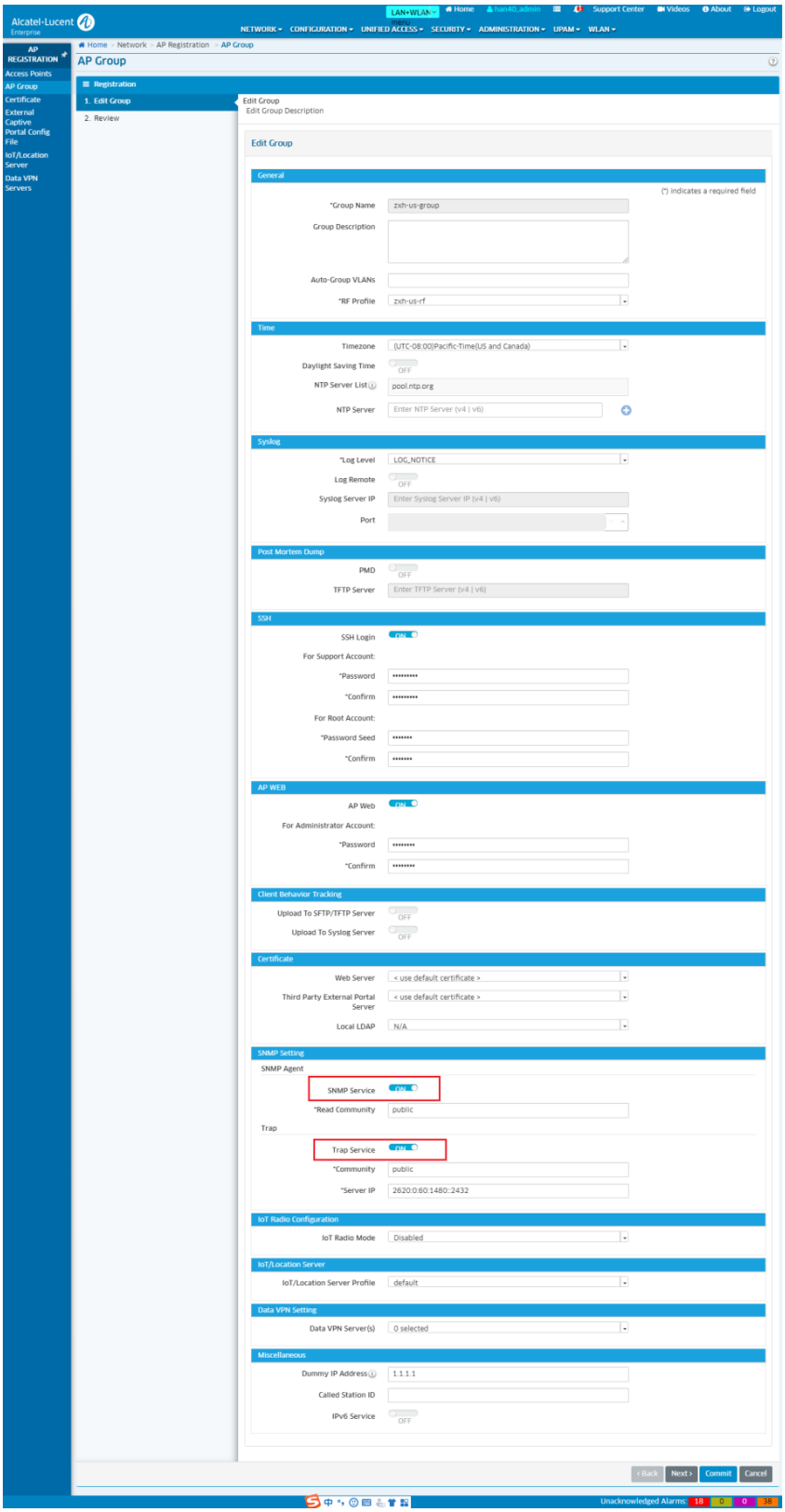
5.48.6 Neighbor (adme show) supports IPv6 address

Neighbor IPv6 address can be seen with the command “adme show”.

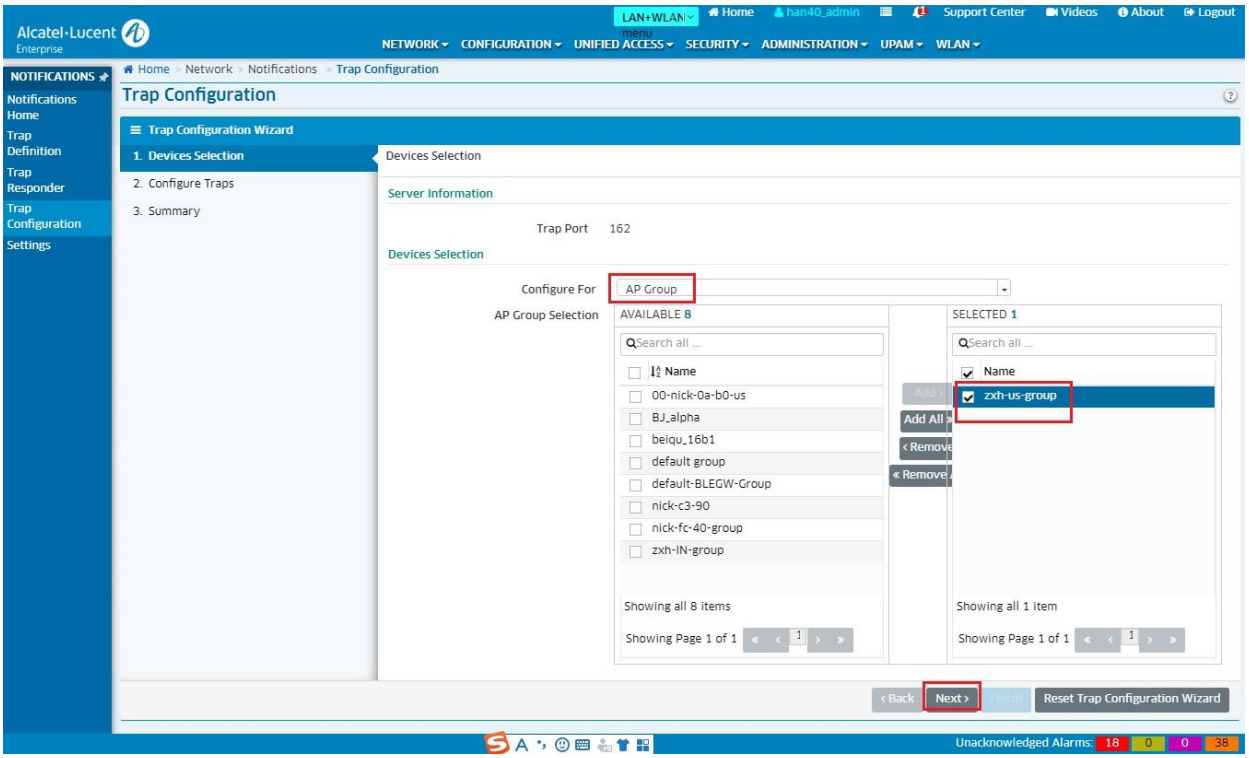
```
support@AP-DA:C0:~$ adme show
mac                ip              ip6                                     ov_ip           tenantId        state  name       version    radiocnt  radioid   ch
annel   bandwidth  rssi    txpower
34:e7:0b:03:c0:70  172.16.120.54   2620:0:60:1480:36e7:bff:fe03:c070       0.0.0.0                         0      AP-C0:70   4.0.1.27   2         0         11
        20         37      17
                                                                                                                                                   1         60
        80         64      7
dc:08:56:0a:31:90  192.168.89.14   ::                                      0.0.0.0                         1                                 2         0         11
        20         15      0
                                                                                                                                                   1         14
9       80         23      0
dc:08:56:13:28:a0  172.16.120.72   2620:0:60:1480::243e                    0.0.0.0                         0      AP-28:A0   4.0.1.27   2         0         11
        20         40      3
                                                                                                                                                   1         56
        80         67      10
34:e7:0b:03:c0:90  192.168.89.26   ::                                      0.0.0.0                         1                                 2         0         0
        0          0       0
                                                                                                                                                   1         14
9       80         24      0
dc:08:56:13:28:c0  172.16.120.205  2620:0:60:1480:de08:56ff:fe13:28c0      0.0.0.0                         0      AP-28:C0   4.0.1.9    2         0         6
        20         17      16
                                                                                                                                                   1         48
        80         50      19
dc:08:56:13:71:60  172.16.200.115  fe80::de08:56ff:fe13:7160               0.0.0.0                         1                                 2         0         11
        20         18      0
                                                                                                                                                   1         36
```

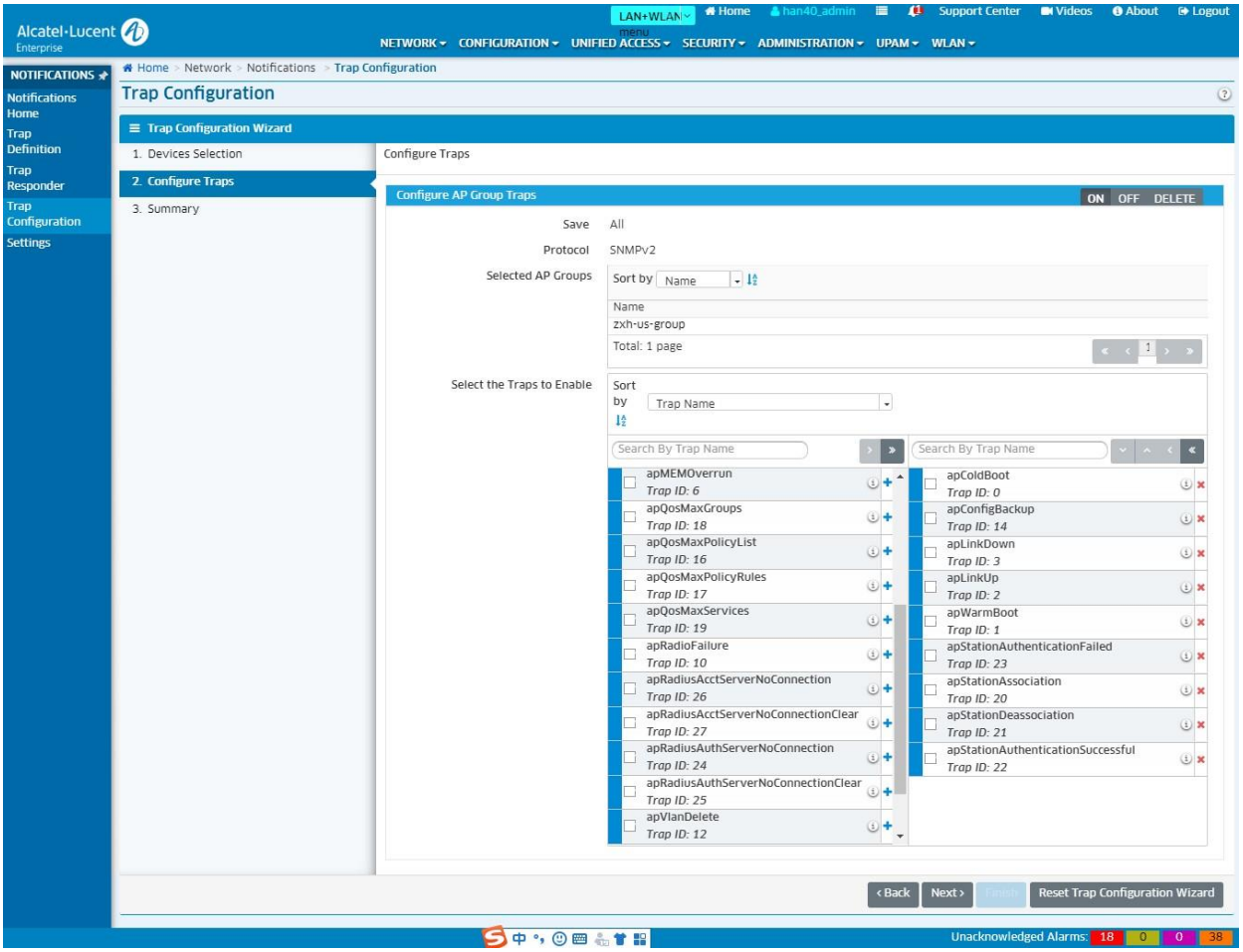
5.48.7 SNMP trap supports IPv6

Enable the SNMP service and Trap service in the group configuration first.

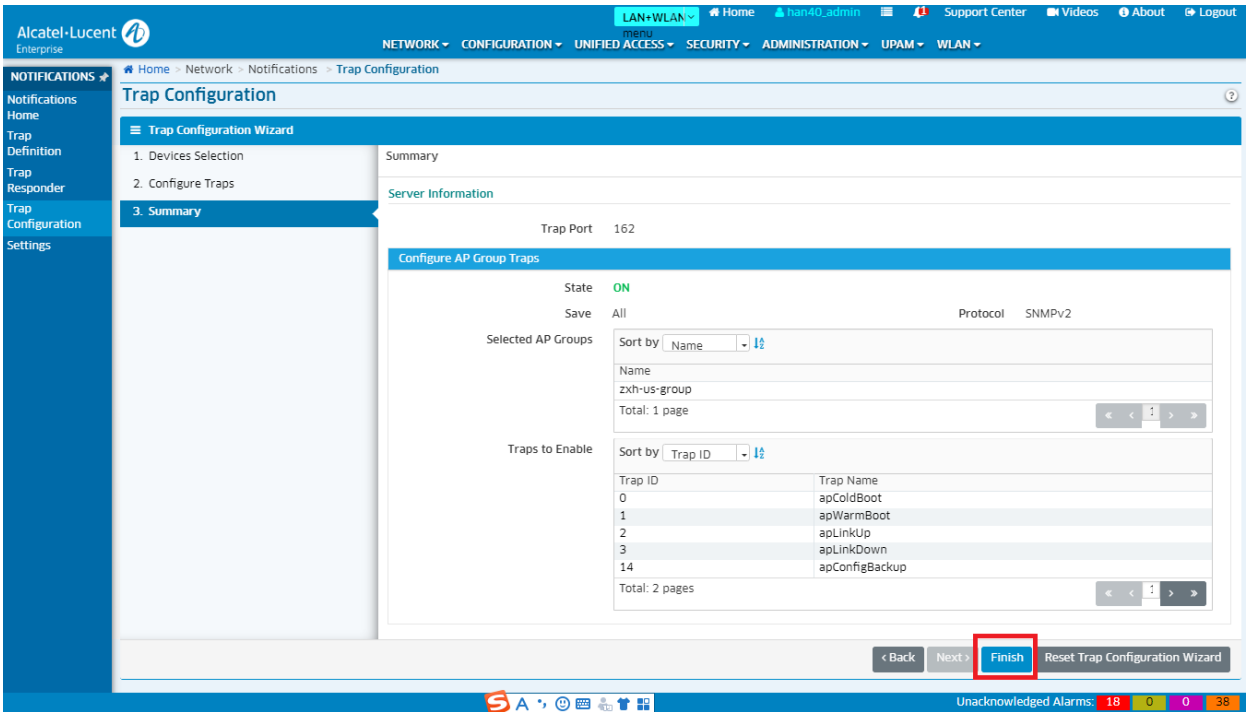


Navigate to Network > Notifications > Trap Configuration, select the device and the traps to enable.

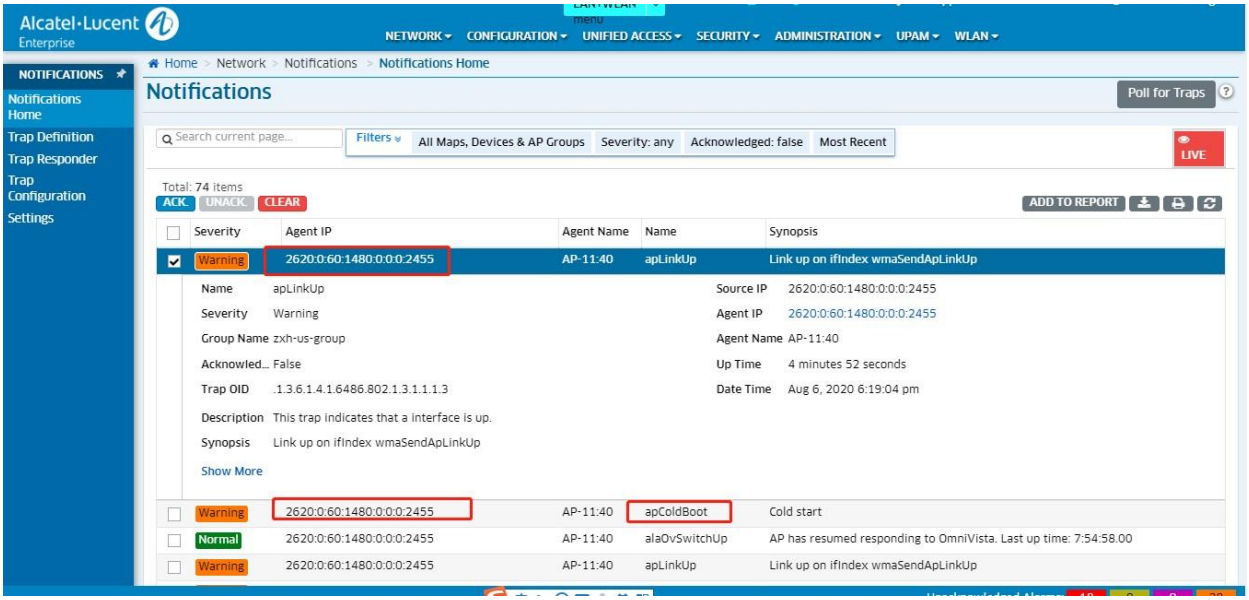




Check the trap summary configuration and save.



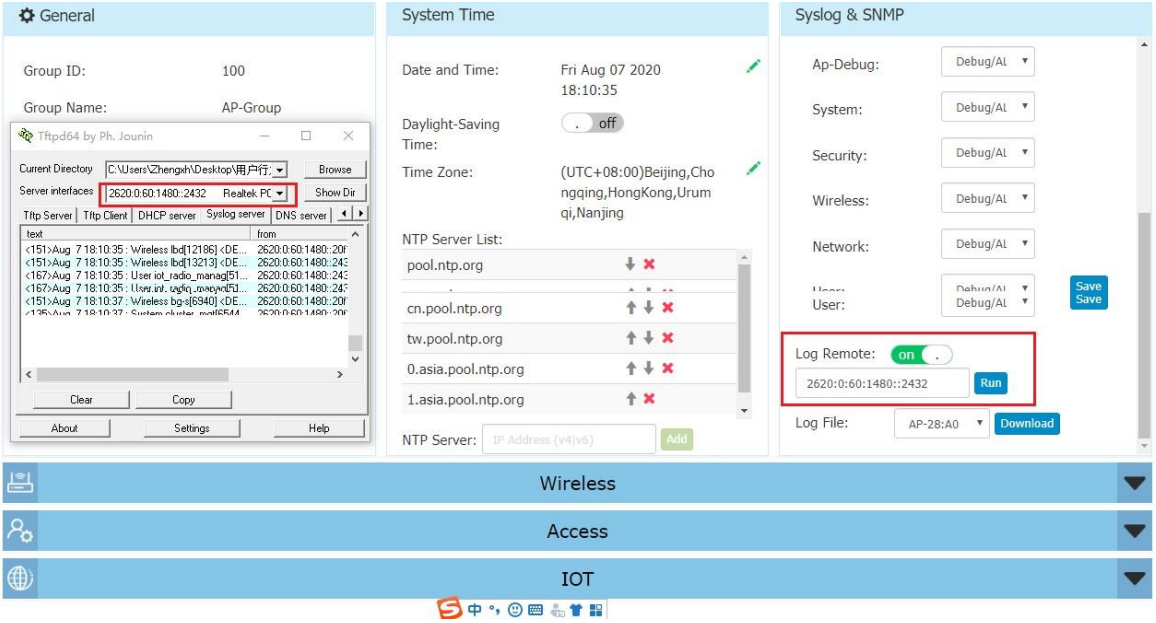
Navigate to Network>Notifications>Notifications Home, Trap notifications are displayed



5.48.8 Support to use IPv6 syslog server.

5.48.8.1 Set IPv6 syslog server on cluster web UI.

Login the cluster, click System > Syslog&SNMP



5.48.8.2 Set IPv6 syslog server on OVC web UI.

Navigate to Network > AP Registration > AP Group, select one group and click the Edit button.

Alcatel·Lucent Enterprise

LAN+WLAN | Home | han40_admin | Support Center | Videos | About | Logout

NETWORK | CONFIGURATION | UNIFIED ACCESS | SECURITY | ADMINISTRATION | UPAM | WLAN

AP REGISTRATION
- Access Points
- AP Group
- Certificate
- External Captive Portal Config File
- IoT/Location Server
- Data VPN Servers

Home > Network > AP Registration > AP Group

AP Group

Registration

1. Edit Group
2. Review

Edit Group
Edit Group Description

Edit Group

General

(*) indicates a required field

*Group Name	zxh-us-group
Group Description	
Auto-Group VLANs	
*RF Profile	zxh-us-rf

Time

Timezone	(UTC+08:00)Beijing,Chongqing,HongKong,Urumqi
Daylight Saving Time	OFF
NTP Server List	pool.ntp.org
NTP Server	Enter NTP Server (v4 | v6)

Syslog

*Log Level	LOG_DEBUG
Log Remote	ON
Syslog Server IP	2620:0:60:1480::2432
Port	514

Post Mortem Dump

PMD	OFF
TFTP Server	Enter TFTP Server (v4 | v6)

SSH

SSH Login	ON
For Support Account:	
*Password	••••••••
*Confirm	••••••••
For Root Account:	
*Password Seed	••••••
*Confirm	••••••

AP WEB

AP Web	ON
For Administrator Account:	
*Password	••••••••
*Confirm	••••••••

Client Behavior Tracking

Upload To SFTP/TFTP Server	OFF
Upload To Syslog Server	OFF

Certificate

Web Server	< use default certificate >
Third Party External Portal Server	< use default certificate >
Local LDAP	N/A

SNMP Setting

SNMP Agent

SNMP Service	ON
*Read Community	public

Trap

Trap Service	ON
*Community	public
*Server IP	2620:0:60:1480::2432

IoT Radio Configuration

IoT Radio Mode	Disabled

IoT/Location Server

IoT/Location Server Profile	default

Data VPN Setting

Data VPN Server(s)	0 selected

Miscellaneous

Dummy IP Address	1.1.1.1
Called Station ID	
IPv6 Service	OFF

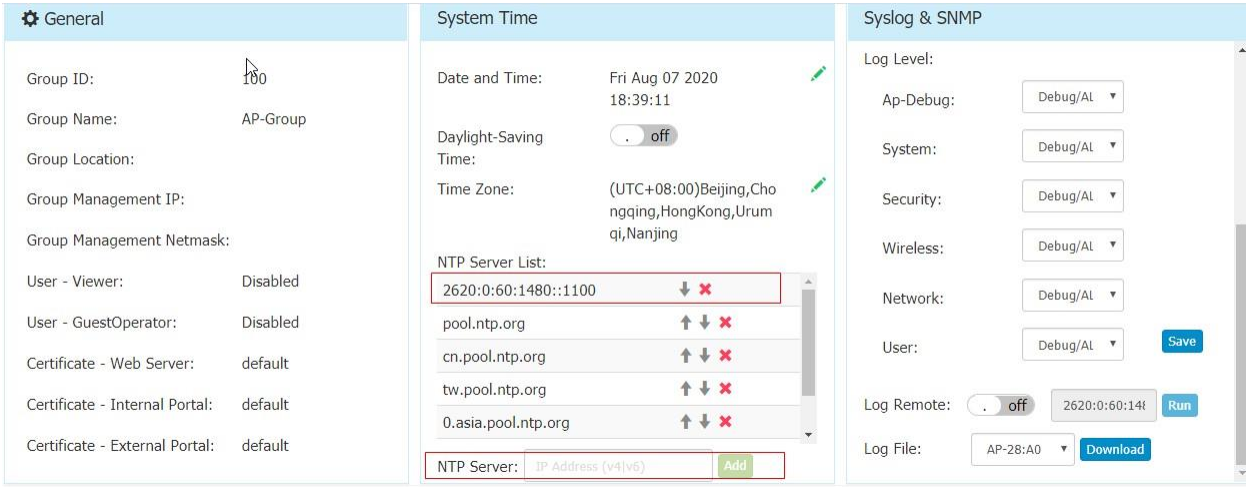
< Back | Next > | Commit | Cancel

Unacknowledged Alarms: 18 | 0 | 0 | 38

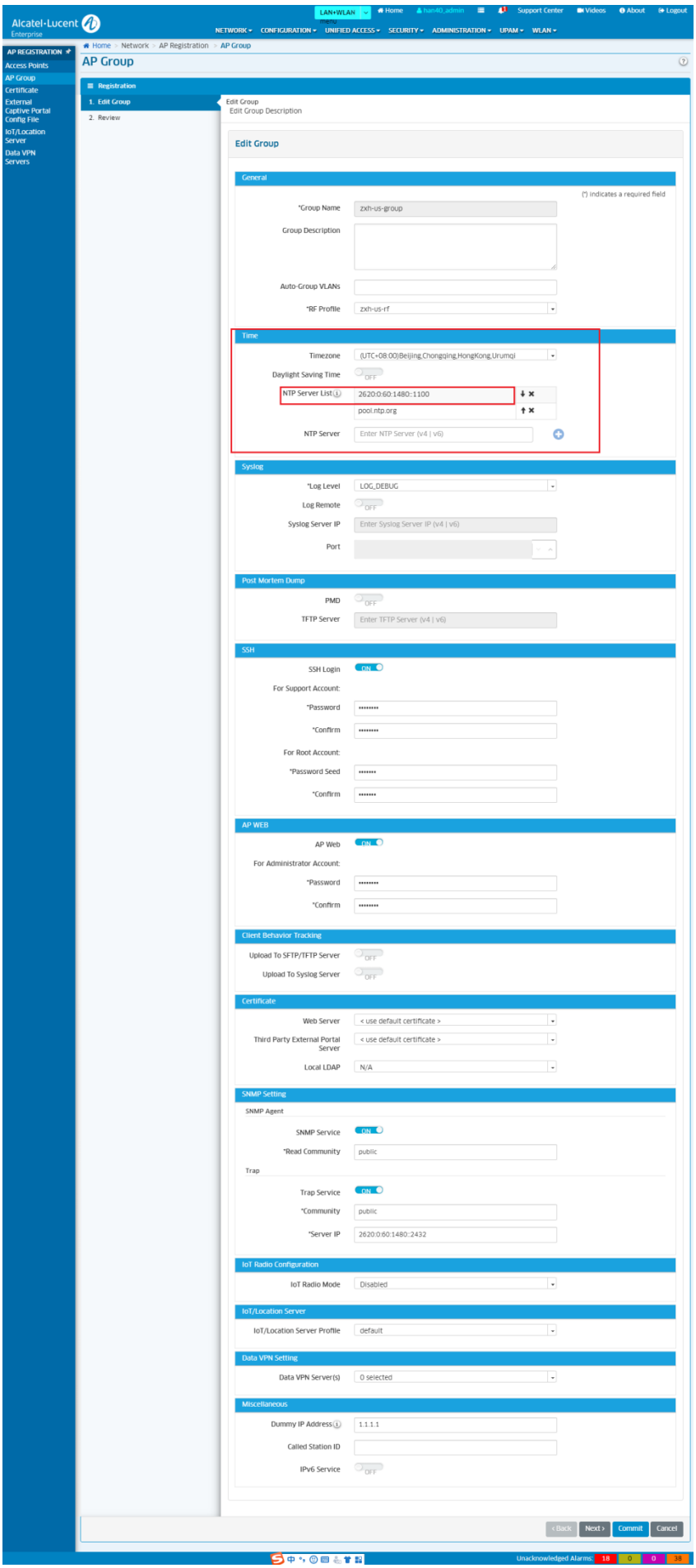
5.48.9 Support to configure IPv6 NTP server

```
root@AP-11:40:~# ntpdate 172.16.120.101
 7 Aug 17:58:48 ntpdate[28274]: adjust time server 172.16.120.101 offset 0.006516 sec
root@AP-11:40:~#
root@AP-11:40:~# ntpdate -6 2620:0:60:1480::1100
 7 Aug 17:59:11 ntpdate[28605]: adjust time server 2620:0:60:1480::1100 offset -0.003662 sec
root@AP-11:40:~#
```

On cluster web UI:

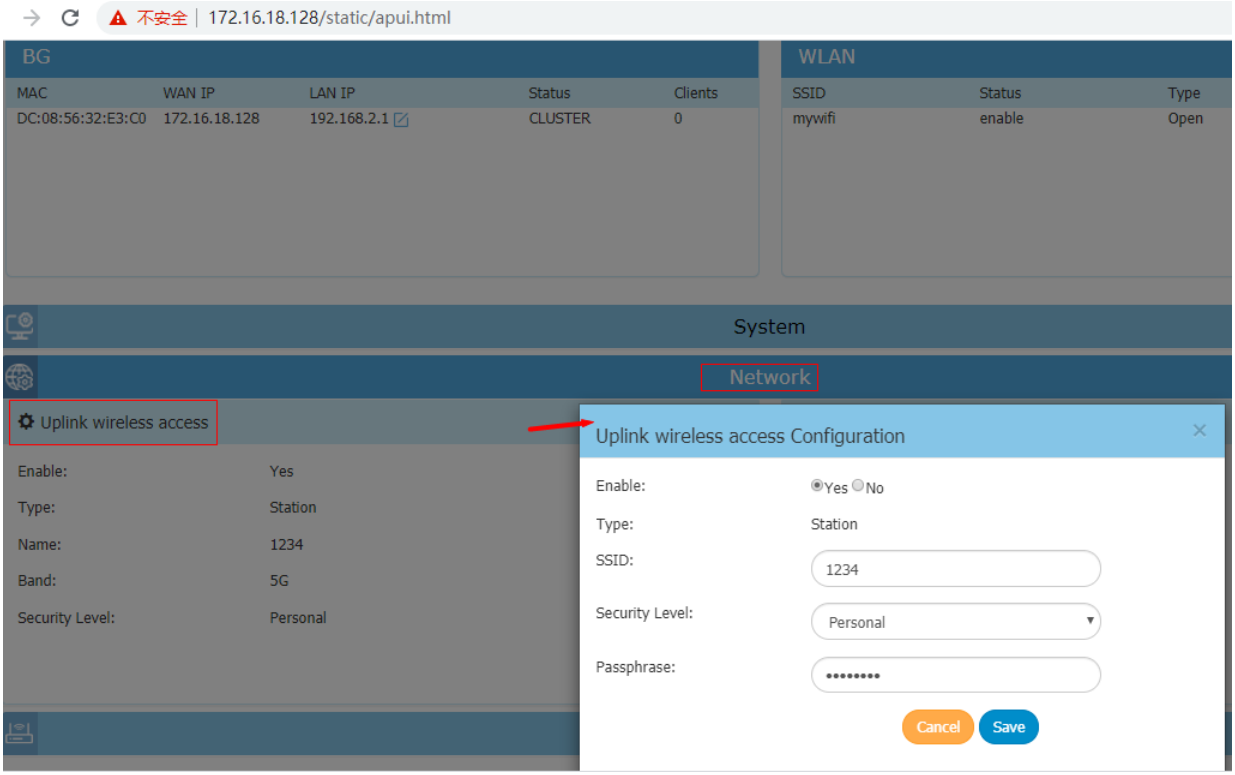


On OVC web UI: Navigate to Network > AP Registration > AP Group, select one group and click the Edit button.


Alcatel-Lucent Enterprise
LAN+WLAN
Home
Support Center
Videos
About
Logout
NETWORK
CONFIGURATION
UNIFIED ACCESS
SECURITY
ADMINISTRATION
UPAM
WLAN
AP REGISTRATION
Access Points
AP Group
Certificate
External Captive Portal Config File
IoT/Location Server
Data VPN Servers
Home > Network > AP Registration > AP Group
AP Group
Registration
1. Edit Group
2. Review
Edit Group
Edit Group Description
Edit Group
General
(*) indicates a required field
*Group Name
zxh-us-group
Group Description
Auto-Group VLANs
*RF Profile
zxh-us-rf
Time
Timezone
(UTC+08:00)Beijing,Chongqing,HongKong,Urumqi
Daylight Saving Time
OFF
NTP Server List
2620:0:60:1480::1100
pool.ntp.org
NTP Server
Enter NTP Server (v4 | v6)
Syslog
*Log Level
LOG_DEBUG
Log Remote
OFF
Syslog Server IP
Enter Syslog Server IP (v4 | v6)
Port
Post Mortem Dump
PMD
OFF
TFTP Server
Enter TFTP Server (v4 | v6)
SSH
SSH Login
ON
For Support Account:
*Password
*Confirm
For Root Account:
*Password Seed
*Confirm
AP WEB
AP Web
ON
For Administrator Account:
*Password
*Confirm
Client Behavior Tracking
Upload To SFTP/TFTP Server
OFF
Upload To Syslog Server
OFF
Certificate
Web Server
< use default certificate >
Third Party External Portal Server
< use default certificate >
Local LDAP
N/A
SNMP Setting
SNMP Agent
SNMP Service
ON
*Read Community
public
Trap
Trap Service
ON
*Community
public
*Server IP
2620:0:60:1480::2432
IoT Radio Configuration
IoT Radio Mode
Disabled
IoT/Location Server
IoT/Location Server Profile
default
Data VPN Setting
Data VPN Server(s)
0 selected
Miscellaneous
Dummy IP Address
1.1.1.1
Called Station ID
IPv6 Service
OFF
< Back
Next >
Commit
Cancel
Unacknowledged Alarms:

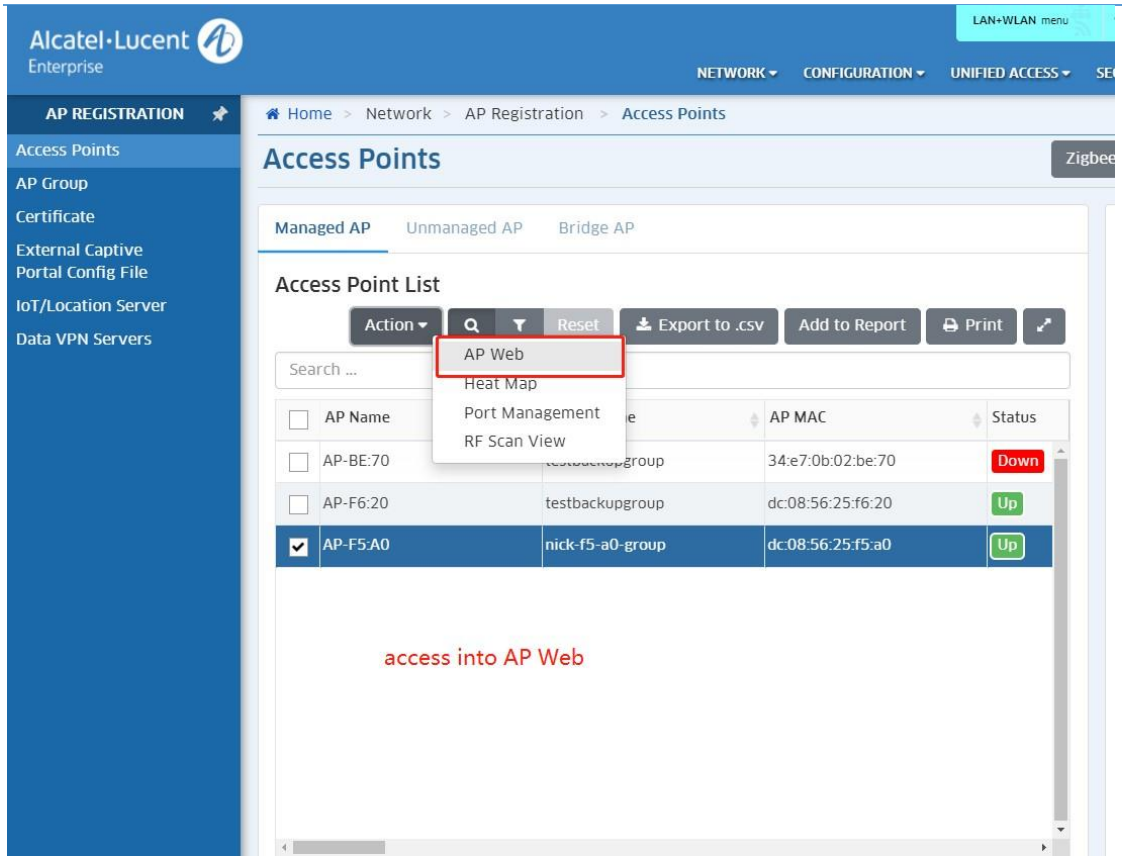
6. Uplink Wireless Access

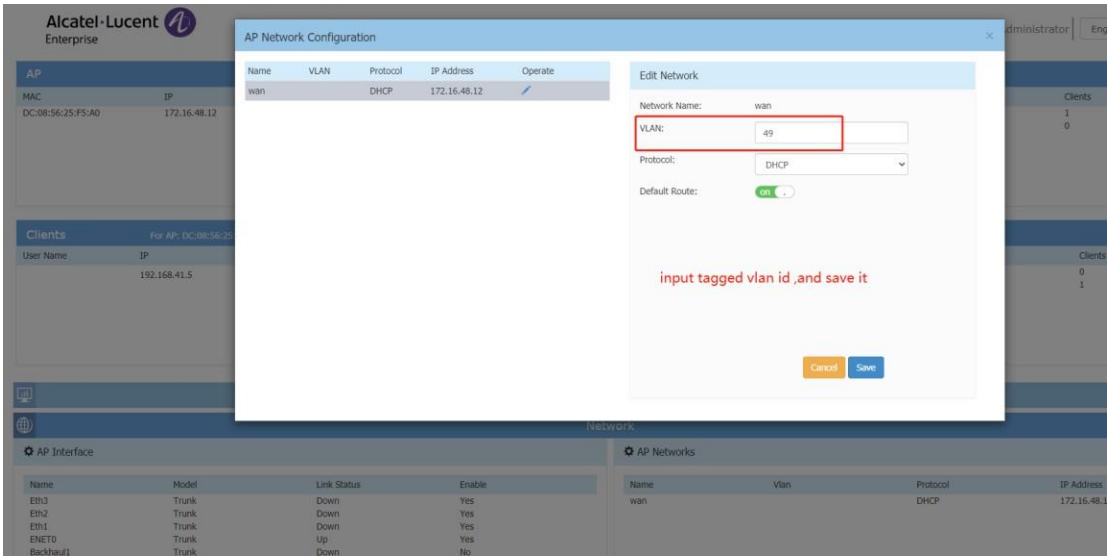
AP1201BG devices can connect to the same WLAN as a client and then create a BG group. The configuration is as below:



5.49 Management Tagged VLAN

5.49.1 Change br-wan interface to tagged





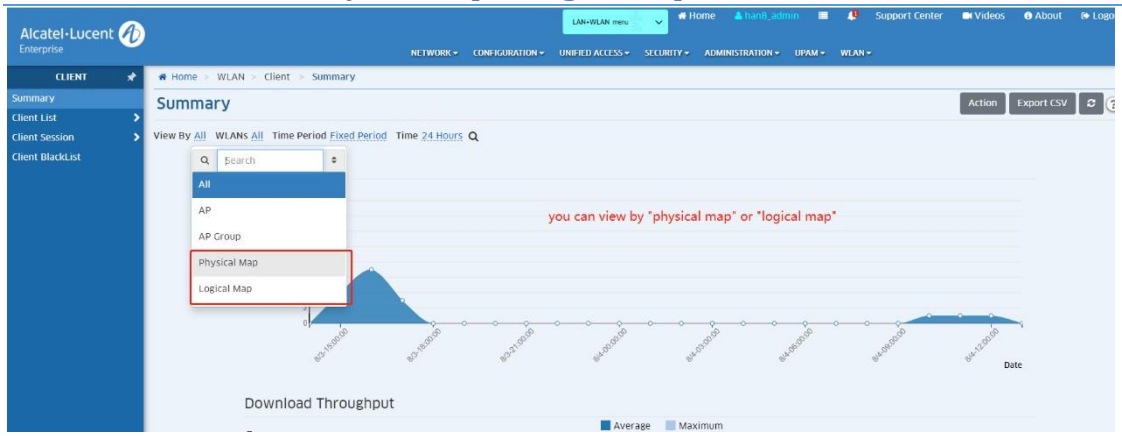
```
support@AP-F5:A0:/etc/config$ cat netmgr
{
        "mode":"AP",
        "visible":[
                {
                        "type":"interface",
                        "visible":[
                                "all"
                        ]
                },
                {
                        "type":"network",
                        "visible":[
                                "common",
                                "vlan"
                        ]
                }
        ],
        "interface":[
                {
                        "name":"Backhaul1",
                        "ifname":"athap1",
                        "enable":"Yes",
                        "type":[
                                "Wireless"
                        ],
                        "mode":"Trunk"
                },
                {
                        "name":"ENET0",
                        "ifname":"eth0",
                        "enable":"Yes",
                        "type":[
                                "Ethernet"
                        ],
                        "mode":"Trunk"
                }
        ],
        "network":[
                {
                        "name":"wan",
                        "iface_name":"wan",
                        "type":"common",
                        "proto":"DHCP",
                        "default_route":"enable",
                        "vid":49,
                        "interface":[]
                }
        ],
        "br_ignore_netfilter":false,
        "br_unicast_drop":true
}
```

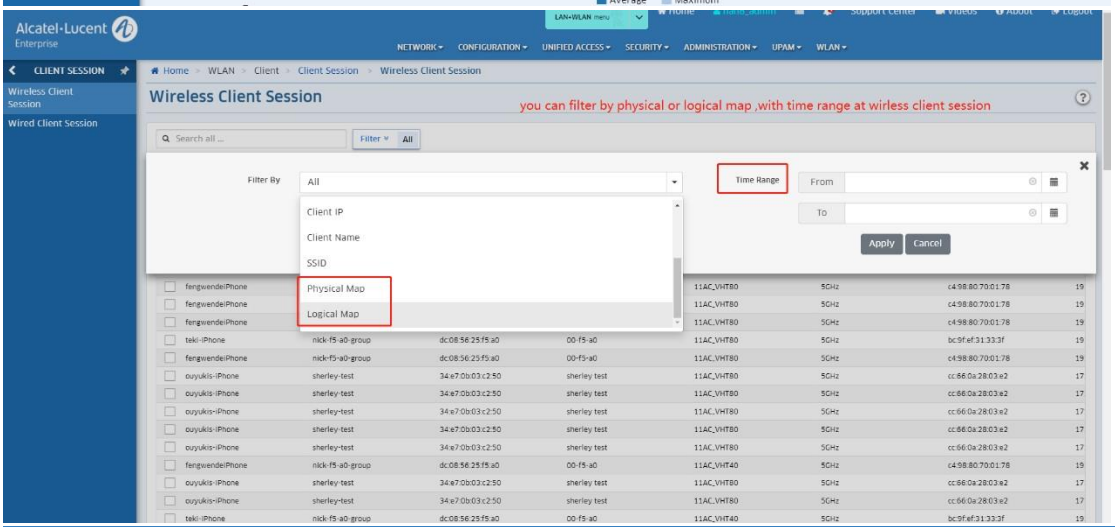
AP would save the configuration at /etc/config/netmgr

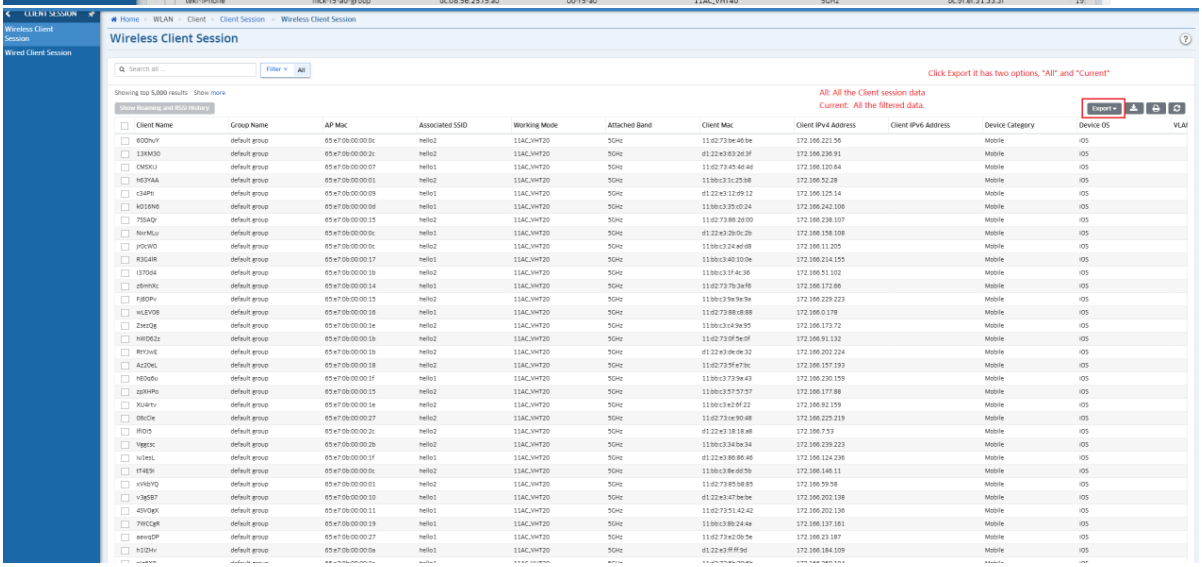
```
br-vlan0  Link encap:Ethernet  HWaddr DC:08:56:25:F5:A0
          inet6 addr: fe80::de08:56ff:fe25:f5a0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1796 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:215725 (210.6 KiB)  TX bytes:1078 (1.0 KiB)

br-wan    Link encap:Ethernet  HWaddr DC:08:56:25:F5:A0
          inet addr:172.16.49.10  Bcast:172.16.49.255  Mask:255.255.255.0
          inet6 addr: fe80::de08:56ff:fe25:f5a0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4722 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1943 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:750289 (732.7 KiB)  TX bytes:296201 (289.2 KiB)
```

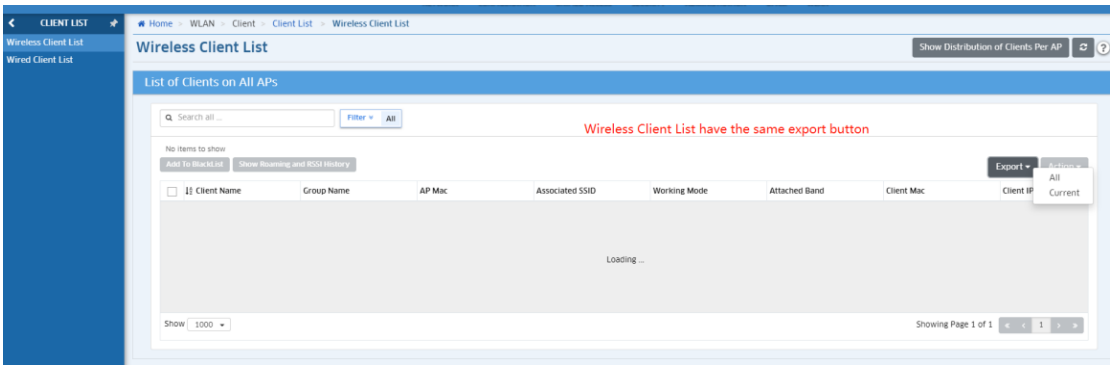
AP would create new bridge named "br-vlan0", and br-wan would get ip from tagged vlan

5.49.2 New button for Physical map vs Logical map







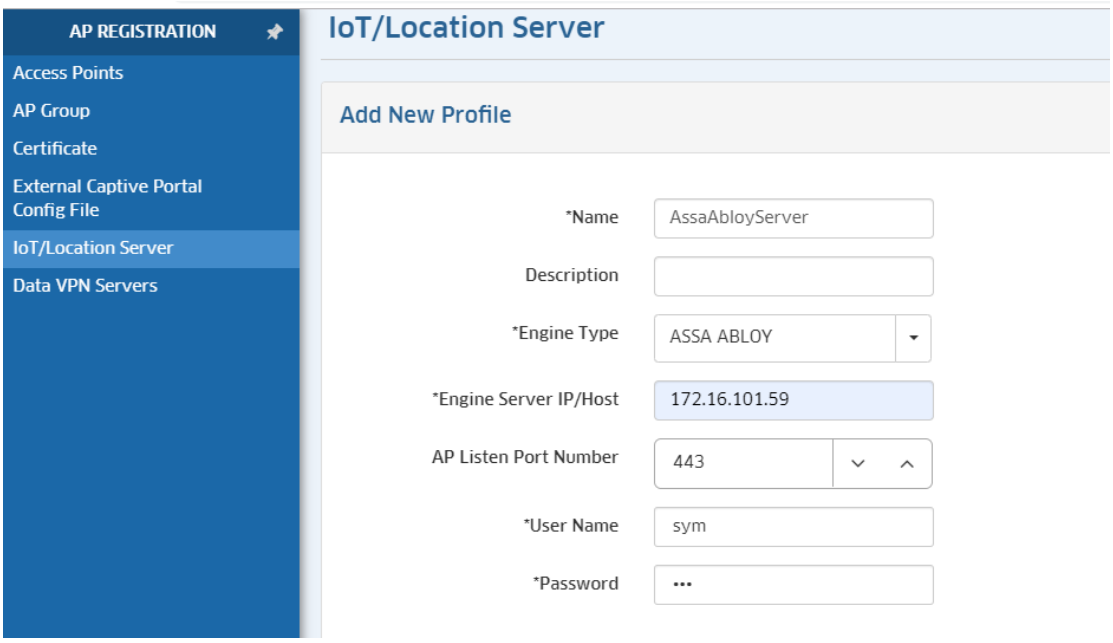


5.50 Zigbee application

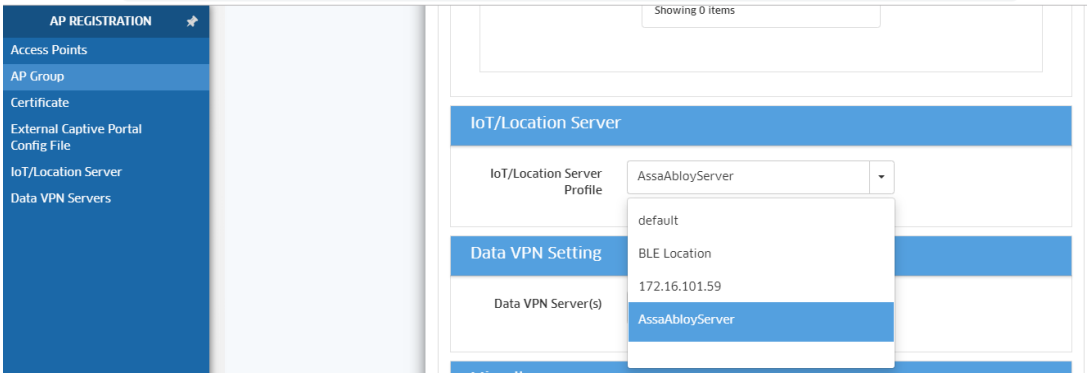
AssaAbloy's electronic door Lock is connected to AP which running Zigbee protocol. The OmniVista System manages the intelligent lock access environment through WMA and ZigbeeControllingService (ZCS for short), and ZCS is responsible for communicating with Visionline Server, thus realizing the communication between Lock and Visionline Server.

5.50.1 Create IoT/Location Server

- Path: Home-->NETWORK-->AP REGISTRATION--> IoT/Location ServerNote: default account and password of Visionline Server is sym/sym.



- Go to AP Group Screen, edit AP Group profile , apply this server profile to AP Group.

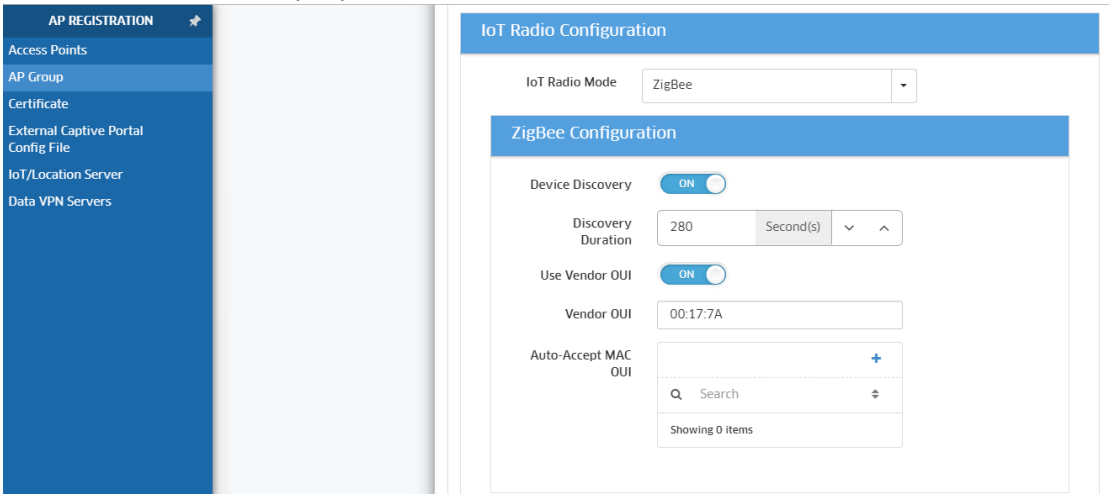


5.50.2 Set Zigbee configuration

Tips: There are two ways to set Zigbee configuration, via AP Group or AP private configuration, Use Private Configuration will prior to AP Group configuration.

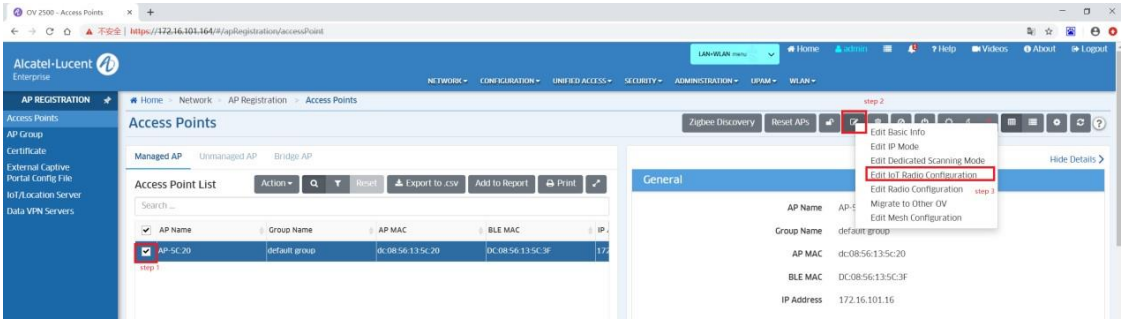
5.50.2.1 Set Zigbee configuration via AP Group.

- Edit the AP Group, open Vendor OUI.

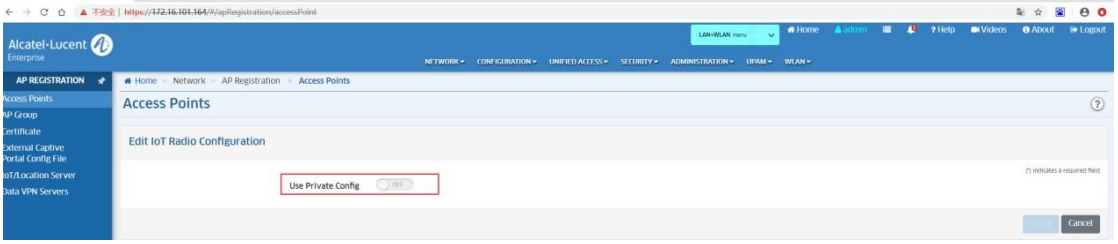


5.50.2.2 Set Zigbee configuration via AP Private config

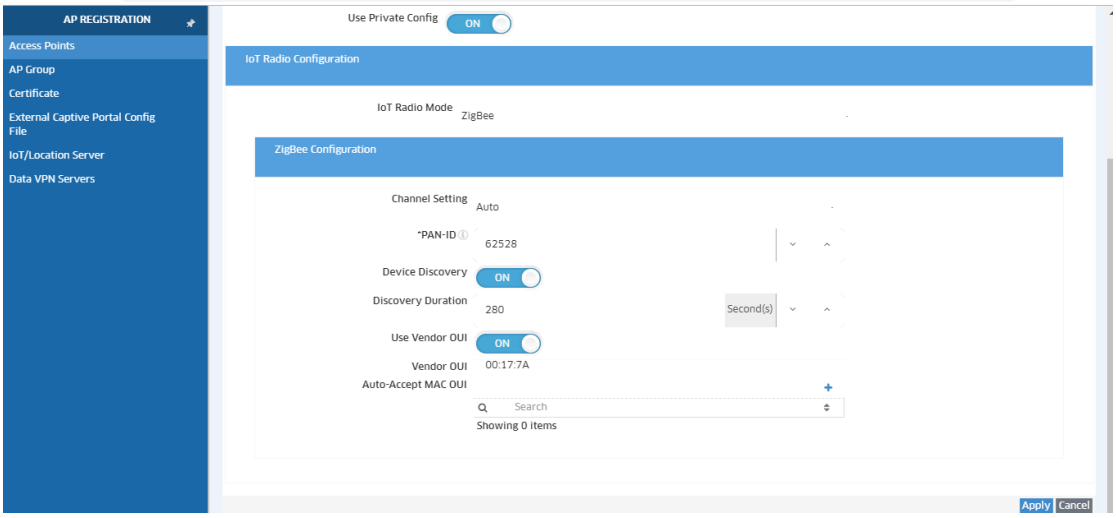
- Path: Home-->NETWORK-->AP REGISTRATION-->Access Point-->Managed AP



- Go to “Edit IoT Radio Configuration” page , open the private switch



- Select “ IoT Radio Mode”--> “Zigbee”. As shown:

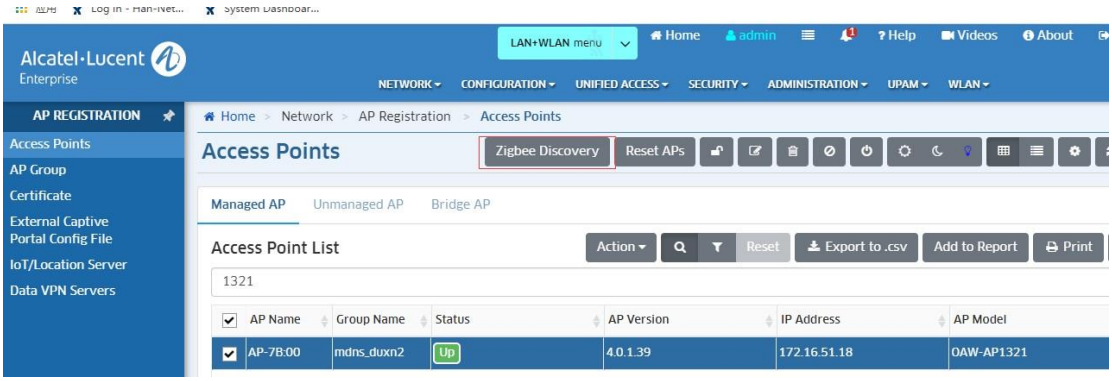


From disable to Zigbee mode, AP will take about 1-2 Minutes , and then activate the Lock with Discovery Card. Card is used for pairing Door lock with AP for the first time. After that lock stores short address of the AP coordinator. After Lock associate with the AP, AP will report the Lock data to OV immediately.

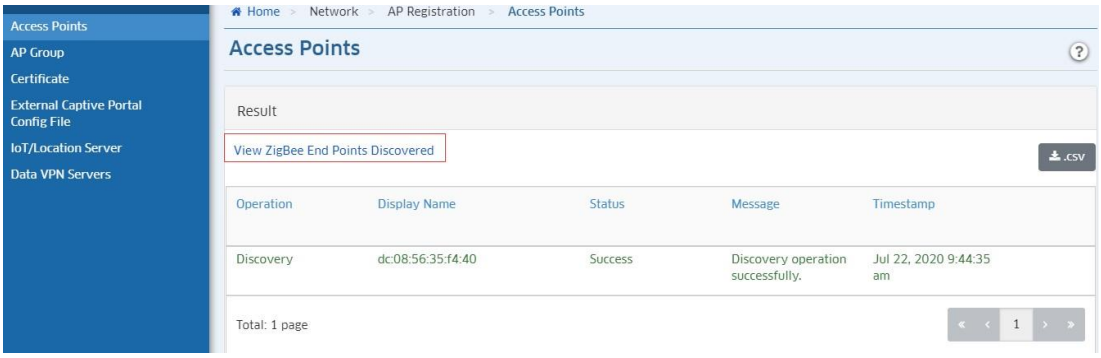
5.50.3 Zigbee Discovery

Select an AP(s) and click on the Zigbee Discovery button. The selected AP(s) will immediately scan for Zigbee devices and the new Discovery Interval will take effect.

Select an AP Group(s) and click on the Zigbee Discovery button. If the selected group’s IoT Radio mode is not Zigbee or the Device Discovery switch is OFF, it can’t apply this function to APs in this group.



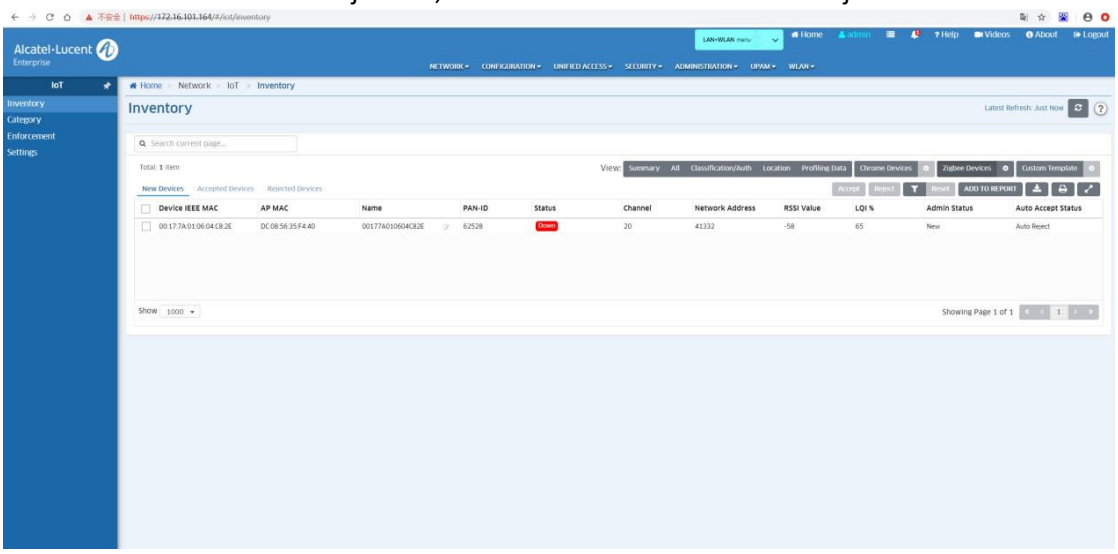
Click “View ZigBee End Points Discovered”. The page will jump to Inventory-Zigbee Devices-New Devices.



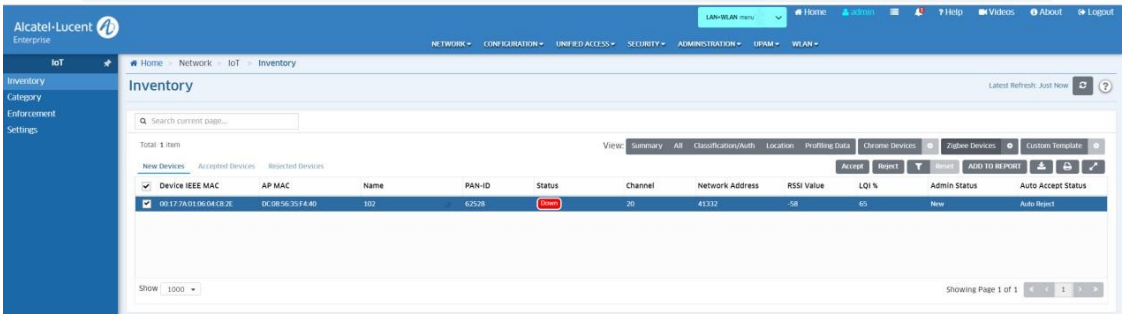
5.50.4 Lock managed by OV

Go to "NETWORK-->IoT-->Inventory-->Zigbee Devices", the Lock info as shown:

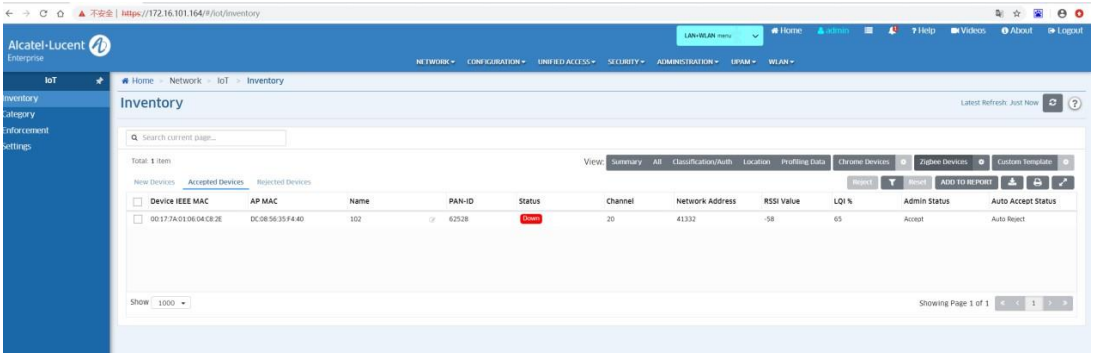
- At first time the Lock join AP, the Status of Lock will be Auto Reject.



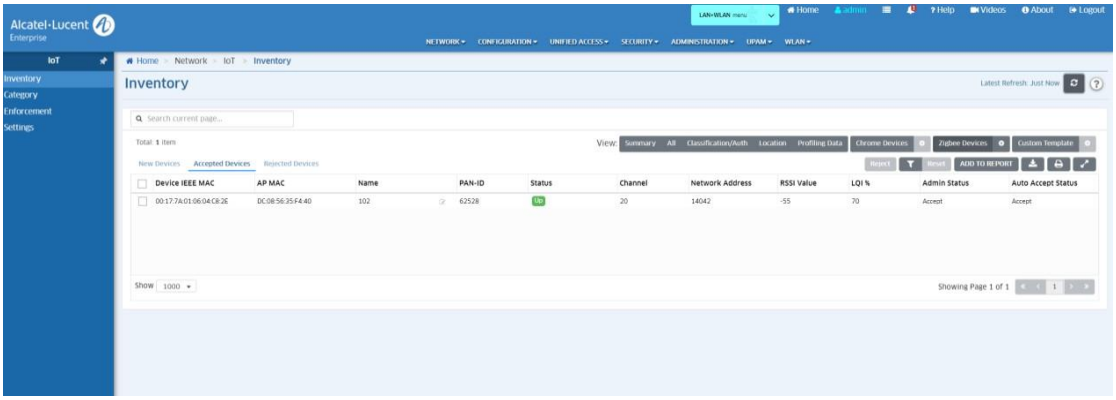
- Rename the lock name , if not do that we can' t accept it (e.g., Room 101)



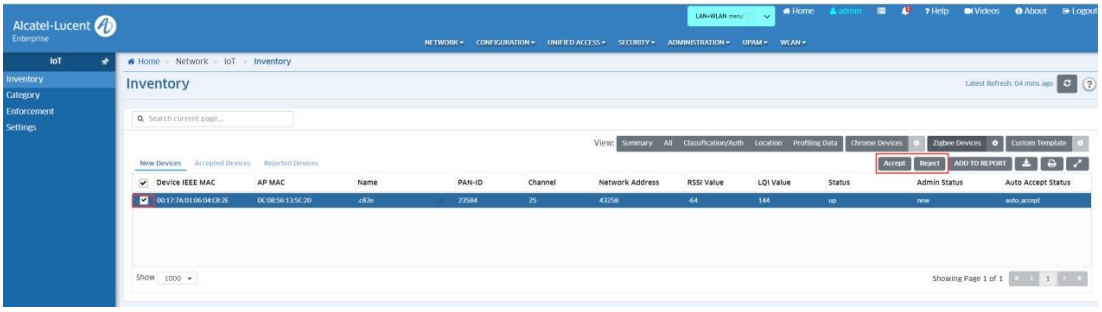
- Accept the lock



- Open Zigbee network and use Discovery Card, Lock re-join AP. This time it will be up

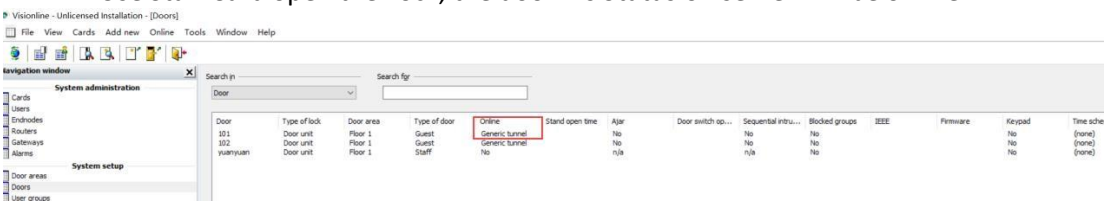


- we can also reject the lock

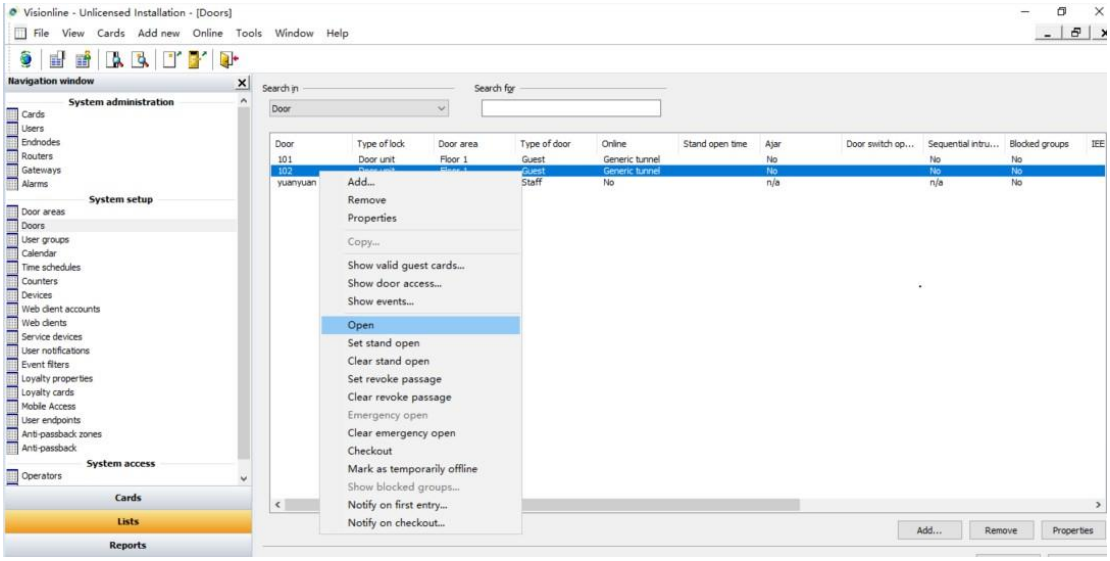


5.50.5 Open the door via Visionline Server

- Use Staff Card open the Lock, the door’s Status on server will be online



- Open the door through Visionline Server, the lock will be opened



5.51 Allow Reflexive policies on AP

5.51.1 Function description

Simplify Policy configuration in OV for Stellar WIFI Policies.

Example of true reflexive policy:

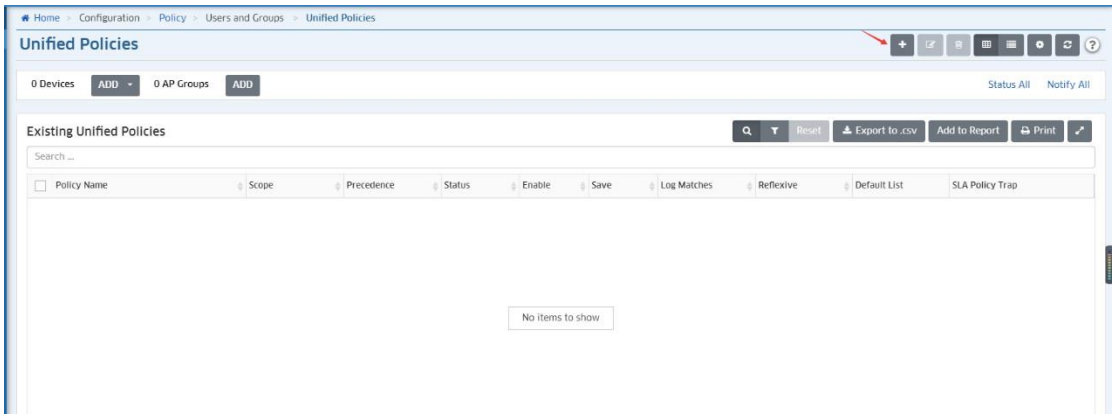
- One Deny All default policy
- One policy to allow destination TCP port 22
- When a client IP1 established a TCP session with src port xxxx to IP2 dst port 22; with reflexive (stateful) policy both "Source IP1, Source TCP Port xxxx, Destination IP2, Destination TCP port 22" and the reverse flow traffic "Source IP2, Source TCP Port 22, Destination IP1, Destination TCP port xxxx" is also allowed. All other traffic is dropped.

There are 3 options for reflexive, namely: Ignore/Yes/No ((Default = Ignore.)

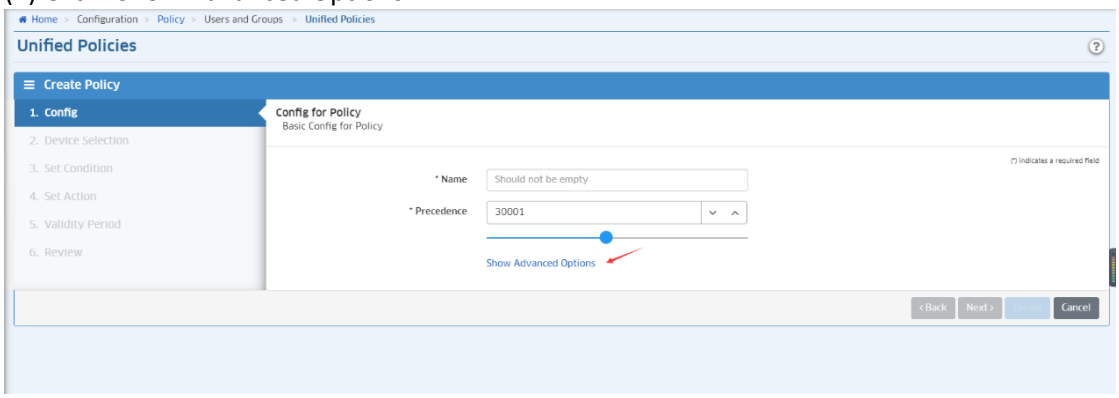
- When reflexive = Ignore, AP will set it to "Yes" state (=Reflexive policy).
- When reflexive = Yes, AP will set it to "Yes" state (=Reflexive policy).
- When reflexive = No, APs will set it to "No" (=Non Reflexive policy). If Reflexive=No, the policy will be stateless rule. In this case, the iptable rule has to be marked with --NOTRACK.

5.51.2 Configuration

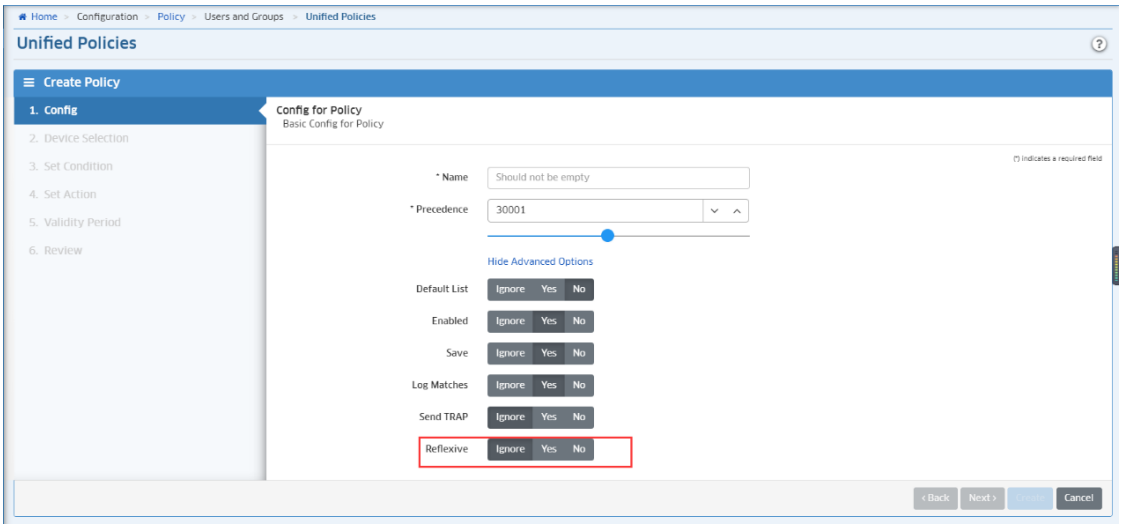
(1) Go to the "Home->Configuration->Policy->Users and Groups->Unified Policies" page, click the "+" button to create a policy, as shown in the figure below:



(2) Click "Show Advanced Options"



(3) You can see the "Reflexive" option, as shown below:



5.51.3 Attention

If some traffic matches NOTRACK rule, then function depends on conntrack will not work.
For example, DPI depends on first 15 packets of the same conntrack session, it might not work if the traffic matches --NOTRACK policy.

5.52 mDNS Self Service

5.52.1 Function description

In 4.5R2, we are introducing new feature mDNS policy, which is applicable in OV mode and not enable by default. So in Cluster mode and in (OV mode without mDNS policy enabled - no responder is configured), the mDNS packets will be forwarded as common multicast and the mDNS service is general without any strict policy control. If the mDNS policy is enabled (mDNS responder configured), the user device sharing should be controlled by mDNS policy configured on OV, if no policy control is configured, the user equipment cannot match the policy, and the mDNS service cannot be discovered.
The main implementation of ALE mDNS service network:
Responder Devices relay mDNS messages and enable the discovery of services across VLANs; and also enables you to configure and apply rules and policies to the data traffic, thereby achieving policy based service sharing.
OV_UPAM provide a BYOD Self Server for authenticated users to list the User Name AND/OR MAC-Addresses with whom service is being shared. Use cases:
Ex.Student A has a printer and apple TV; He wants to share the printer with Student B and not the apple TV
Ex. Student A has a printer and apple TV; He wants to share the printer and apple TV with Student B and Student C
Ex. Student A has a printer and apple TV; He wants to share the printer with Student B and Student C laptop ONLY
Note: It is clear that users can find out the IP address of the mDNS service client and get access directly.

5.52.2 Configuration

(1) The version of the switch supporting mDNS must be above 8.7.70.R01.
Telnet to the 6860 switch, use the "show system" command to view.
Take the 6860 switch as an example:

```
-> show system
System:
  Description:  Alcatel-Lucent Enterprise OS6860E-48 8.7.169.R01 Development, May 28, 2020.,
  Object ID:    1.3.6.1.4.1.6486.801.1.1.2.1.11.1.7,
  Up Time:      8 days 20 hours 18 minutes and 50 seconds,
  Contact:      Alcatel-Lucent Enterprise, https://www.al-enterprise.com,
  Name:         OS6860,
  Location:     Unknown,
  Services:     78,
  Date & Time:  WED JUL 29 2020 06:45:21 (UTC)
Flash Space:
    Primary CMM:
      Available (bytes):  604491776,
      Comments          :  None

->
```

(2) Register the 6860 switch to the OV system. Take the OVE system as an example:

Telnet to connect 6860 switch, execute the following command:

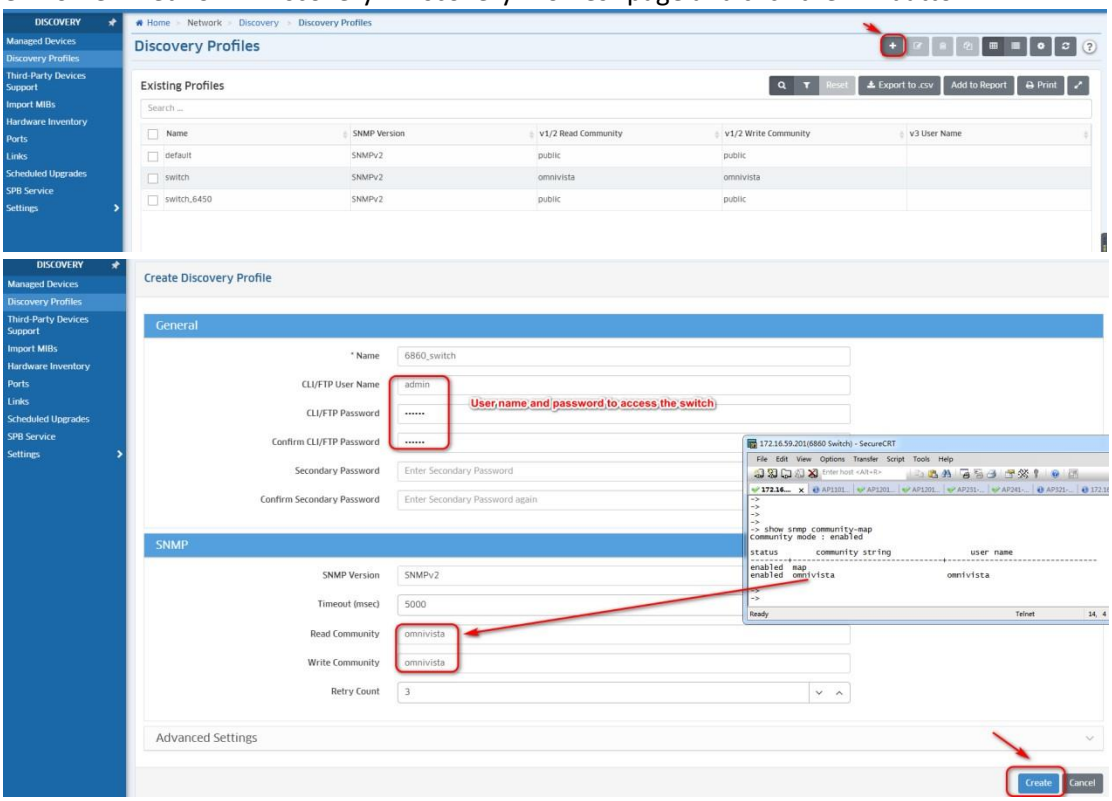
user omnivista password Ss12345$ read-write all no auth

aaa authentication snmp local

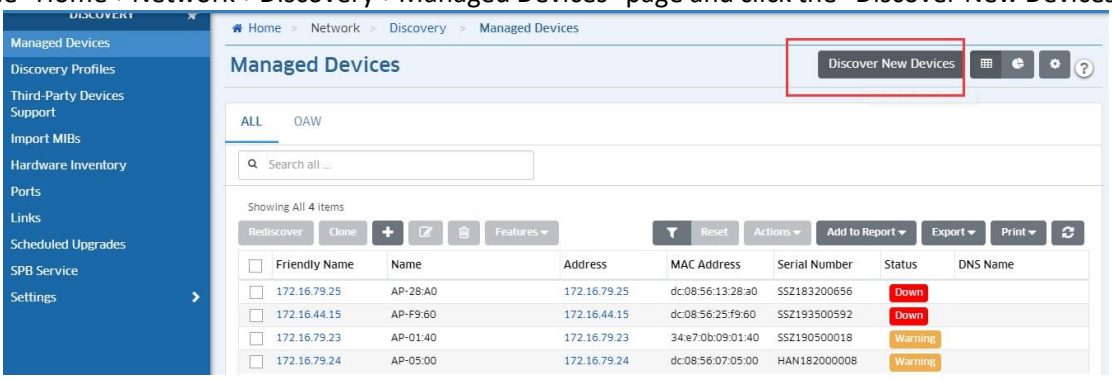
snmp community map public user omnivista enable

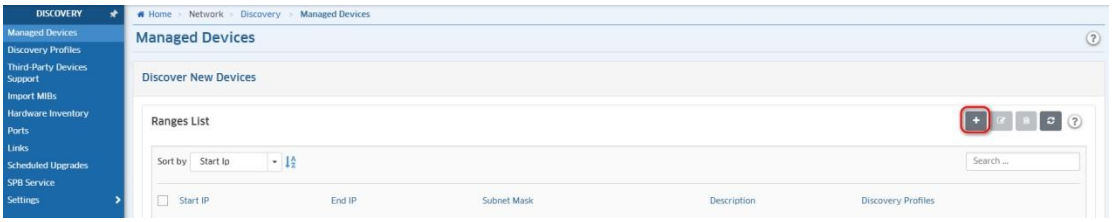
snmp security no

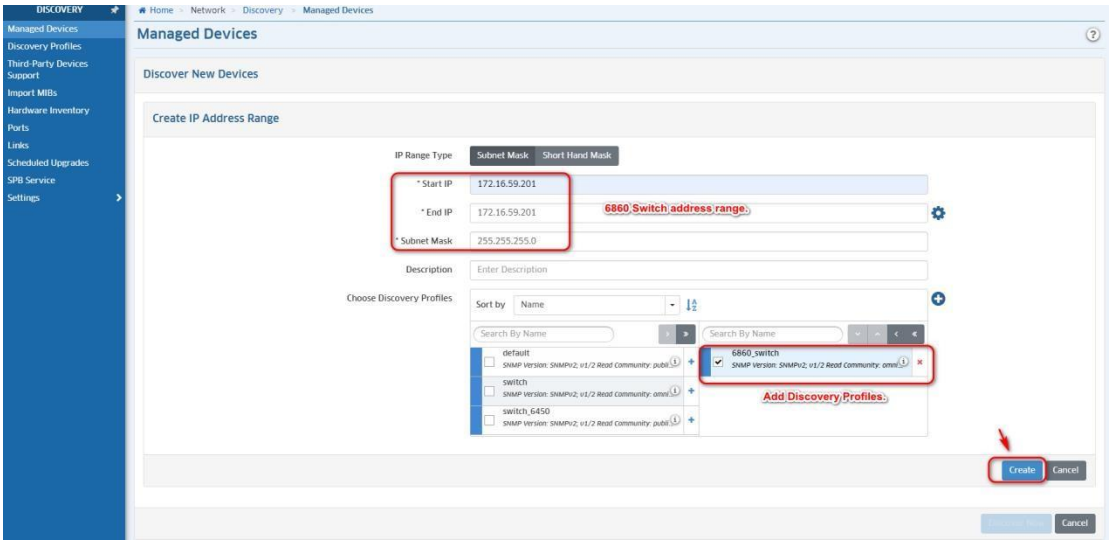
Go to the "Home->Network->Discovery->Discovery Profiles" page and click the "+" button.

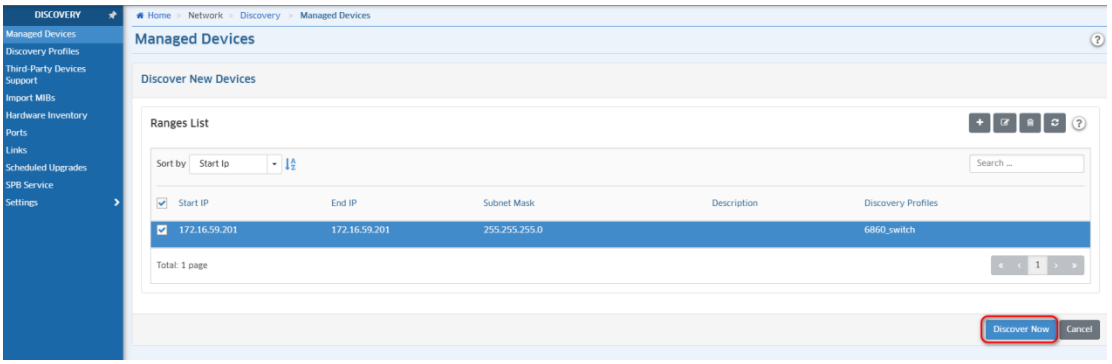


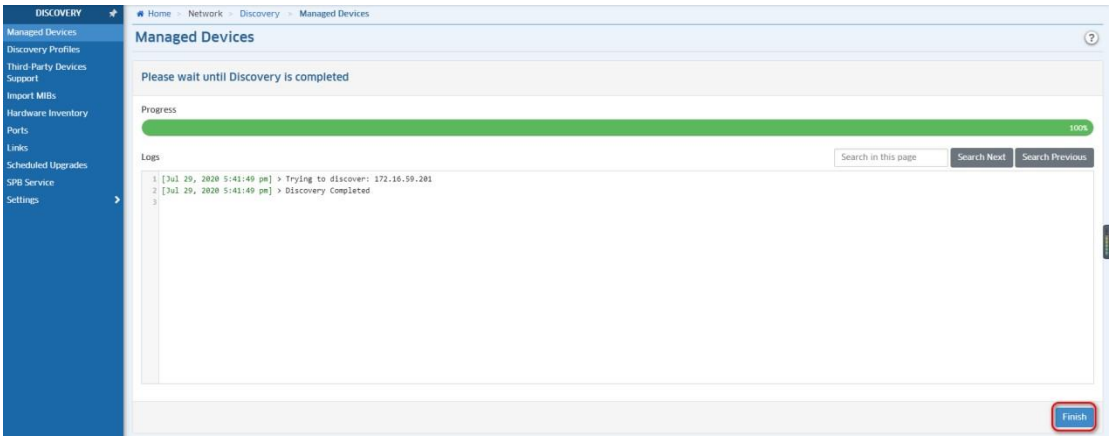
Go to the "Home->Network->Discovery->Managed Devices" page and click the "Discover New Devices" button.

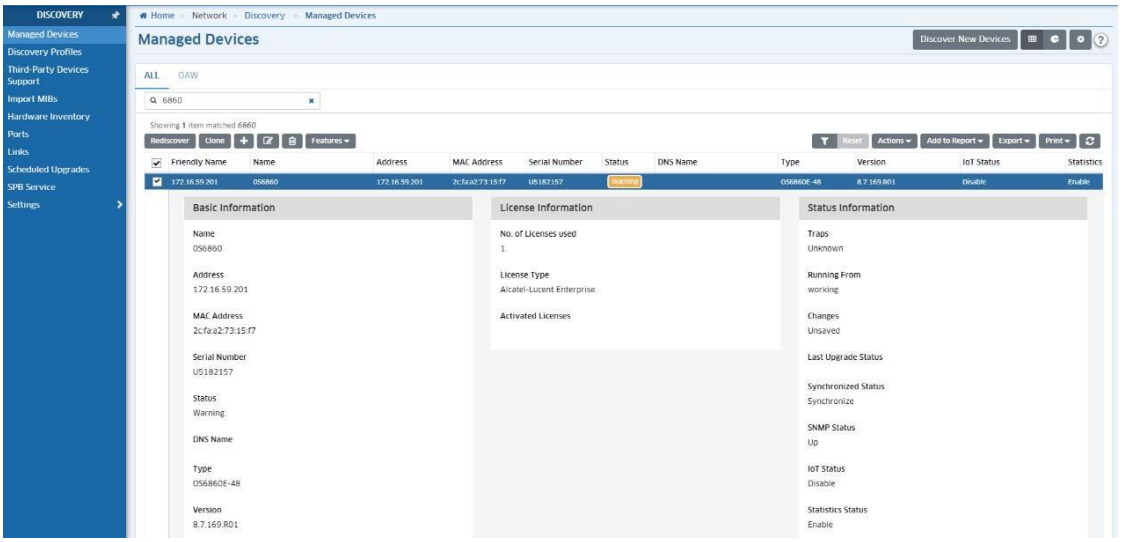



DISCOVERY
Managed Devices
Discovery Profiles
Third-Party Devices Support
Import MIBs
Hardware Inventory
Ports
Links
Scheduled Upgrades
SPB Service
Settings
Home > Network > Discovery > Managed Devices
Managed Devices
Discover New Devices
Ranges List
Sort by Start Ip
Search ...
Start IP
End IP
Subnet Mask
Description
Discovery Profiles


Managed Devices
Discover New Devices
Create IP Address Range
IP Range Type
Subnet Mask
Short Hand Mask
* Start IP
172.16.59.201
* End IP
172.16.59.201
* Subnet Mask
255.255.255.0
6860_Switch address range
Description
Enter Description
Choose Discovery Profiles
Sort by Name
Search By Name
default
switch
switch_6450
6860_switch
Add Discovery Profiles
Create
Cancel

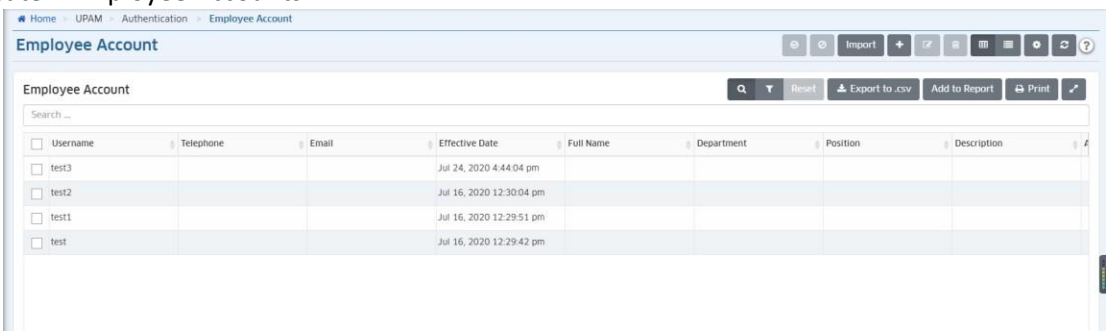

Managed Devices
Discover New Devices
Ranges List
Sort by Start Ip
Search ...
Start IP
End IP
Subnet Mask
Description
Discovery Profiles
172.16.59.201
172.16.59.201
255.255.255.0
6860_switch
Total: 1 page
Discover Now
Cancel


Managed Devices
Please wait until Discovery is completed
Progress
100%
Logs
Search in this page
Search Next
Search Previous
[Jul 29, 2020 5:41:49 pm] > Trying to discover: 172.16.59.201
[Jul 29, 2020 5:41:49 pm] > Discovery Completed
Finish

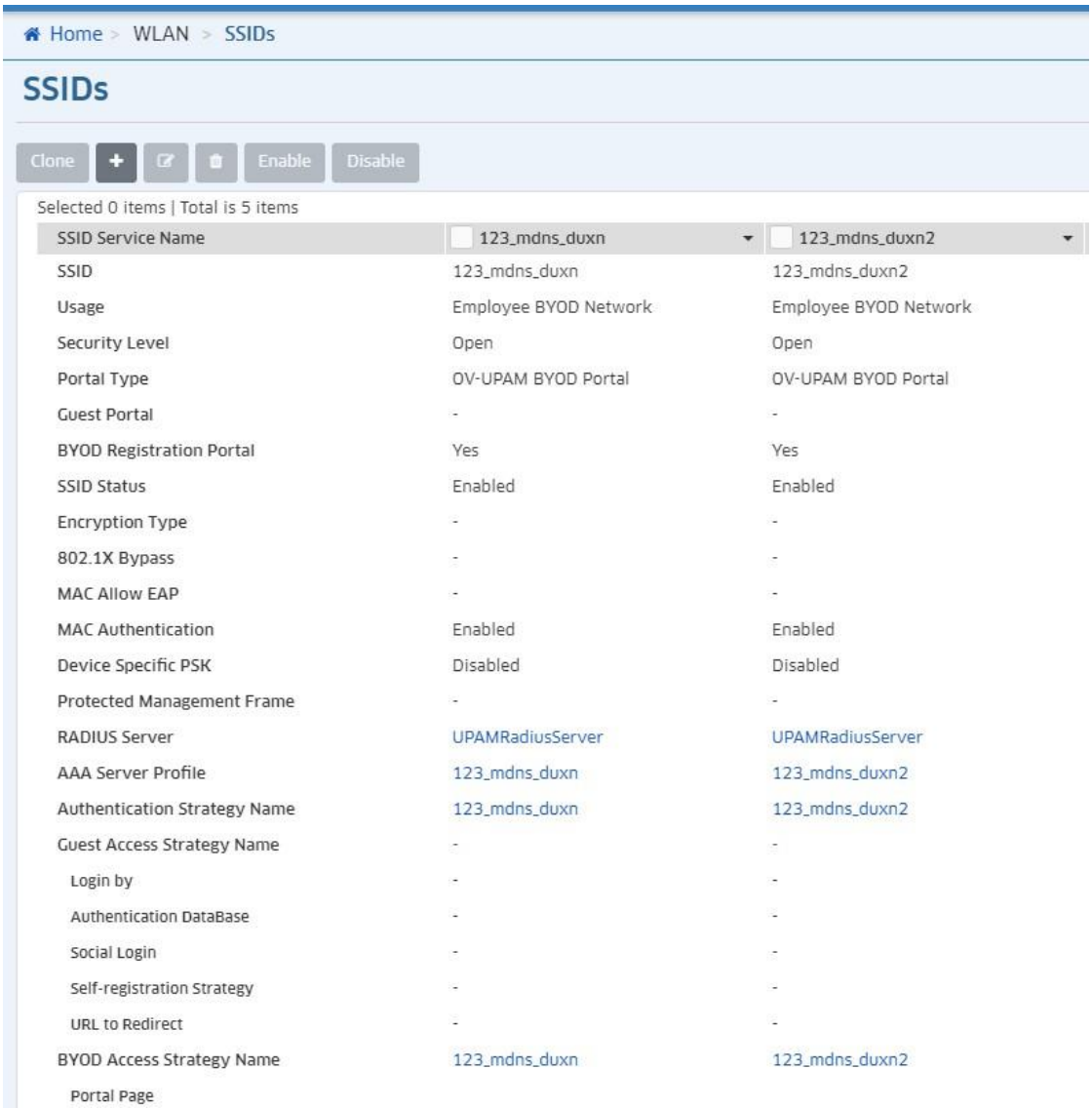


In this way, the 6860 switch was successfully added to OVE.

(3) Create 4 Employee Accounts.



(4) Create two BYOD WLANs and map them to AP Group "123_mdns_duxn" and "123_mdns_duxn2" respectively.

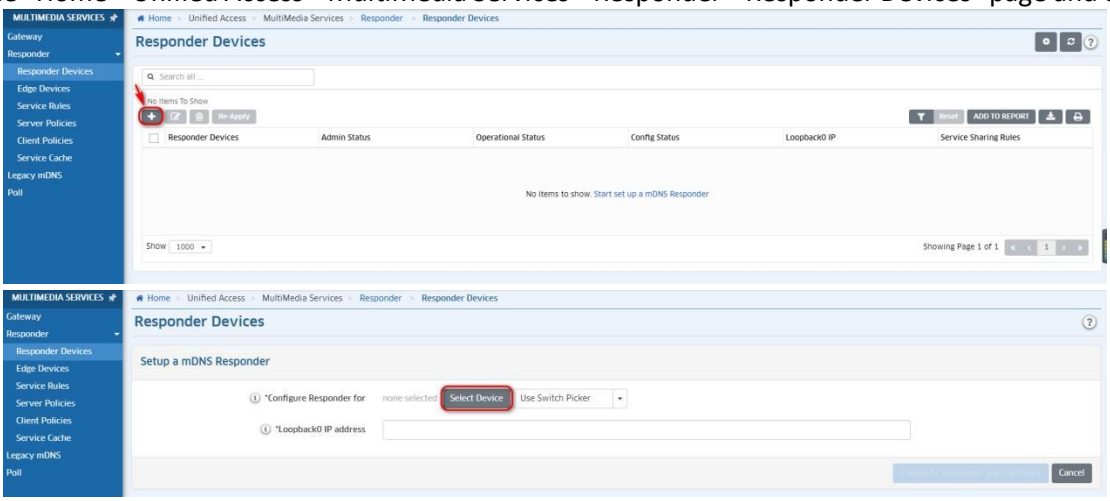


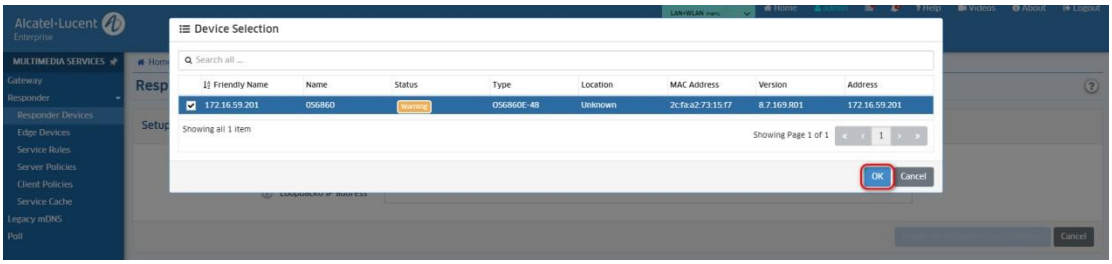
SSID Service Name	123_mdns_duxn	123_mdns_duxn2
SSID	123_mdns_duxn	123_mdns_duxn2
Usage	Employee BYOD Network	Employee BYOD Network
Security Level	Open	Open
Portal Type	OV-UPAM BYOD Portal	OV-UPAM BYOD Portal
Guest Portal	-	-
BYOD Registration Portal	Yes	Yes
SSID Status	Enabled	Enabled
Encryption Type	-	-
802.1X Bypass	-	-
MAC Allow EAP	-	-
MAC Authentication	Enabled	Enabled
Device Specific PSK	Disabled	Disabled
Protected Management Frame	-	-
RADIUS Server	UPAMRadiusServer	UPAMRadiusServer
AAA Server Profile	123_mdns_duxn	123_mdns_duxn2
Authentication Strategy Name	123_mdns_duxn	123_mdns_duxn2
Guest Access Strategy Name	-	-
Login by	-	-
Authentication DataBase	-	-
Social Login	-	-
Self-registration Strategy	-	-
URL to Redirect	-	-
BYOD Access Strategy Name	123_mdns_duxn	123_mdns_duxn2
Portal Page		

The above preparations are complete.

(5) Configure the 6860 switch as a responder.

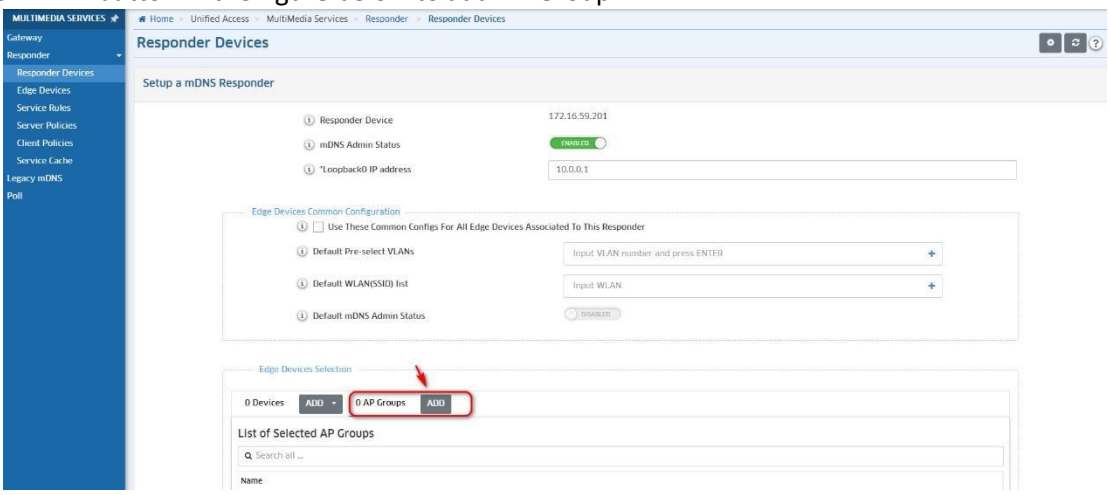
Go to the "Home->Unified Access->MultiMedia Services->Responder->Responder Devices" page and click the "+" button.

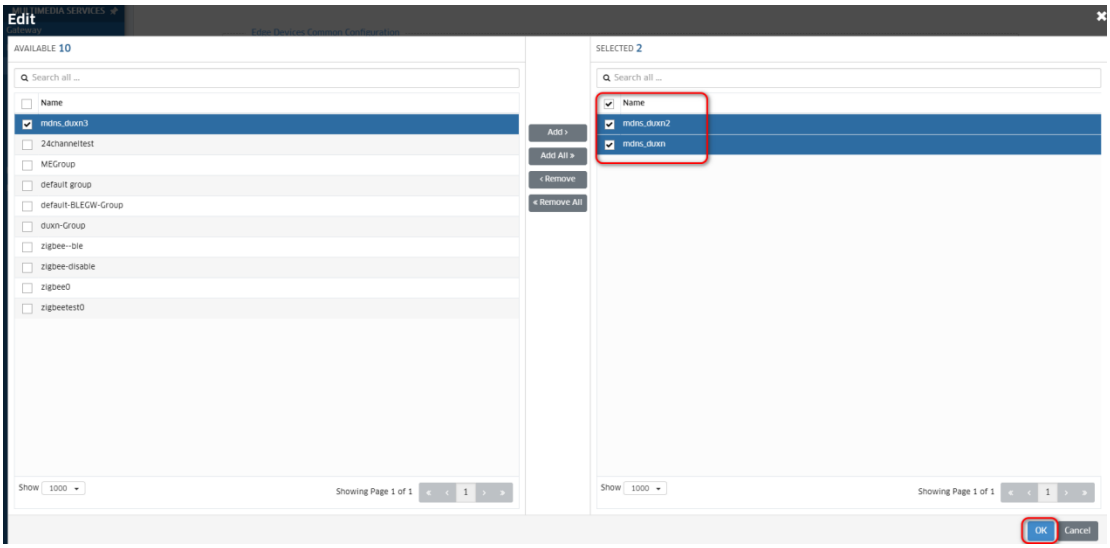


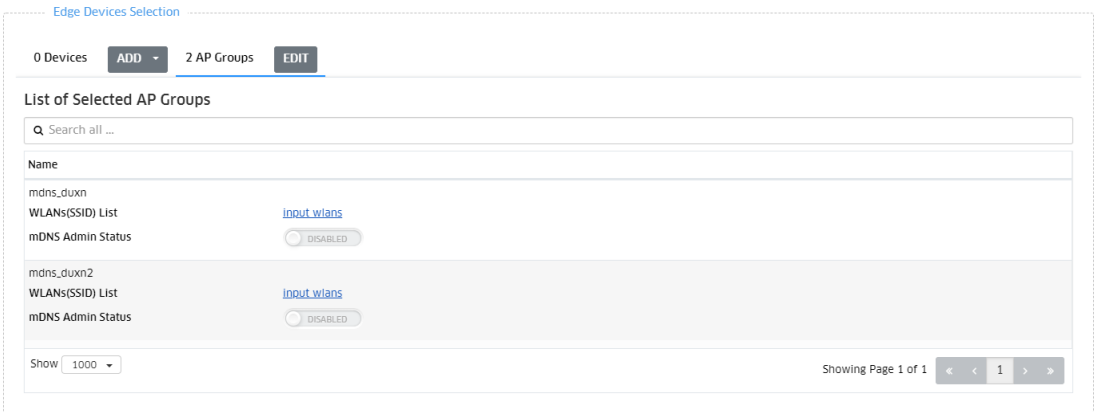


(6) Add AP Group to edge device mode.

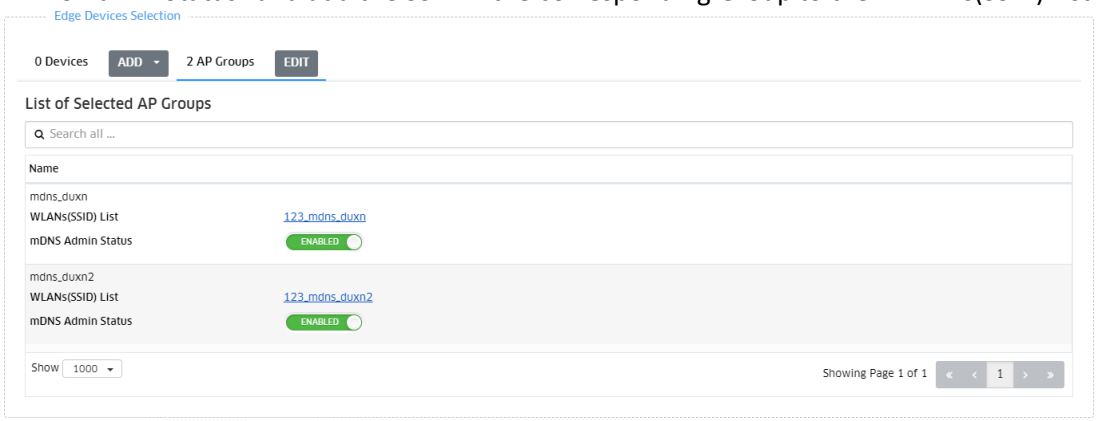
Click the "ADD" button in the figure below to add AP Group.





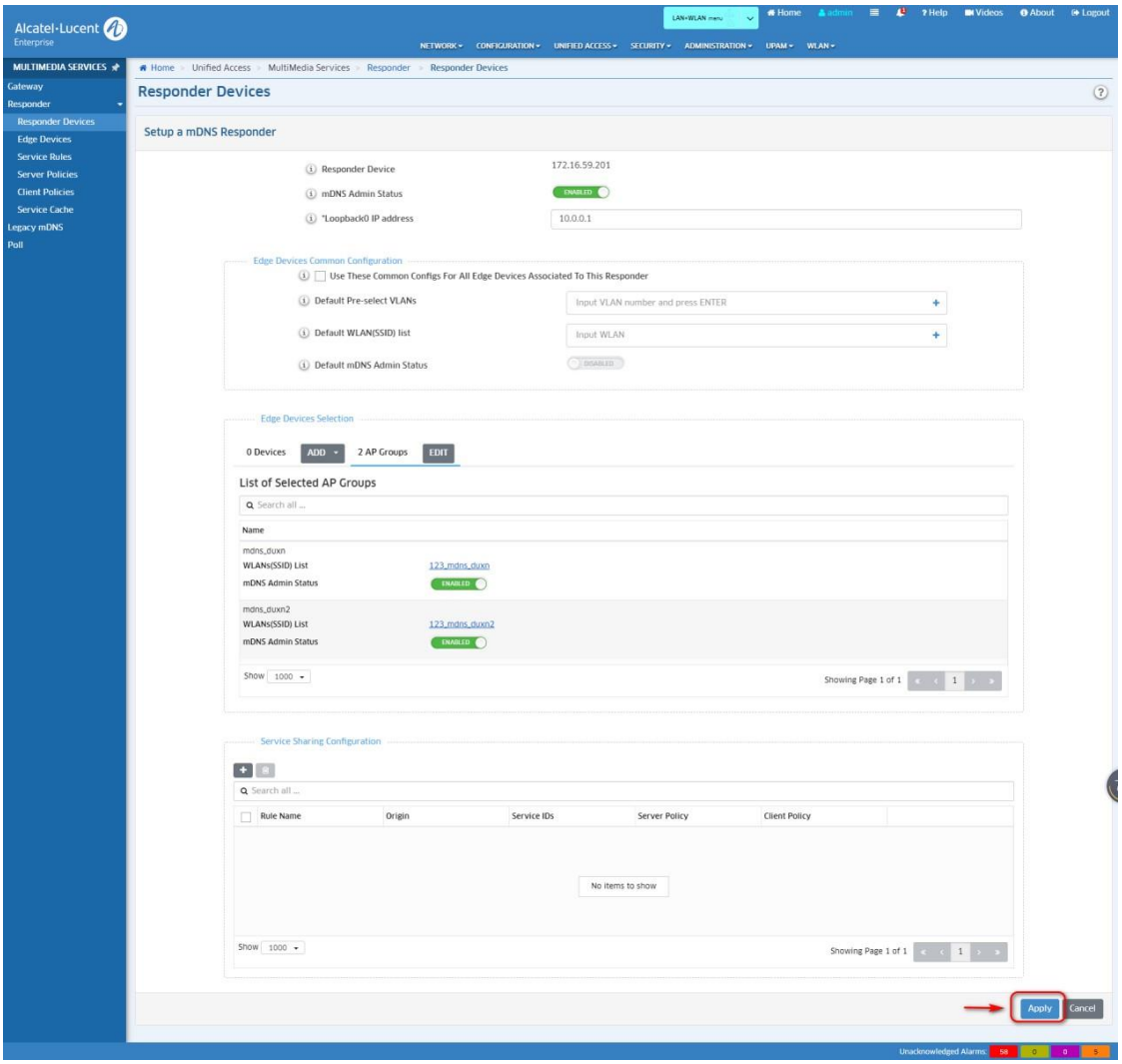


Enable "mDNS Admin Status" and add the SSID in the corresponding Group to the "WLANs(SSID) List" as follows:



Note: We support mDNS client and mDNS server to connect to different APs; of course, mDNS client and mDNS server can also connect to different SSIDs and can cross different VLAN IDs, but the prerequisites are: The WLAN accessed by the mDNS client and mDNS server must be added to the mDNS SSID List.

After the above operations are completed, click the "Apply" button to apply it to the switch and AP group, as shown below.



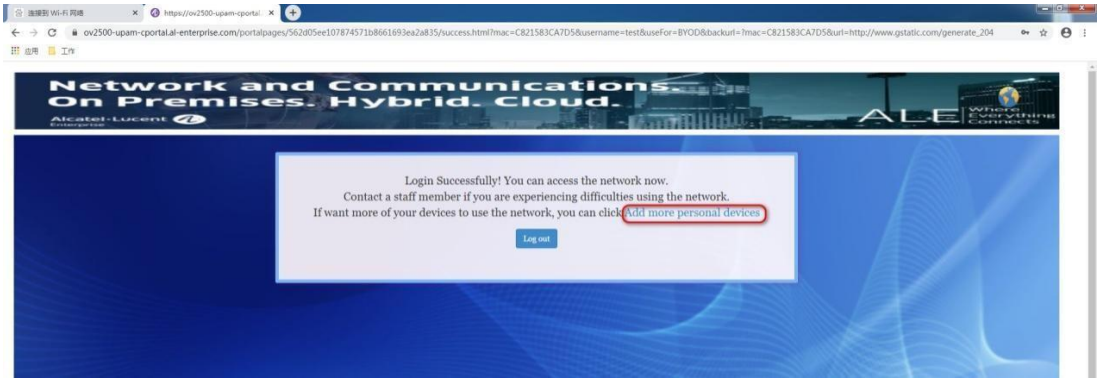
(7) User use.

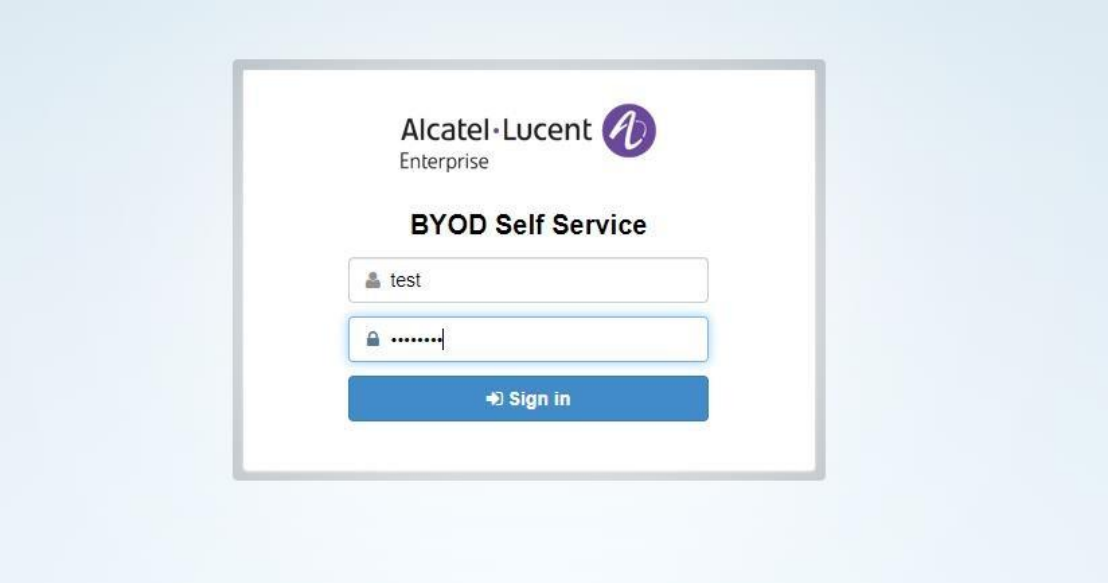
Take BYOD Self Server provided by OV_UPAM as an example:

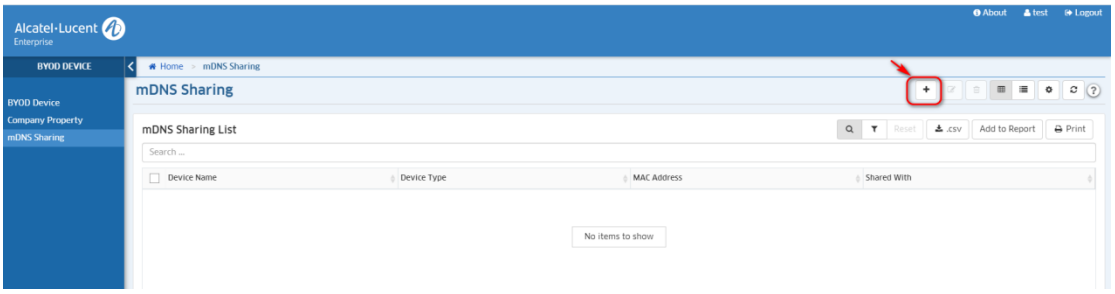
Of course, OV also supports Service Rules, containing Server Policies and Client Policies define the criteria by which the Responder Device determines which services can be shared with which client requests. It is not explained here.

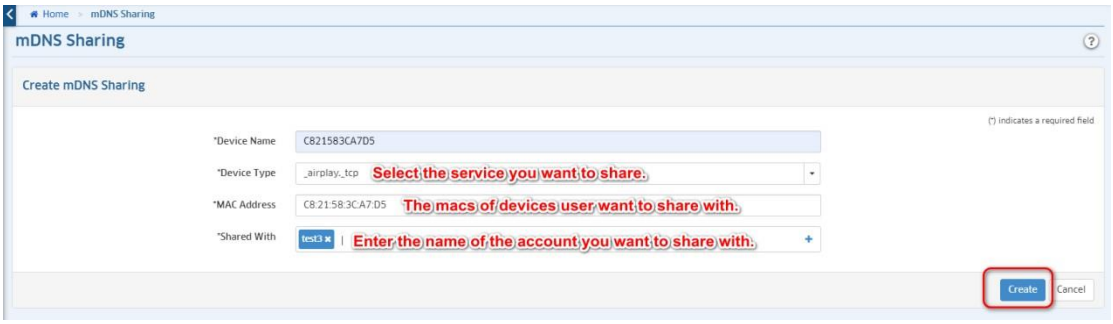
Server device BYOD Self Service Configuration. The server device accesses the "123_mdns_duxn" WLAN and uses the "test" account for BYOD authentication.

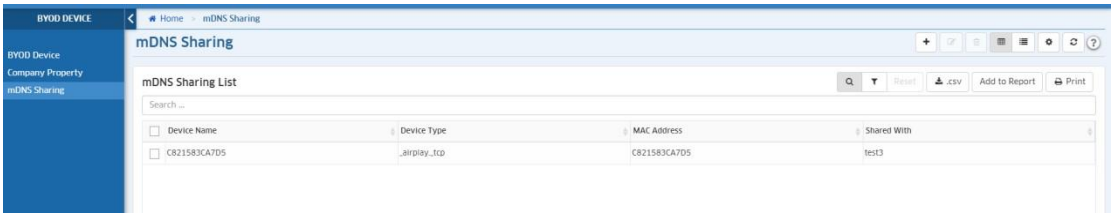
After passing BYOD authentication, you can click the "Add more personal devices" link to jump to BYOD Self Server and add mDNS sharing rules.







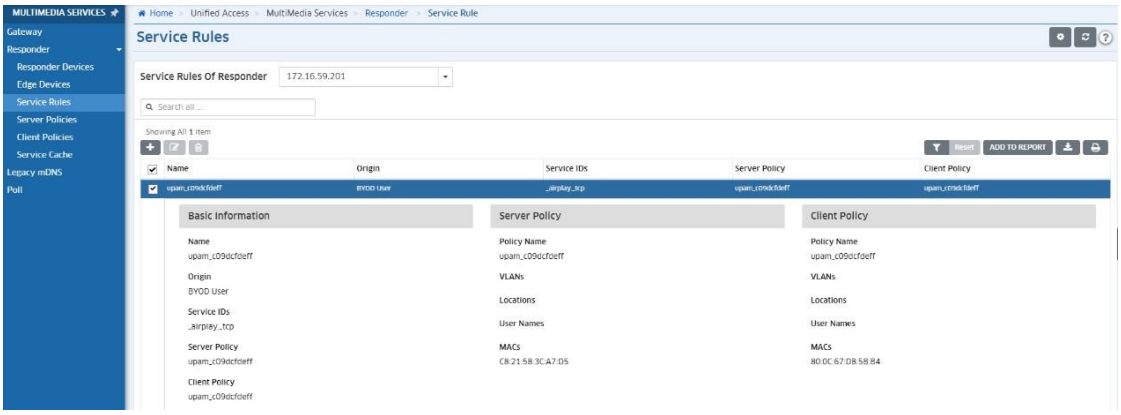




Client device configuration.

① The client device (iPhone 11) connects to the "123_mdns_duxn2" WLAN and uses the "test3" account for BYOD authentication.

Rules are automatically generated on the OV page, as follows:



>>> Result: iPhone 11 can discover the airplay service shared by the server and can use it.

② The client device (iPhone 7) connects to the "123_mdns_duxn2" WLAN, and uses the "test2" account for BYOD authentication.

>>> Result: iPhone 7 cannot find the airplay service shared by the server.

5.52.3 Attention

AWOS 4.0.1 version does not support the forwarding of wired mDNS messages, it can only work in WLAN.
AP1101 does not support the mDNS function. If you want the mDNS function to take effect, please use other APs models.
Only limited to BYOD certification and Employee Account.
Shared account must have online or remembered information
If the shared account is neither online nor remembered, UPAM will not send a synchronization notification to OV. Therefore, do not configure "disable remembered" as much as possible.
After the shared account is disabled and then enabled, it must be re-authenticated
If the shared account is disabled and then enabled, remembered will be deleted. At this time, the shared account is neither online nor remembered, and the previously created mDNS rules cannot be edited. Therefore, the shared account needs to be authenticated again.
After the user's first BYOD authentication, it is recommended that the user record the URL for accessing BYOD Self Server. Because in the implementation of the first stage, BYOD Self Server does not have a good entry point, if users want to add, delete, modify, and check mDNS sharing rules in the future, must use the URL passed in BYOD Access Strategy. Only then can you access the BYOD Self Server login page.

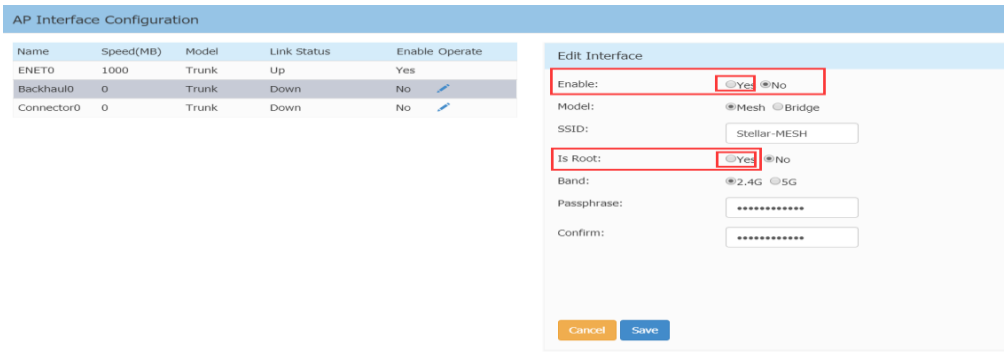
5.53 Deliver Out of the Box MESH

5.53.1 Function description

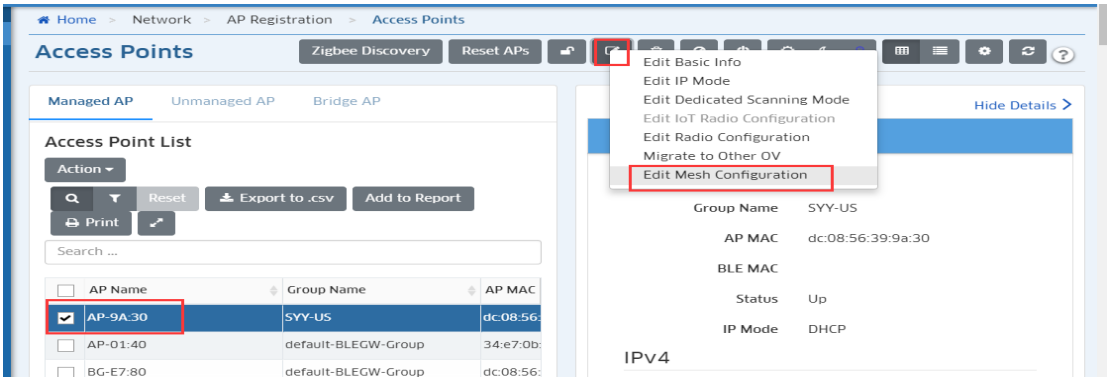
The mesh function has been supported in the previous project, but the MESH configuration is very cumbersome. The administrator must configure each AP one by one from the AP-UI (specify the MESH SSID, Band, Passphrase) for configuration. Out-of-the- box Mesh is a feature that helps you quickly set up a Mesh Network without configuring the out-of-box APs. The out-of-box APs will establish a Mesh network with hardcoded settings. You only need to specify the MESH root, then other APs will establish a Mesh configuration automatically. Support all AP models except Bluetooth devices. If your AP is upgraded from 4.0.0.x to 4.0.1.x, you should reset the AP.

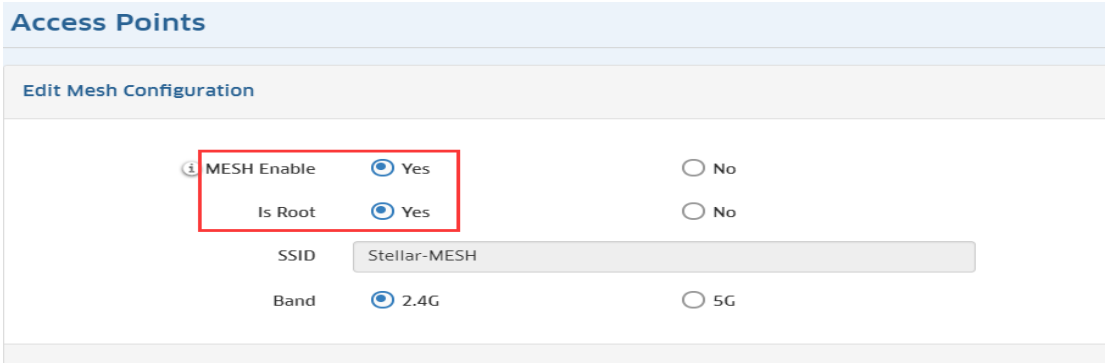
5.53.2 Configuration

Make sure the AP is factory configuration to perform Deliver Out of the Box MESH connection
Keep one of the AP (no matter the ap models) connect to LAN. If the AP works in cluster mode, user need login the AP UI and enable mesh and set to root AP, shown as below picture



If AP works in OV mode, user just need login the access point page, select an AP (no matter the ap models) in the Access Points List and click the edit button then select Edit Mesh Configuration. For the Mesh Enable field, select the "Yes" radio button, then for the Is Root field, select the "Yes" radio button, shown as below pictures



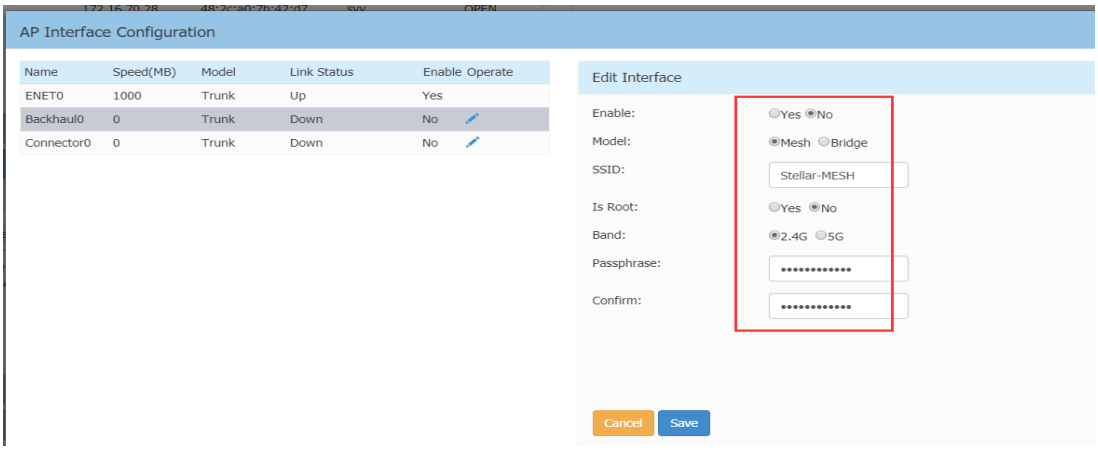


Attentions: If user want to change band from 2.4G to 5G or change other values, the option should begin from the last leaf AP, otherwise, if user change root AP firstly, the non-root AP will lose management and the modification fails.

As for non-root AP, we only need to supply power to the AP with power adaptor.

Attentions: As for PoE Adaptor, we test only three models AFI-POE20-480032A and GM-480040, GM-480040 (shown as the below pictures). In theory, other models of power adaptor will not have problems. If there is a problem, you can create a BUG, and our team will analyze and solve it.

The default model of the Deliver Out of the Box MESH is mesh and works in 2.4G band, if user want to change the work band in OV mode mesh, user can modify the value as pic3.3, if user want to change the other parameter values such as SSID ,password, work mode, please modify in the AP UI page (both cluster and OVE), shown as below picture



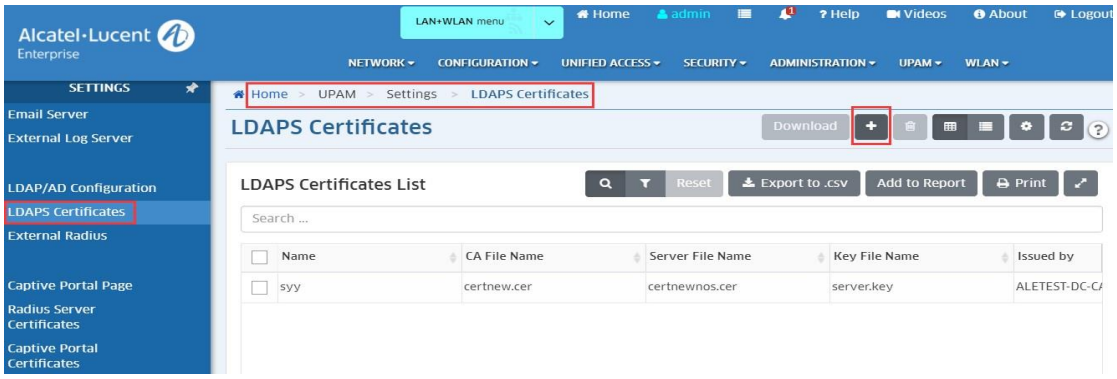
5.54 LDAP over SSL

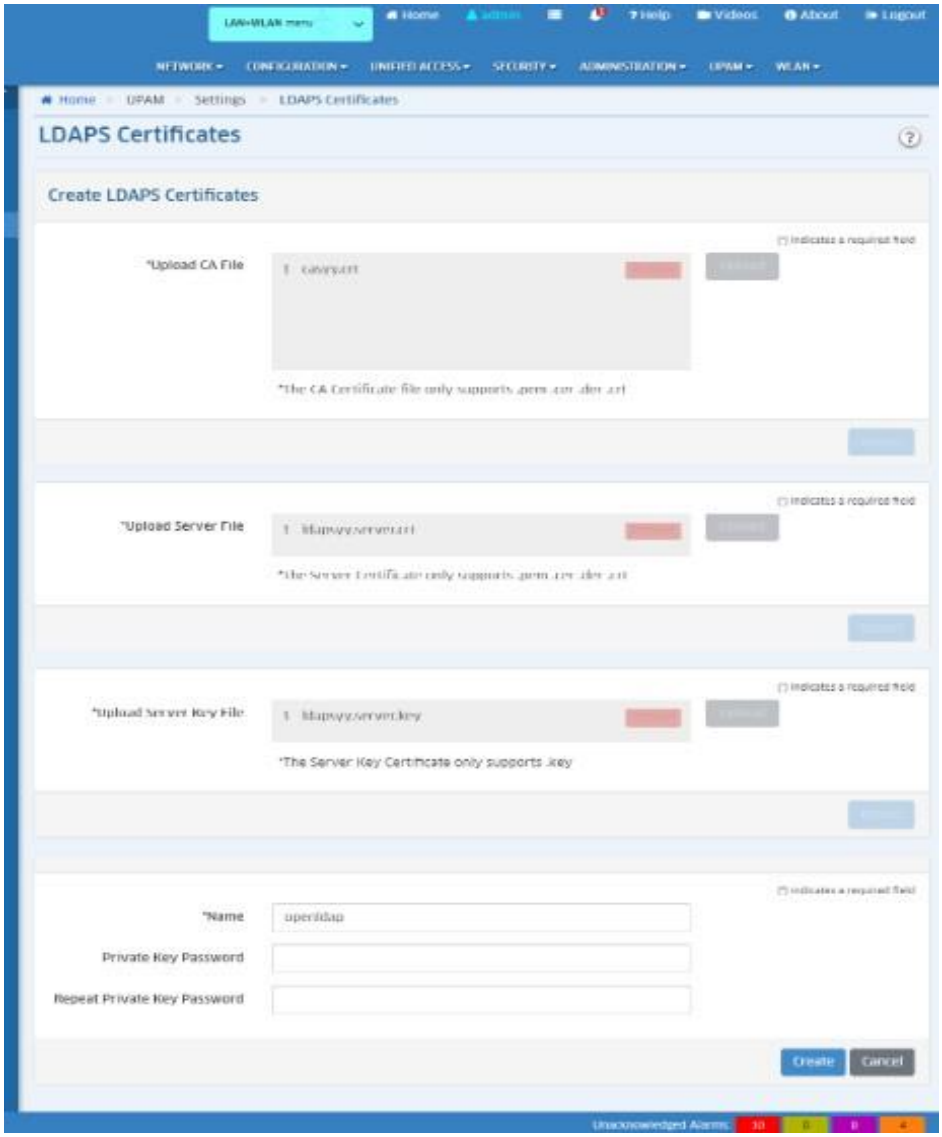
5.54.1 Function description

UPAM application acts as proxy for authenticating clients against LDAP server and against Active Directory (AD). Currently the protocol used by UPAM for authentication with LDAP server and for authorization during AD role-mapping is LDAP which is not secure, so we support LDAPS for secure authentication against LDAP server and support LDAPS for secure authorization when performing client role-mapping against AD server. Now we only support 802.1x/BYOD authentication via UPAM with OVE mode not support OVC mode.

5.54.2 Configuration

1. Upload LDAPS Certificates profiles following below pictures including CA Certificates, Server Certificates and Server Key Certificates.

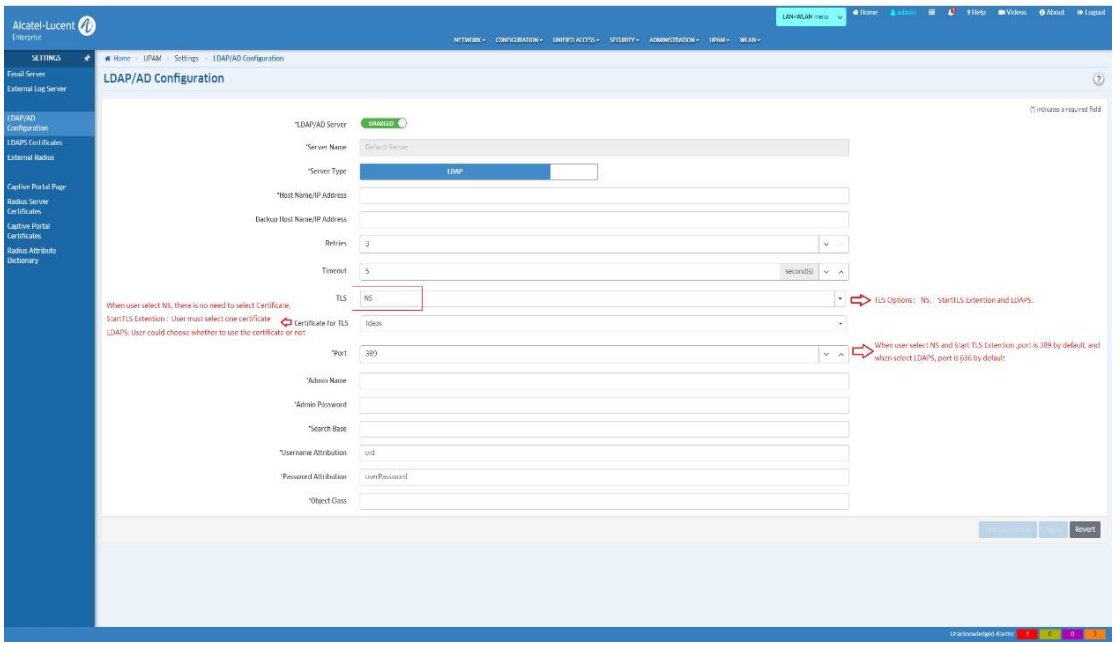




If user want delete the certificates profile, make sure the profile is not in use.

2. LDAP/AD Configuration

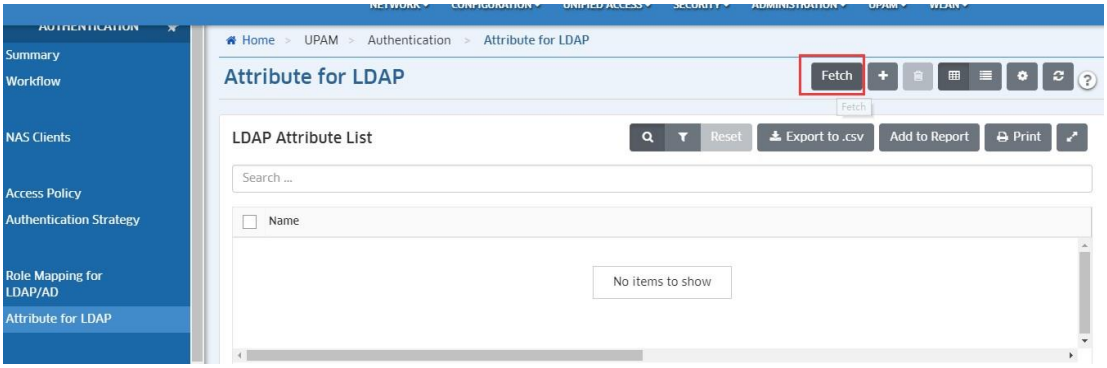
Most of the parameter settings are still the same as before, only the value of new button should be attention (shown as below picture).



- Host Name/IP Address: when user select certificates profile the value should be FQDN
- TLS: There are three options to be choose.
  - NS - Non-secure encryption between UPAM and the LDAP Server.
  - LDAPS - Use LDAPS protocol as the secure communication method between UPAM and the LDAP Server.
  - Start TLS Extension - Use Start TLS Extension mechanism as the secure communication method between UPAM and the LDAP Server
- Certificate for TLS: Select an LDAP Certificate from the drop-down. You can also click on the "Add New" link to go to the LDAPS Certificate Screen and create a new certificate, then select the certificate profile.
- Port: When user select NS or Start TLS Extension, the default port is 389, when user select LDAPS, the default port is 636

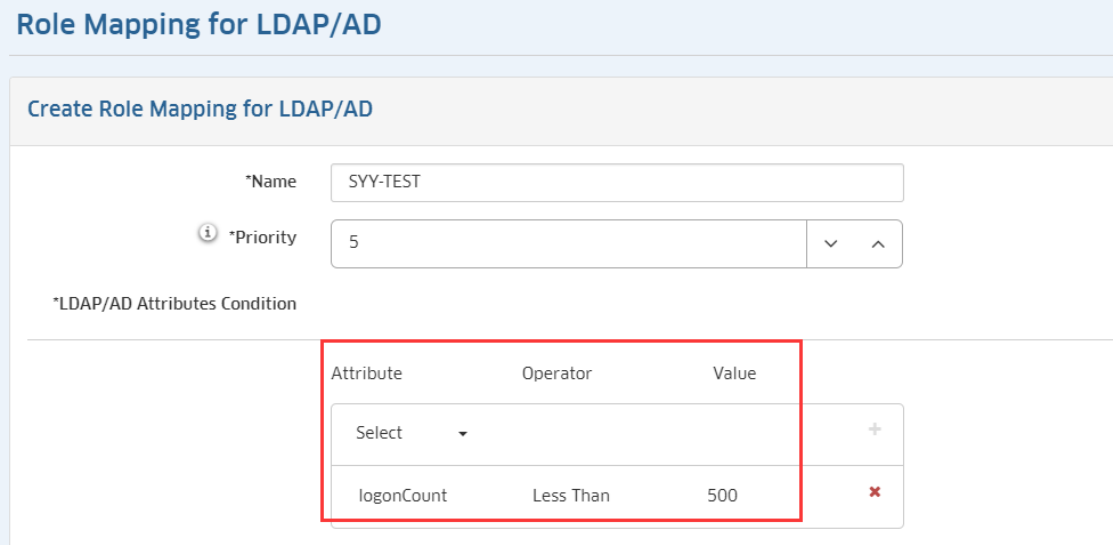
3. Attribute for LDAP

User can select fetch or add to get attribute (shown as below picture)



4. Role Mapping for LDAP/AD

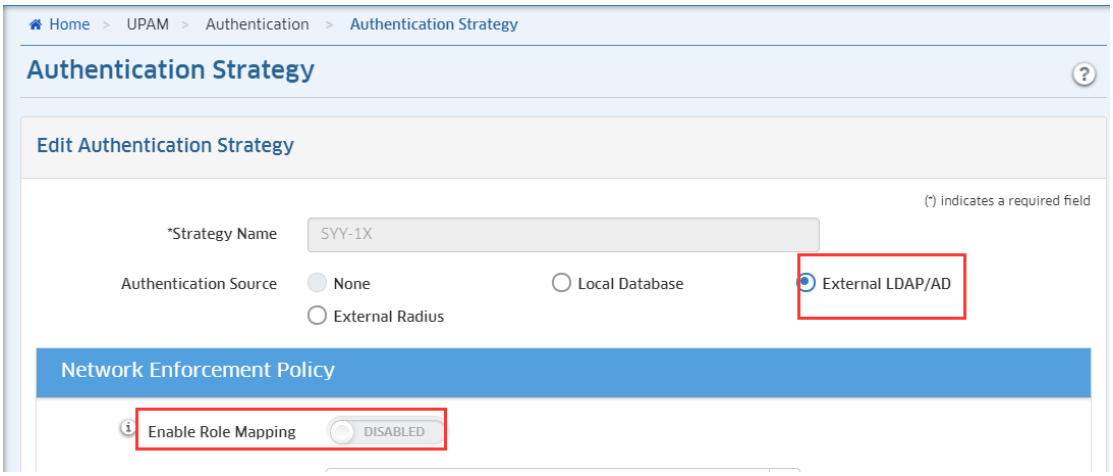
For role mapping configuration, user can set condition follow he wants. Such as below picture



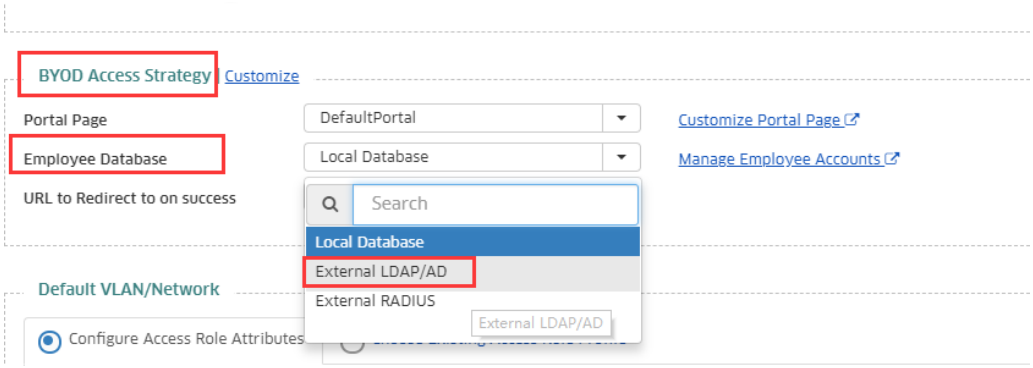
5.WLAN configurations

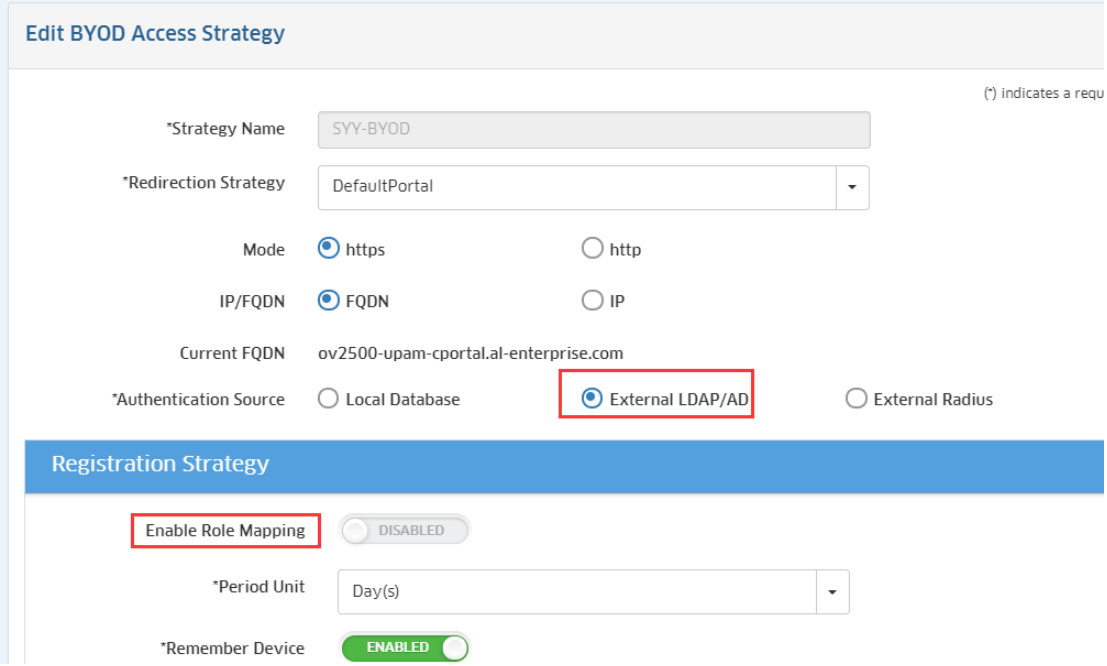
Now we only support 802.1x/BYOD authentication via UPAM

For WLAN with 802.1X, in auth strategy user should select External LDAP/AD. If want use role mapping, please enable role mapping follow below picture)



For WLAN with BYOD, user should select External LDAP/AD as Employee Database value when create WLAN by SSIDS (shown as the below picture) or modify in the BYOD access strategy page (shown as below picture). If want enable role mapping user can enable as the picture (shown as below picture).





5.55 Stellar AP as 802.1x client

5.55.1 Function description

As of AWOS 4.0.4/ OV 4.6R02/OVC 4.6.2 Stellar AP can authenticate over 802.1x UPAM Radius Server or other 3rd Party Radius Server.

By default, the 802.1X Client function is disabled, and APs can register to OV without 1X wired authentication, for example by using default built-in profile defaultWLANProfile on OmniSwitches that is classifying based on LLDP capabilities sent by Stellar AP. After all relevant 1X configurations are configured on OV, the 1X authentication port on the switch will be opened. After the AP restarts, as a client for wired 1X authentication, use the process wpa_supplicant to perform 802.1X EAP-TLS authentication.

If NAS Client is an OmniSwitch, the AOS minimum version must be AOS 6.7.2R08 Build 160 / AOS 8.8R01 GA with the support of AP “secure” mode.

Behavior if “secure” ap-mode is enabled on OmniSwitch:

unp port would be deemed ap-detected port, and accordingly implicit trust-tag enabled, only when AP is 1x-authenticated on the port. However, if AP is learnt in forwarding by any means other than 1x-auth, the implicit trust-tag will NOT be enabled, and any AP-Clients on that port will have to still undergo learning based on existing unp-port config (i.e; NOT through implicit trust-tag).

5.55.2 Feature limitations

Limitations:

- AOS 6.x does not support untagged VLAN from SSID if AP is connected in secure mode
- Stellar OAW-AP1101 does not support this feature

<u>AOS 6.x configuration sample</u>

```
vlan port mobile 1/1
vlan port 1/1 802.1x enable
```

```
! AAA :
aaa radius-server "UPAMRadiusServer" host 10.130.7.17 hash-key xx retransmit 2 timeout 5 auth-port
1812 acct-port 1813
aaa authentication 802.1x "UPAMRadiusServer"
aaa accounting 802.1x  "UPAMRadiusServer"
aaa user-network-profile name "AP-Secured-UNP" vlan 80 hic disable
aaa user-network-profile name "defaultWLANProfile" vlan 1307 hic disable
! 802.1x :
802.1x 1/1 direction both port-control auto quiet-period 60 tx-period 30 supp-timeout 30 server-
timeout 30 max-req 2 re-authperiod 3600 no reauthenticatione
802.1x 1/1 ap-mode enable secure enable
802.1x 1/1 supplicant policy authentication pass block fail block
802.1x 1/1 non-supplicant policy group-mobility block

-> show 802.1x users

Slot         MAC             Port        Classification                    Auth
   Auth         Last Successful              User
Port       Address           State           Policy                    Failure
Reason               Retry Count        Auth Time                  Name
-----------+-----------------------------+---------------------------+-------------------------------------+-------------------------------------------------------------
+----------------------+-----------------------------------------------+-----------------------------------
01/01 dc:08:56:1b:c3:b0 Authenticated   Basic-UNP-Auth
Svr                     -                    0           WED DEC 08 10:15:01 2021  DC08561BC3B0
```

AOS 8.x configuration sample:

```
OS6860E_VC_Core -> show configuration snapshot all | grep 1/1/7
unp port 1/1/7 port-type bridge
unp port 1/1/7 redirect-port-bounce direction both default-profile "defaultWLANProfile"
classification trust-tag ap-mode secure dynamic-service none
unp port 1/1/7 admin-state enable
unp port 1/1/7 802.1x-authentication
unp port 1/1/7 mac-authentication
```

Below example AP MAC Address dc:08:56:36:17:80 is authenticated in 802.1x over UPAM and associated to VLAN 80, all WLAN Clients (here 7e:23:38:61:3c:9c) classified to same port have VLAN tag trusted (secure mode)

```
OS6860E_VC_Core -> show unp user details port 1/1/7
Port: 1/1/7
    MAC-Address: 7e:23:38:61:3c:9c
…
      Access Timestamp                = 11/24/2021 17:10:59,
      User Name                       = 7e:23:38:61:3c:9c,
      IP-Address                      = 10.130.7.91,
      Vlan                            = 1307,
      Profile Source                  = Trust Tag,
..
      Encap Value                     = 1307,
Port: 1/1/7
    MAC-Address: dc:08:56:36:17:80
…
      User Name                       = DC0856361780,
      IP-Address                      = 192.168.80.20,
      Vlan                            = 80,
      Authentication Type             = 802.1x,
      Authentication Status           = Authenticated,
      Authentication Server IP Used   = 10.130.7.17,
```

```
Authentication Server Used      = UPAMRadiusServer_local,
Server Reply-Message            = -,
Profile                         = AP-Secured-UNP,
Profile Source                  = Auth - Pass - Server UNP,
Profile From Auth Server        = AP-Secured-UNP,
```

5.55.3 How does it work ?

802.1x is disabled by default on AP, this is up to admin to enable the feature on AP Group or per AP level
AP running AWOS 4.0.4 will have a built-in COMMON client certificate based on OVC CA
OVC and OV 2500 UPAM will have a built-in CA to trust Stellar APs
OVC and OV 2500 UPAM will offer ability to import customer CA certificate at AP or AP group level
OVC and OV 2500 UPAM CA will be downloadable to be imported on an external Radius Server

"AP-mode" secure can be disabled/enabled globally or on per port basis
If AP-Mode secure is enabled and switch detects the device as AP, it will check if the AP is supplicant or non-supplicant. It will then mark port as AP if supplicant authentication is successful and mac is learnt as bridging.
If the AP is non-supplicant, the port will not be marked as AP and consider as normal 802.1x user port.
By default “AP-Mode secure” would be disabled globally. Admin would be allowed to modify global status. Default value would not be saved in boot.cfg and not displayed in snapshot
When 802.1x is enabled on a port it takes global config as its default value. Admin would be allowed to modify status on per-port basis. AP-Mode secure status on port would be saved in boot.cfg and displayed in snapshot
Port level configuration takes precedence over global config.
When AP-Mode secure status is modified (either from enable to disable or vice-versa) on per-port basis AOS would flush previously learned users on the port
If AP-Mode secure is modified globally then existing 802.1x ports will not have any impact. This global value would reflect only for the new ports that are created henceforth.
If there is a change in global AP-Mode secure status then switch would not flush previously learned macs on the switch. Only per port configuration change has an impact
Global and per-port AP-Mode configuration would be synced to secondary CMM

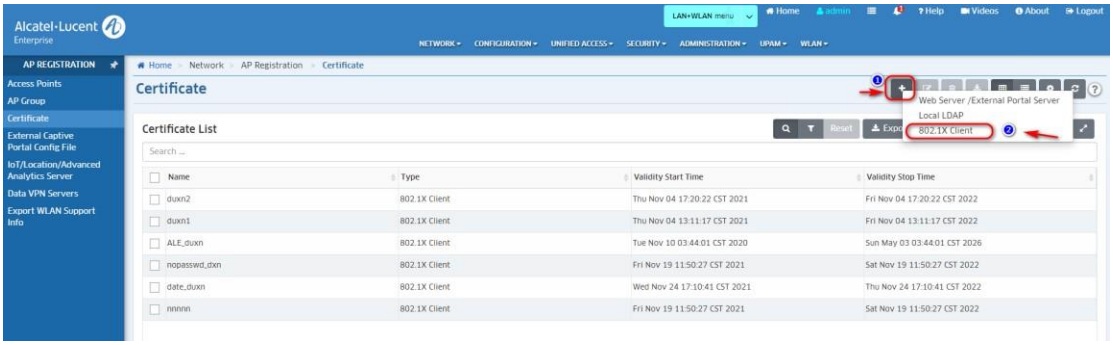
```
802.1x ap-mode {enable | disable} [secure {enable | disable}]
802.1 x {<slot>/<port > | <num/num-num>} ap-mode {enable | disable} [secure {enable | disable}]
show 802.1x ap-mode status
AP WLAN Mode        = Enabled
AP Secure Mode      = Enabled
```

On OV -> AP Registration -> AP Group a new option "802.1x supplicant"

If above option is On, a droplist is displayed with:

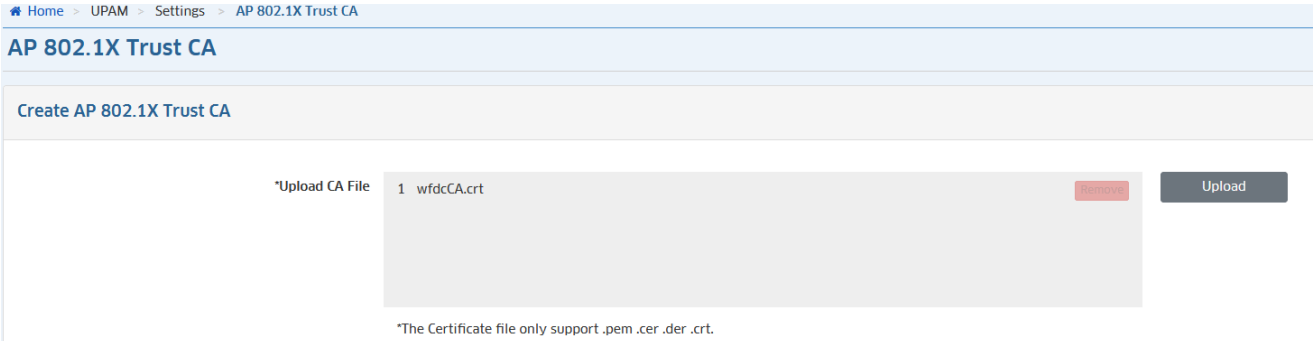
- Buit-in certificate
- Customer imported certificate

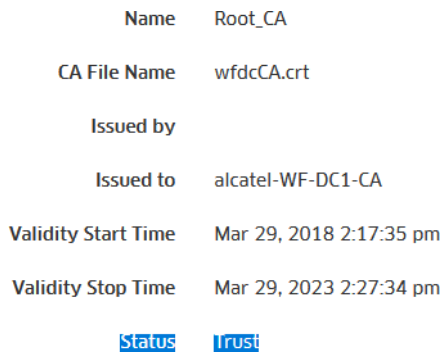
If you want to use a customer certificate, go to Network->AP Registration-> Certificate and upload the 802.1X client certificate:



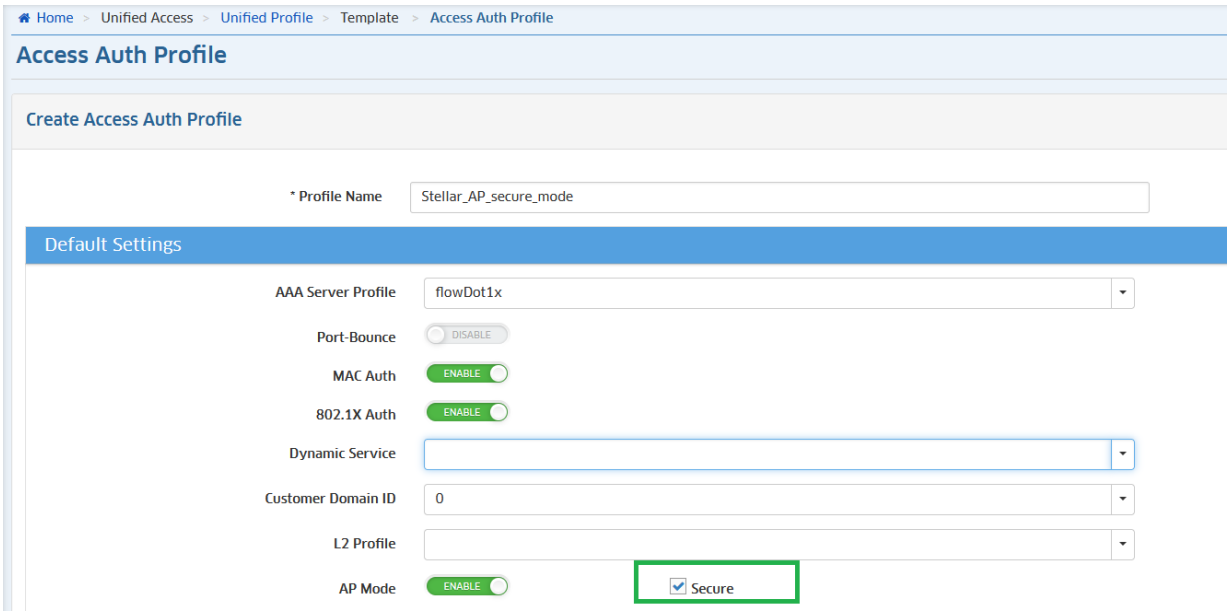
Select the customer certificate in the AP Group -> 802.1x Supplicant on AP Management Port section -> Certificate for 802.1X

Then trust the certificate in UPAM -> Settings -> AP 802.1X Trust CA and upload the Root CA used for signin the certificate:





From OV 4.6R02 / OVC 4.6.2 the Unified Access -> Unified Profile -> Template -> Access Auth Profile used for configuring 802.1X/UNP Port on OmniSwitchs is enhanced with new checkbox “Secure” for enabling AP secure mode on port.



Note: UPAM Access Policies with condition matching with Stellar AP as 802.1x client must be created and associated with a UPAM Authentication Strategy:

- If network type is wired
- If authentication type is 802.1X

Note: To learn about 802.1x Auth failures where AP is the client, check your RADIUS Server's Authentication Records

Note: Switch is NAS client and must be managed on OV 2500/OVC before the Stellar AP is able to authenticate, otherwise the Radius Access-Requests will be discarded

5.56 Stellar RAP and DS-Lite support

5.56.1 Function description

As of AWOS 4.0.4/ OV 4.6R02/OVC 4.6.2 Stellar Remote Access Points can register thru a Provider supporting DS-Lite (

Dual-Stack Lite enables a broadband service provider to share IPv4 addresses among customers by combining two well-known technologies: IP in IP (IPv4-in-IPv6) and Network Address Translation (NAT).

DS-Lite router imposes additional IP in IP overhead. This degrades the performance when clients use default MTU value.

Known issues prior to this feature:

- The Stellar RAPs will stay "DOWN" in OmniVista Enterprise, even if a "ping" will go through.
- The throughput of Stellar RAPs is too low (2-3 Mbps)

5.56.2 How does it work ?

For TCP applications, we need to expose on RAP VPN settings the tcpmss setting. Based on the reduced setting, AP and VPN Server will cause the TCP endpoint (client and app-server) to choose smaller TCP window and the frame size from the source will be reduced to 1382, the fragmentation can be avoided in AP & VPN server before tunnel encapsulation. For VPN management connection, the AP registration phase also needs to use this setting.

For UDP, fragmentation cannot be avoided unless router sends PMTU (Path MTU discovery) to notify endpoints (client and app-server) to use smaller MTU (such as 1382). We cannot guarantee every router facing the client or app-server will provide PMTU support.

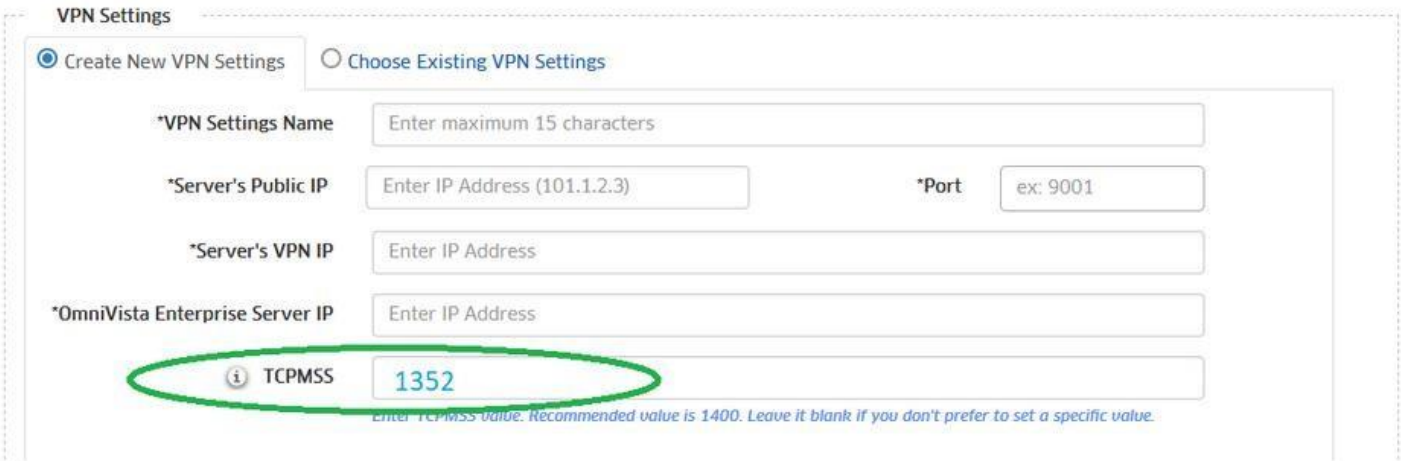
RAP solution is setup as L2GRE over Wireguard. This adds to overhead and reduces the RAP performance over the WAN.

Starting this release we provide an option to configure:

- TCPMSS for Management VPN: Recommended value is 1352 bytes. Configurable range can be 500~1460.
- TCPMSS for Data VPN: Recommended value is 1300 bytes. Configurable range can be 500~1460.

- MTU for L2GRE over tunnle: Recommended value is 1376, vlan-sub-interface should be 4 bytes less automatically. Configurable range can be 500 ~ 1500.

Step1: When creating RAP on GOV (Freemium Tenant at https://registration.ovcirrus.com/login.html) we have now new attribute TCPMSS for Management VPN Tunnel:



Once applied and RAP reset to factory, RAP will register to OVC Freemium and will get the TCPMSS value applied on the iptables, to verify execute command iptables -S:

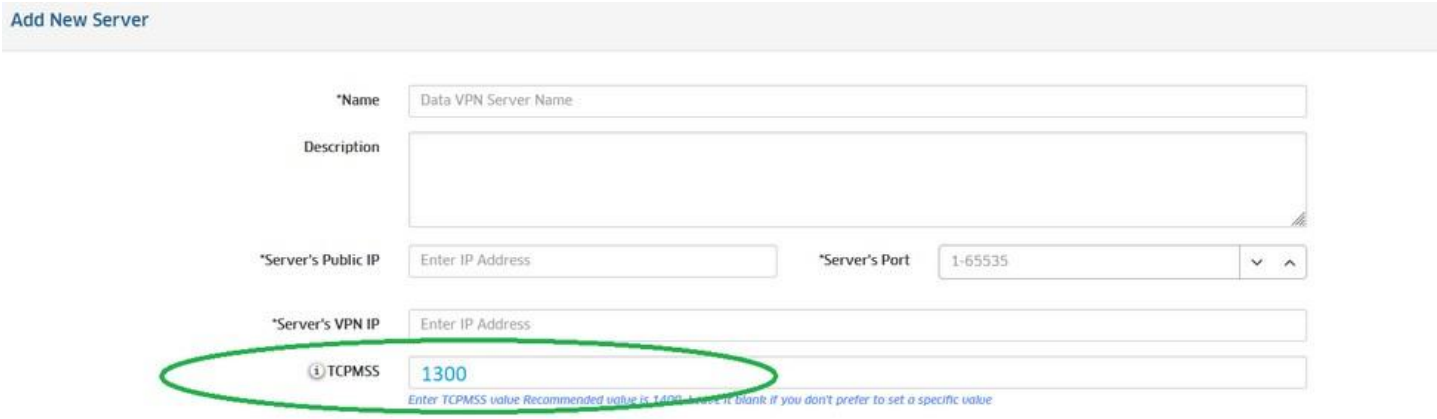
```
-A INPUT -i wg0 -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --set-mss 1352
-A OUTPUT -o wg0 -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --set-mss 1352
```

The AP must be Registered on OV 2500 - Status UP, wireguard tunnel wg0 UP with an handshake:

```
support@AP-31:50:~$ ssudo wg
interface: wg0
  public key: R/prSRc=
  private key: (hidden)
  listening port: 58161

peer: uQy1Hvyz+oUk=
  endpoint: x.x.x.x:6570
  allowed ips: 10.130.7.24/32, 10.69.145.153/32
  latest handshake: 17 seconds ago
  transfer: 2.66 MiB received, 4.83 MiB sent
  persistent keepalive: every 5 seconds
```

If RAP is registered to OVC Tenant Paid-Account, the above step is not required

Step2: On OV 2500 running 4.6R02 go to Network -> AP -> Data VPN Servers -> edit the TCPMSS setting:



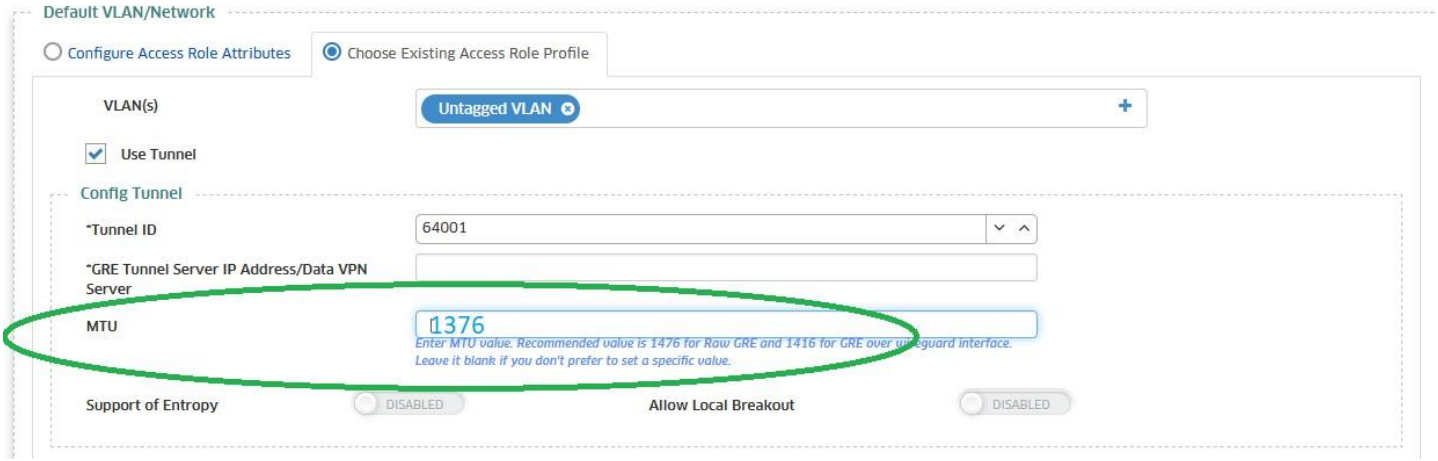
When RAP is registering to OV, RAP is getting Data VPN Settings and TCPMSS value, you can check on Stellar AP /var/config/datavpn.conf and new iptables rule:

```
iptables -S => new rule -A rap tcpmss -o br-g1 -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCMPSS --
set-mss 1300
```

Check the MTU of wireguard tunnel 1:

```
ifconfig wg1 => MTU is 1472
ifconfig g1 => MTU is 1376
```

<u>Step3</u>: On OV 2500 -> WLAN -> SSID edit the MTU value:



<u>Note</u>: There is no need for exporting/importing VPN Settings on VPN-VA Server to support this feature

<u>Fine tune the above settings</u>

Use ping command with OV's ipaddress as destination to check what is the maximum data allowed "ping -s [packetSize] destination"

For example, on the RAP we ping -s 1380 192.168.26.10. The destination should be the OV IP because RAP has a route to forward it to WG mgmt interface.
If the ping does not receive a successful reply, we need to adjust the packet size moving up/down of 100 bytes, and repeat the ping command until we get a successful reply.

Starting with a number around 1200-1380 bytes.
If we started with 1200 and got a successful reply, then move up to 100 bytes and ping again. Repeat the process until we find the best packet size.

For example, if we find that 1352 is the best value that is going through the path over WG interface successfully, so 1352 is the data payload size or maximum segment size(MSS).

Using iPerf tool for testing a TCP connection.
To use iPerf, we need to setup iperf client and iperf server.
iperf-client-PC -> RAP -> ISP-Network -> VPN-Server -> iperf-server

Before we start to test the performance data MTU of GRE needs to be calculated.
Recommended default value of MTU for GRE interface:
GRE over wireguard interface : 1500 -20(IP) -8(UDP) - 32(WG) - 20(IP) - 4(GRE) = 1416

When the tunnel is over DS-Lite (IPv4 over IPv6 tunnel), additional 40 bytes of IPv6HDR should be subtracted. So MTU of GRE tunnel will be 1416 - 40 = 1376.

Continue to subtract 58 bytes to get TCP MSS for data vpn interface.
TCPMSS-for-traffic-inside-GRE = MTU-of-GRE-Tunnel - 14(ETH) + 4(VLAN) + 20(IP) + 20(TCP) = 1376 - 58 = 1318.

Now we get two values: GRE interface MTU = 1376 & TCPMSS-inside-GRE-over-Wireward = 1318.

Run the following commands to test download/upload speed from client-PC:

Test upload (client sends, server receives)
iperf3 -c 192.168.26.10 -V -t 20

Test download (server sends, client receives)
iperf3 -c 192.168.26.10 -V -R -t 20

5.57 Bypass and Trust tag (Express/OVE/OVC)

Bypass and Trust tag settings are dedicated to Stellar AP's downlink ports. When Trust tag is enabled, Stellar AP can transfer tagged packets received from wired user to AP's uplink port. When Bypass is enabled, user is prompted to select a VLAN ID that will be used to transfer the untagged packets received from wired user into tagged packets through the AP's uplink port.
These 2 settings are supported on Stellar AP 1201H/1201HL/1301H/1311.

Through OVE/OVC, go to Unified Access -> Unified Profile -> Template -> create an Access Auth Profile:

- Enable Trust Tag and select a Default Access Role Profile, the tagged traffic received from downlink ports will be forwarded thru UPLINK with same tag VID
- Enable Bypass and set a tag VID that will be used for tagging the untagged traffic received from downlink ports forwarded thru UPLINK

Then apply the Access Auth Profile to Stellar AP Groups (Apply to devices button), select the Ethernet Downlink Ports

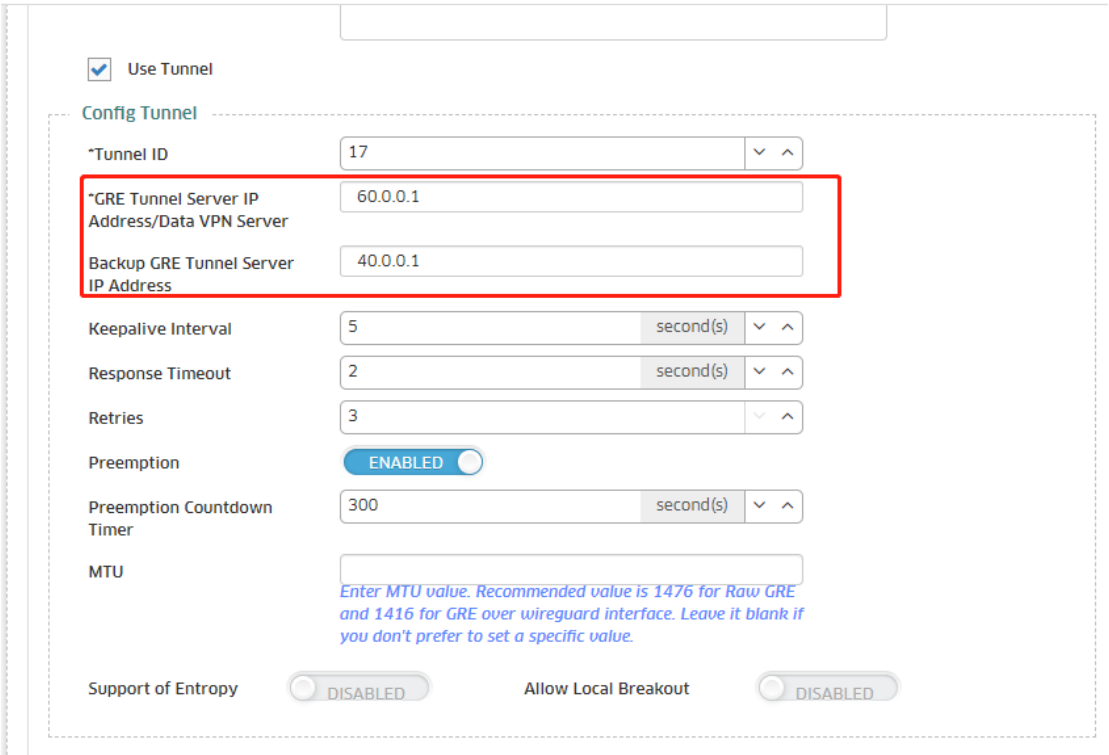
5.58 SNMPv3

On AP running in Express mode, go to System -> Syslog & SNMP -> SNMP and select the version v3 and fill-in the Username/Passphrase. Authentication protocol is SHA and privacy protocol is AES.
For configuring SNMPv3 for traps, when enabling the SNMP Trap feature, you can select the version v3 and fill-in the Trap Server, Username and password.

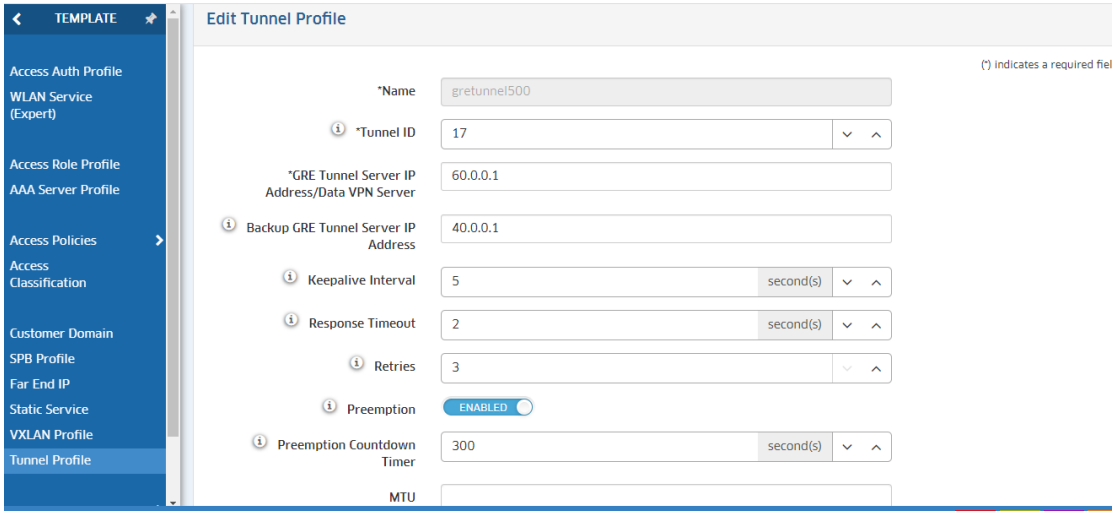
5.59 GRE Tunnel Resiliency (OVE/OVC)

We can define a Primary and Backup GRE Tunnel server. Two GRE tunnels termination are configured on two separate switches. Stellar AP will choose the Primary server, if Primary is down, Stellar AP will choose the Backup server till the Primary is Down. Once Primary is UP, Stellar AP will change to Primary server.

On the SSID configuration, you can define the Primary and Backup GRE servers:



Or in Home -> Unified Access -> Unified Profile -> Template -> Tunnel Profile:



When applying to the devices you can select the method Map to Tunnel and the above Tunnel profile

5.60 Multiple options in DHCP option82 string (OVE/OVC)

Admin can configure the custom string as $$vlan-$ssid-$apmac.
The first $ character can signal it is a custom parameter string.
The subsequent $ character signals the parameter required.

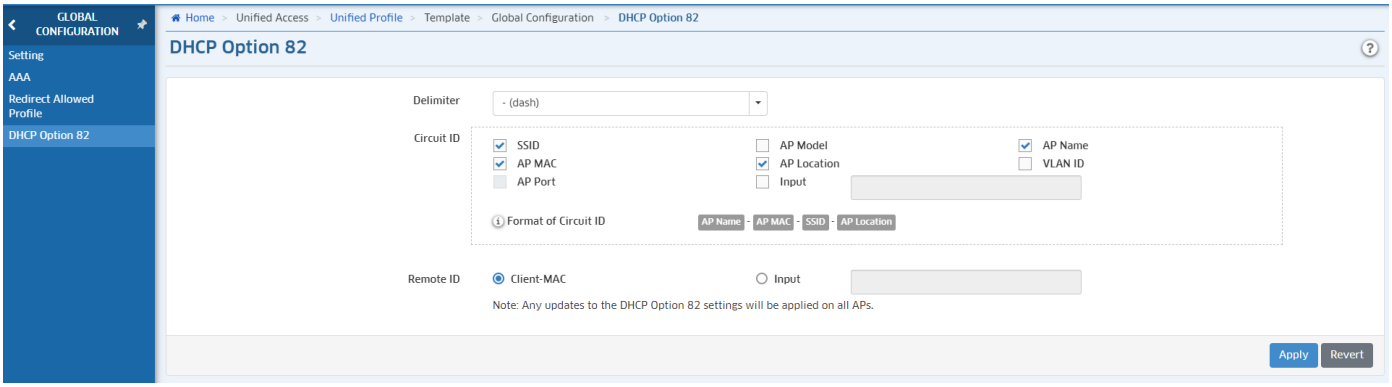
This provides flexibility to the user on the order of the parameters and the delimiter to use between each parameter. The access point will parse the string and send the required fields as part of the DHCP option82 parameter.

Caution: The length of the Circuit ID is limited to 128bytes. If it is too long, the option attribute is not added.

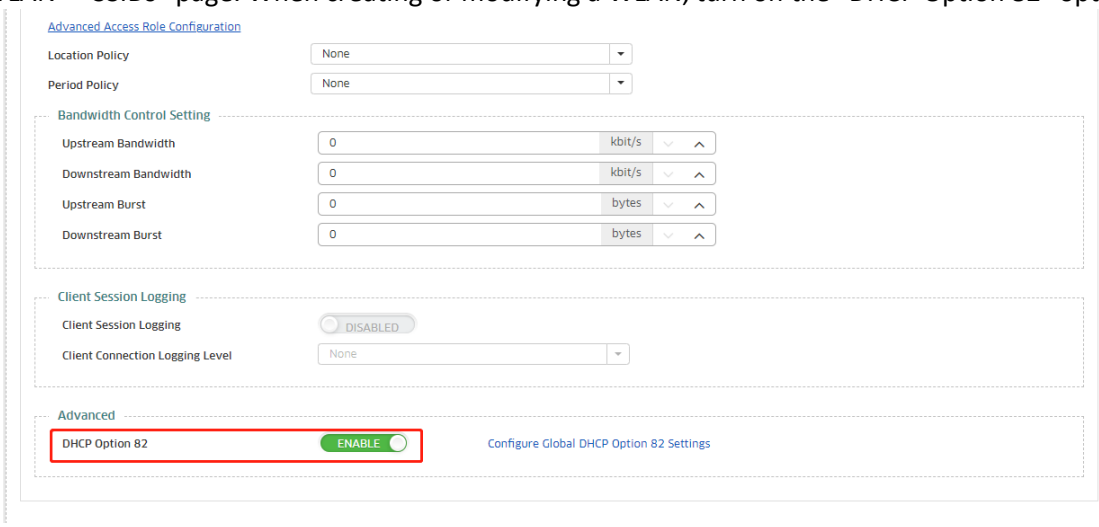
Configuration

1. Go to the «Unified Access -> Unified Profile -> Template -> Global Configuration -> DHCP Option 82" page.

Delimiter - The character to use as a delimiter between values specified in the Circuit ID sub-option.
Format of Circuit ID - Displays the format of the selected Circuit ID sub-option information with the specified delimiter character. For example, if a dash is the specified delimiter the format should be "AP Name - AP MAC - SSID - AP Location".



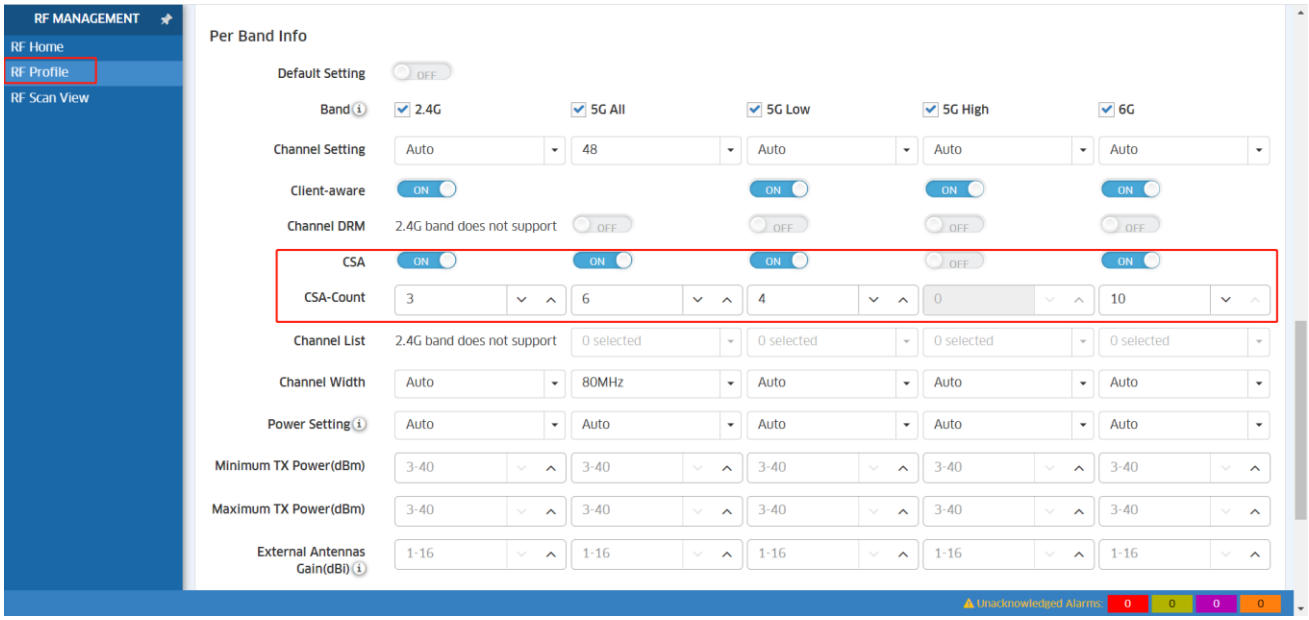
2. Go to the "WLAN -> SSIDs" page. When creating or modifying a WLAN, turn on the "DHCP Option 82" option.



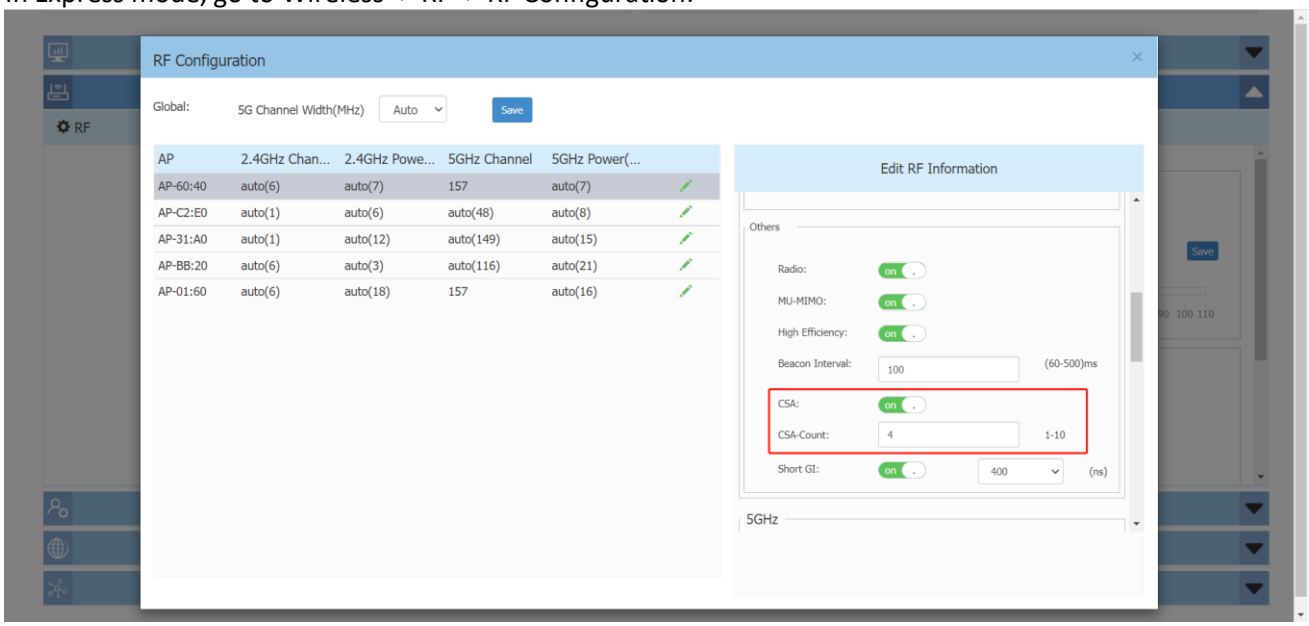
5.61 CSA support in RF Profile (Express/OVE/OVC)

Channel Switch Announcement (CSA) as defined by IEEE 802.11h allows an AP to announce that it is switching to a new channel before it begins transmitting on that channel. This allows clients who support CSA to transition to the new channel with minimal downtime.
All AP models support CSA
2.4GHz and 5GHz Band support CSA, 6GHz is not supported
5GHz DFS chqnnel switching supports CSA
Automatic channel switching of AP supports CSA
Fixed channel switch of AP does not support CSA

In the WLAN -> RF Profile are added new settings:



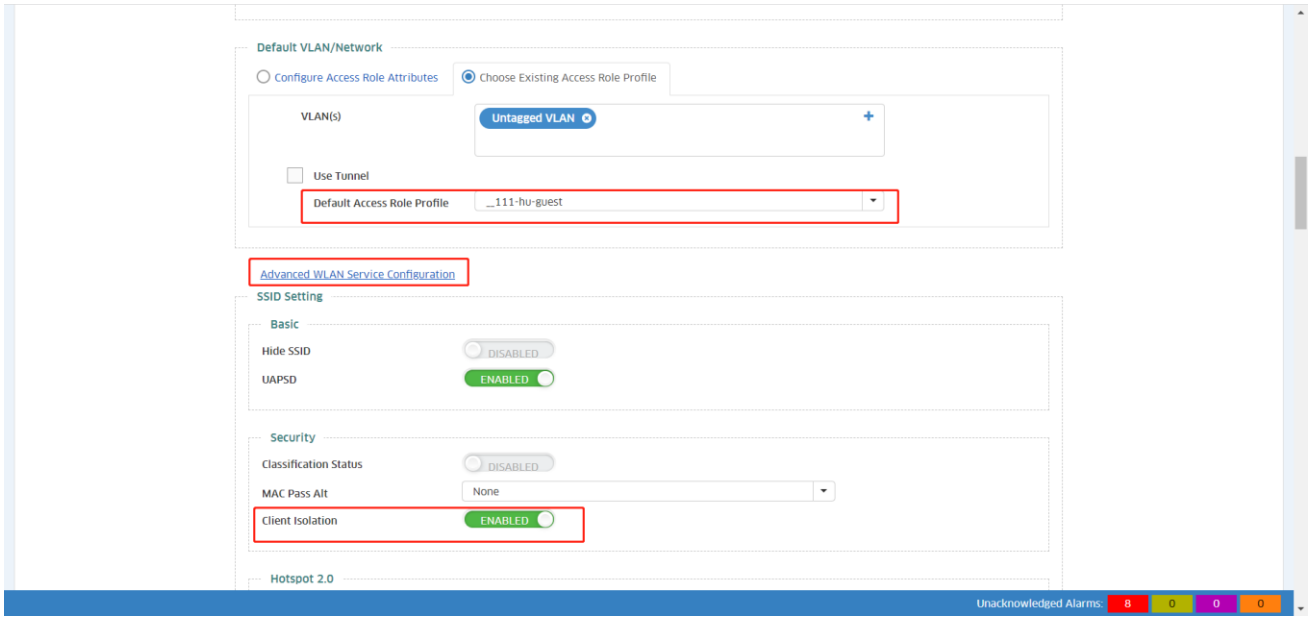
In Express mode, go to Wireless -> RF -> RF Configuration:



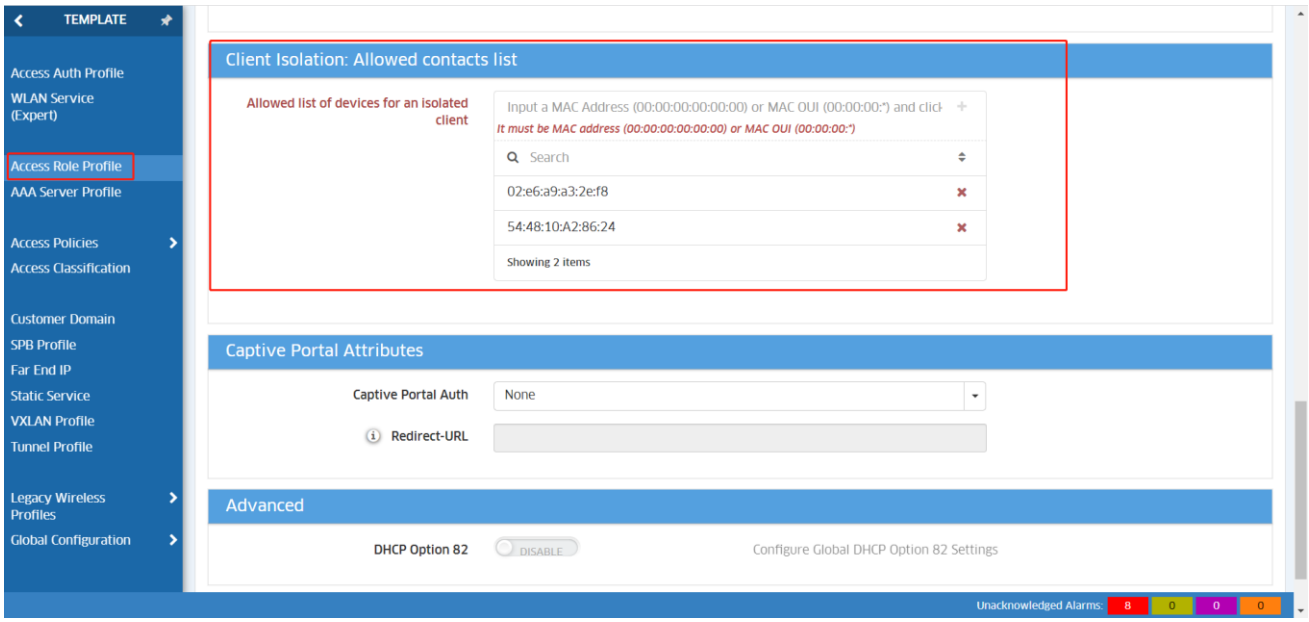
5.62 Client isolation allow list (OVE/OVC)

After client isolation is enabled on the SSID, all clients connected to the SSID can communicate with the default gateway and the devices allowed by the client allow list.

- This function only takes effect when SSID enables Client Isolation.
- The Client Isolation function is only applicable to the Layer 2 network.
- User isolation only supports the wireless side isolation function, and the allow list only takes effect between wireless clients. At present, this function does not take effect on wired clients connected to the AP downlink.
- If the user is accessed before the isolation function is enabled, the user needs to go online again for the isolation function to take effect

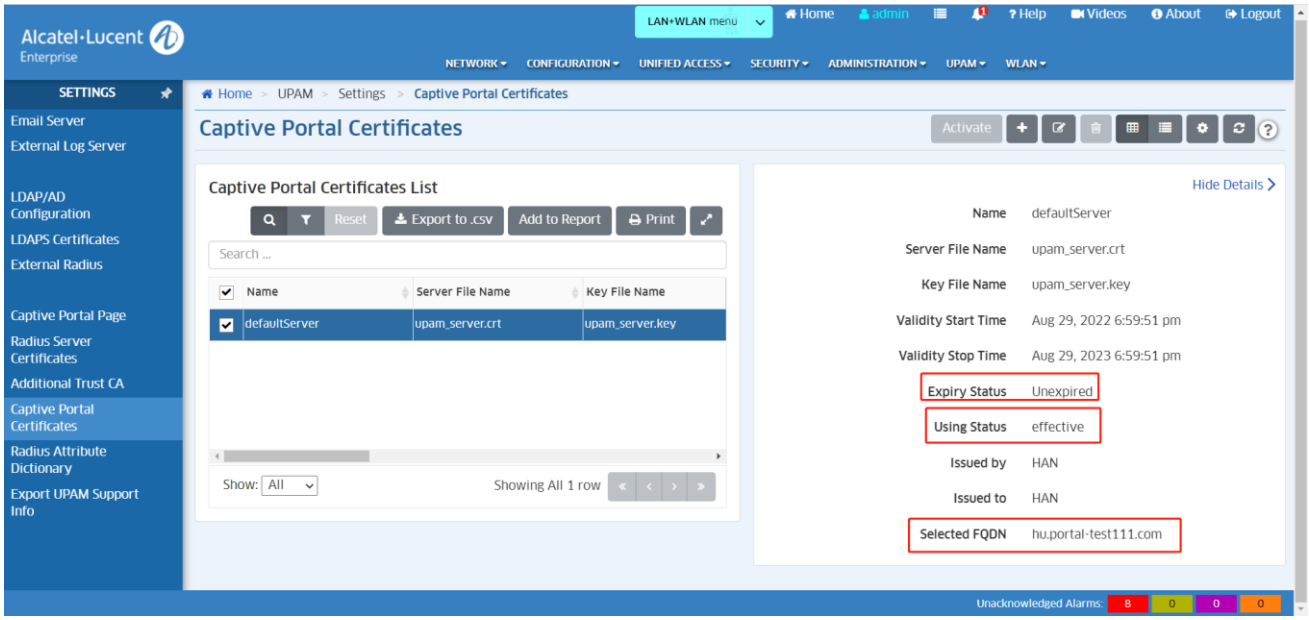


Add a device MAC Address to the ARP associated to the SSID to allow device to communication with that device.



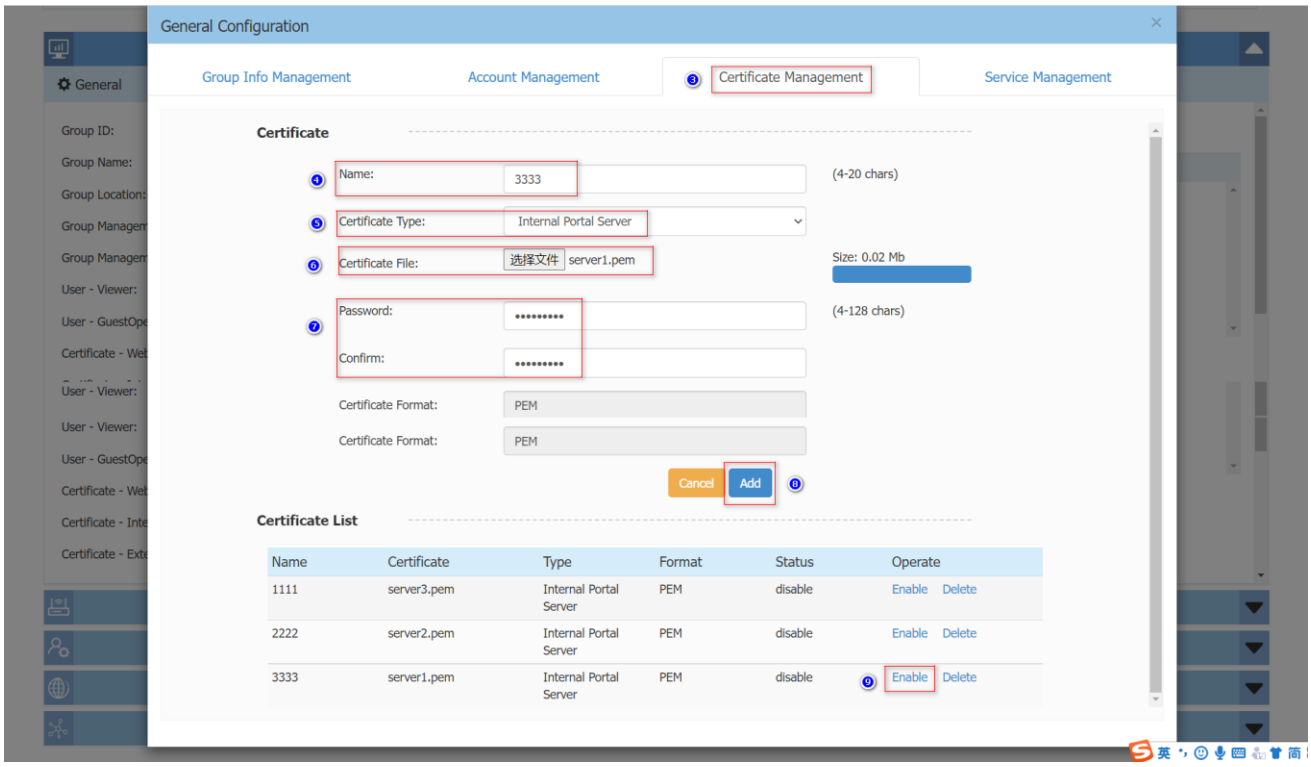
5.63 Update the Captive Portal certificate (OVE)

When the default captive portal certificate of OV 2500 expires, users can update his own Captive Portal certificate. Once imported thru UPAM -> Captive Portal Certificates, select it and click on Activate to be effective.



5.64 Update the Captive Portal certificate (Express)

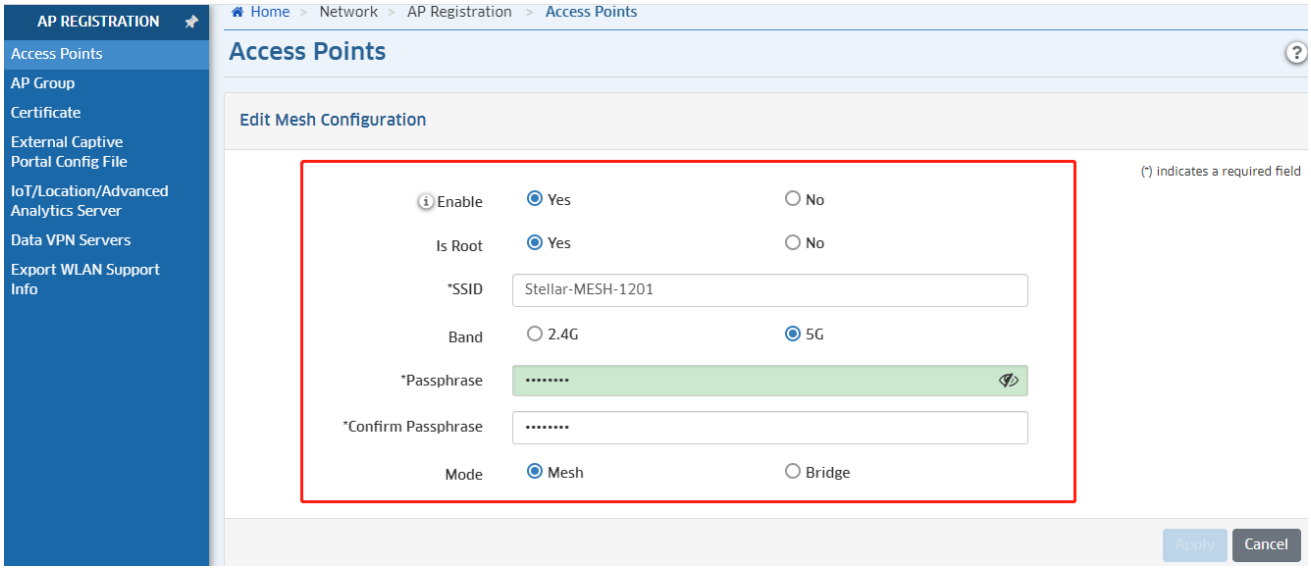
All models support updating certificates
Certificates with or without password are supported
Up to 6 certificates can be uploaded
Only one certificate can be enabled



5.65 Mesh configuration thru OV (OVE/OVC)

Through Home -> Network -> AP Registration -> Access Points, you can edit the Mesh configuration:

- Enable: Yes/No
- Is Root: Yes/No
- SSID broadcasted by Mesh APs
- Band: 2.4G/5G
- Passphrase
- Mode: Mesh/Bridge
  - ⇨ Note that Bridge mode is not supported on OVC



6 Useful CLI Commands

All available commands with support account can be listed with command tech_support_command ?

```
support@AP-C3:B0~$ tech_support_command ?
usage:
1           show system info
2           show WIFI info
3           show traps info
4           show syslog info
5           show cpu utilization
6           show mem utilization
7           tcpdump command
8 [HOST]    traceroute [HOST] command
9 [HOST]    ping command
10          check reboot reason
11          tar syslog
12          take snapshot IP
13          show ap channel and channel utilization
13          show ap channel and channel utilization
14          lldpctl
15          iptables -nvL
16          ubus call wam sta_list
17          ubus call eag show_user_info
18          ubus call ap_manage showlldp
19          ubus call policy show
20          ubus call wam GetSyncInfo
21          ubus call network.macvlan macvlan_info
22          ubus call wam wired_user
23          wam_debug mdns_status
24          ubus call mesh show
```

6.1 System information

✓ ***Free*** ***// To check the memory usage.***

Example:

```
support@AP-C3:B0~$ free
             total       used       free     shared    buffers     cached
Mem:        123728      94856      28872          0       5072      20296
-/+ buffers/cache:      69488      54240
Swap:            0          0          0
```

✓ ***top*** ***// To check the memory&CPU usage.***

Example:

```
support@AP-D1:40:~$ top -n 1
Mem: 150888K used, 82016K free, 4732K shrd, 2716K buff, 15348K cached
CPU:   0% usr   4% sys   0% nic  88% idle   0% io   6% irq   0% sirq
Load average: 0.18 0.25 0.30 1/123 12620
  PID  PPID USER     STAT   VSZ %VSZ %CPU COMMAND
12620  8342 support  R     1312   1%   2% top -n 1
 5010     1 root     S    12384   5%   0% bg-s -q -X
```

```
 5105     1 root     S    10028   4%   0% dpi-mgr
 9148     1 root     S     7960   3%   0% /usr/sbin/drm
 4997     1 root     S     7704   3%   0% /usr/bin/wland
10183 10020 root     S     7492   3%   0% /usr/bin/echo.fcgi
 4970     1 root     S     6612   3%   0% /usr/sbin/policy
 1624     1 root     S     6280   3%   0% /sbin/adme
 8281     1 root     S     6224   3%   0% /usr/sbin/eag_app
 5460     1 root     S     5296   2%   0% /usr/bin/wmaagenttrap
 4697     1 root     S <   4752   2%   0% wam -g /var/run/wam/global -m -d -f /
10020     1 root     S     4692   2%   0% /usr/sbin/lighttpd -D -f /etc/lighttp
 1506     1 root     S     4124   2%   0% wpa_supplicant -g /var/run/wpa_suppli
 4715     1 root     S     4040   2%   0% /usr/bin/wmaagent
 4988     1 root     S     3812   2%   0% /usr/sbin/AG-manager
 5038     1 root     S     3808   2%   0% /usr/sbin/dhcp_relay
 5029     1 root     S     3744   2%   0% /usr/sbin/client_behavior -m
 3100     1 root     S     3568   2%   0% /usr/bin/ap_manage
12076     1 root     S     3440   1%   0% /usr/sbin/lbd -d -C /tmp/lbd.conf
12336     1 root     S     3428   1%   0% /usr/sbin/collect_log_manager
```

- ✓ ***sar*** ***// To check the CPU usage by specified frequency.***

  Example:

```
support@AP-D1:40:~$ sar 2
Linux 3.14.77 (AP-D1:40)        04/02/20        _armv7l_        (4 CPU)

01:01:46        CPU     %user     %nice   %system   %iowait    %steal     %idle
01:01:48        all      0.75      0.00      6.40      0.00      0.00     92.85
01:01:50        all      0.38      0.00      7.40      0.00      0.00     92.22
01:01:52        all      3.90      0.00     14.97      0.00      0.00     81.13
01:01:54        all      1.38      0.00     11.06      0.00      0.00     87.56
01:01:56        all      1.13      0.00     10.93      0.00      0.00     87.94
01:01:58        all      1.64      0.00     12.34      0.00      0.00     86.02
01:02:00        all      2.64      0.00     14.34      0.00      0.00     83.02
01:02:01        all      2.91      0.00      9.64      0.00      0.00     87.44
Average:        all      1.78      0.00     10.95      0.00      0.00     87.27
```

- ✓ ***Showsysinfo*** ***// To check the AP hardware information.***

  Example:

```
support@AP-D1:40:~$ showsysinfo
    Company Name:ALE USA Inc
              SN:SSZ171100060
    Device Model:OAW-AP1221
             MAC:34:E7:0B:03:D1:40
         Country:RW
   Software Name:AWOS
Software Version:3.0.7
Hardware Version:1.10
              Oid:1.3.6.1.4.1.6486
     Part Number:903919-90
        Revision:
    Essid Prefix:mywifi
Cluster Describe:AP Group
         Website:http://www.al-enterprise.com
           Legal:Copyright 漏 1995-2020 ALE USA Inc.   ALL RIGHTS RESERVED WORLDWIDE
        Describe:HOS 30
```

```
```

- ✓ ***ps |grep <process>*** ***// To check the status of the related software process.***

  Example:

```
support@AP-D1:40:~$ ps |grep drm
 9148 root      7960 S    /usr/sbin/drm
18602 support   1304 S    grep drm
support@AP-D1:40:~$
support@AP-D1:40:~$ ps |grep wmaagent
 4715 root      4040 S    /usr/bin/wmaagent
 5460 root      5296 S    /usr/bin/wmaagenttrap
18744 support   1304 S    grep wmaagent
```

- ✓ ***ps |grep D*** ***// To check if there's any software process in D (dead) state.***

  Example:

```
support@AP-D1:40:~$  ps |grep D
  PID USER       VSZ STAT COMMAND
 1677 root      2180 S    /usr/sbin/DNS_Snooping
10020 root      4692 S    /usr/sbin/lighttpd -D -f /etc/lighttpd/lighttpd_http
27129 support   1304 S    grep D
```

- ✓ ***uptime*** ***// To check the AP run time***

  Example:

```
support@AP-D1:40:~$ uptime
 01:27:34 up  1:48,  load average: 0.13, 0.28, 0.30
```

- ✓ ***date*** ***// To check AP system date and time***

  Example:

```
support@AP-D1:40:~$ date
Thu Apr  2 01:38:33 2020
```

- ✓ ***ssudo passwd*** ***// To modify the password of "support" account***

  Example:

```
support@AP-D1:40:~$ ssudo passwd
Changing password for support
New password:
Retype password:
Password for support changed by root
support@AP-D1:40:~$
```

- ✓ ***showver*** ***// To check AP firmware version***

  Example:

```
support@AP-D1:40:~$ showver
3.0.7.2056
```

- ✓ ***reset_record get*** ***// To check the recent reset reasons***

  Example:

```
support@AP-CA:70:~$ reset_record get
[0] * 2020/03/25 07:36:35 +0000 * A040 * Watchdog starve
[1] * 2020/03/24 08:04:32 +0000 * C010 * osupgrade: update firmware
[1] * 2020/03/24 08:08:47 +0000 * B021 * acv_clientd: cloud->cluster, clear configuration
[1] * 2020/03/24 09:52:27 +0000 * A010 * Power Off
[1] * 2020/03/25 07:31:39 +0000 * A010 * Power Off
```

Note：The reset_record mainly records the restart event at the business level, regarding some abnormal restarts on system level, it will not be recorded in this list, the /tmp/kes_history_traps.log is responsible for record kernel panic logs, and it can record at least 10 times of kernel error reboot logs.

- ✓ ***ssudo firstboot // To clear all the settings and reset to factory.***

Example:

```
support@AP-D1:40:~$ ssudo firstboot
This will erase all settings and remove any installed packages. Are you sure? [N/y]
y
support@AP-D1:40:~$
support@AP-D1:40:~$ ssudo reboot
```

- ✓ ***ssudo reboot // To reboot the AP device***

Example:

```
support@AP-D1:40:~$ ssudo reboot
```

- ✓ ***iwpriv wifi0 getCountry //To check the "Country Code" of the AP***

Example:

```
support@AP-D1:40:~$ iwpriv wifi1 getCountry
wifi1     getCountry:SG
support@AP-D1:40:~$
support@AP-D1:40:~$ iwpriv wifi0 getCountry
wifi0     getCountry:SG
support@AP-D1:40:~$
```

- ✓ ***cat /proc/kes_syslog // To check the system log and filter could be used for specific requests.***

Example:

```
support@AP-D1:40:~$ cat /proc/kes_syslog |tail -10
2020-04-02 01:59:33 System wmaagent[4715] <NOTICE> [AP 34:E7:0B:03:D1:40@] : Client
AP_34:E7:0B:03:D1:40 sending PINGREQ
2020-04-02 01:59:34 System wmaagent[4715] <NOTICE> [AP 34:E7:0B:03:D1:40@] : Client
AP_34:E7:0B:03:D1:40 received PINGRESP
2020-04-02 01:59:45 Ap-Debug syslog[null] <WARNING> [AP 34:E7:0B:03:D1:40@] <kernel> :
[ 8415.238246] Sending SCAN START cmd
```

6.2 Wireless Management

- ✓ ***Iwconfig // To check the wireless configuration***

Example:

```
support@AP-70:20:~$  iwconfig
gre0      no wireless extensions.
```

```
ath03     IEEE 802.11ng  ESSID:"12345/123"
          Mode:Master  Frequency:2.412 GHz  Access Point: DC:08:56:13:70:23
          Bit Rate:192 Mb/s   Tx-Power=9 dBm
          RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality=89/94 Signal level=-60 dBm  Noise level=-95 dBm
          Rx invalid nwid:323937 Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0

ath13     IEEE 802.11ac  ESSID:"12345/123"
          Mode:Master  Frequency:5.26 GHz  Access Point: DC:08:56:13:70:2B
          Bit Rate:866.7 Mb/s   Tx-Power=16 dBm
          RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality=94/94 Signal level=-52 dBm  Noise level=-95 dBm
          Rx invalid nwid:5146277  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

- ✓ ***cat /tmp/config/rfprofile.conf // To check the RF configuration***

  Example:

```
support@AP-70:20:~$ cat /var/config/rfprofile.conf
{
        "RFService":[
                {
                        "bandSteering":"enable",
                        "bandSteeringForce5g":"disable",
                        "LoadBalance":"enable",
                        "backgroundScanning":"enable",
                        "scanningEnhance":"disable",
                        "countryCode":"CN",
                        "scanningInterval":20,
                        "scanningDuration":50,
                        "voiceVedioAwareness":"disable",
                        "airtimeFairnessAt2G":"disable",
                        "airtimeFairnessAt5G":"disable",
                        "perBandInfo":{
```

- ✓ ***iwlist ath11 channel // To check the cannel of ath01 interface. The same for other interfaces***

  Example:

```
support@AP-70:20:~$
support@AP-70:20:~$ iwlist ath11 channel
ath11     75 channels in total; available frequencies :
          Channel 36 : 5.18 GHz
          Channel 40 : 5.2 GHz
          Channel 44 : 5.22 GHz
          Channel 48 : 5.24 GHz
          Channel 52 : 5.26 GHz
          Channel 56 : 5.28 GHz
          Channel 60 : 5.3 GHz
          Channel 64 : 5.32 GHz
          Channel 149 : 5.745 GHz
          Channel 153 : 5.765 GHz
          Channel 157 : 5.785 GHz
          Channel 161 : 5.805 GHz
          Channel 165 : 5.825 GHz
```

```
          Current Frequency:5.26 GHz (Channel 52)
```

- ✓ ***iwlist ath11 txpower*** ***// To check the txpower of ath01 interface. The same for other interfaces***

Example:

```
   support@A-70 :20:~$ iwlist ath11 txpower
ath11     8 available transmit-powers :
          0 dBm         (1 mW)
          5 dBm         (3 mW)
          6 dBm         (3 mW)
          7 dBm         (5 mW)
          8 dBm         (6 mW)
          9 dBm         (7 mW)
          10 dBm        (10 mW)
          11 dBm        (12 mW)
          Current Tx-Power=11 dBm       (12 mW)
```

- ✓ ***iwlist athxx bitrate*** ***//To check the bit rate of athxx interface.***

Example:

```
       support@AP-70:20:~$ iwlist ath11 bitrate
ath11     8 available bit-rates :
          6 Mb/s
          9 Mb/s
          12 Mb/s
          18 Mb/s
          24 Mb/s
          36 Mb/s
          48 Mb/s
          54 Mb/s
          Current Bit Rate:866.7 Mb/s
```

- ✓ ***iwpriv athxx get_mode*** ***//To check the interface mode of athxx.***

Example:

```
support@AP-70:20:~$ iwprivat11 get_mode
ath11     get_mode:11ACVHT80
```

- ✓ ***iwpriv wifi0 get_txchainmask or iwpriv wifi1 get_txchainmask*** ***//To check the spatial streams quantity supported by the Steller AP***

Example:

```
support@AP-70:20:~$ iwpriv wifi1 get_txchainmask
wifi1     get_txchainmask:3
```

- ✓ ***telnet 127.0.0.1:7787 then stadb and s*** ***//To check*** the clients supported band currently detected by the AP

Example:

```
support@AP-70:20:~$ telnet 127.0.0.1:7787
Use `h' ad7 `help' for help messages
Use `dbg here' to see log messages; other dbg cmds for log level
@stadb s
Num entries = 182

MAC Address       Age    Bands     Assoc? (age)
Active? (age)       Flags
34:F3:9A:AB:79:30  21    25    APId 255 ChanId 52  ESSId 2   (1407)    yes (56)  BTM
RRM   Steer Allowed
```

```
@stadb

Press ctrl+d to exit
```

✓ ***cat /proc/kes_syslog |grep DRM*** ***//To check the logs of ACS and APC management***

Example:

```
support@AP-70:20:~$ cat /proc/kes_syslog |grep DRM
2020-07-31 14:23:49 Wireless wland[5953] <NOTICE> [AP
DC:08:56:13:70:20@172.16.10.115] : _GOLSOH_change 2.4G channel from 6 to 1 by DRM.
2020-07-31 14:56:05 Wireless wland[5953] <NOTICE> [AP
DC:08:56:13:70:20@172.16.10.115] : _GOLSOH_change 2.4G channel from 1 to 11 by DRM.
```

6.3 Client Management

✓ ***ssudo sta_list*** ***// To list all the clients associated with this AP***

✓ ***ssudo wam_debug sta_list*** ***// List the detailed attributes that AP sends to the client.***

```
{
                                        "staMAC": "34:f3:9a:ab:79:30",
                                        "staIP": "172.16.10.102",
                                        "staGlobalIPv6":  "2008::13",
                                        "staLocalIPv6": "fe80::7c08:5dfd:7dd8:18c3",
                                        "associationTime": 2028,
                                        "mappingType": 0,
                                        "assignedVLAN": 0,
                                        "assignedAR": "1594971518165arp",
                                        "assignedPL": "",
                                        "macAuthResult": "",
                                        "ARFromMACAuth": "",
                                        "PLFromMACAuth": "",
                                        "redirectURLFromMACAuth": "",
                                        "ARFrom8021xAuth": "",
                                        "PLFrom8021xAuth": "",
                                        "redirectURLFrom8021xAuth": "",
```

✓ ***wlanconfig ath11 list*** ***// To list all clients on specific AP interface***

Example:

```
root@AP-34:D0:~#
root@AP-34:D0:~#
root@AP-34:D0:~# wlanconfig ath12 list
ADDR              AID CHAN TXRATE RXRATE RSSI MINRSSI MAXRSSI IDLE  TXSEQ  RXSEQ  CAPS XCAPS       ACAPS     ERP    STATE MAXRATE(DOT11) HTCAPS VHTCAPS ASSOCTIME    IEs   MODE
       PSMODE RXNSS TXNSS
34:f3:9a:ab:79:30    1   36 866M    866M   39      39      46    1      0   65535   EPs  EBQO        0         b            0          AWPSM          gGTRs 00:00:20  RSN WME IEEE80211
_MODE_11AC_VHT80   0 2 2 Minimum Tx Power              : 0
 Maximum Tx Power               : 14
 HT Capability                  : Yes
 VHT Capability                 : Yes
 MU capable                     : No
 SNR                            : 39
 Operating band                 : 5GHz
 Current Operating class        : 0
 Supported Rates                : 12  18  24  36  48  72  96  108
root@AP-34:D0:~#
```

Below are the elements descriptions

Element	Description					
ADDR	MAC address of the STA					
AID	Association ID; determines the specific AP/STA association pair used in 802.11n test commands					
CAPS	**E**	ESS	**P**	Privacy	**s**	Short Slot Time
	I	IBSS	**S**	Short Preamble	**D**	DSSS/OFDM
	c	Pollable	**B**	PBCC		
	C	Poll Request	**A**	Channel Agility		
CHAN	Channel the device is associated on					
ERP	Extended Rate PHY capabilities in dBm. A value of 0 indicates a legacy STA. Printed in hex.					
HTCAPS	HT capabilities flags; these are character indicators that represent a capability of the 802.11n STA					
	A	Advanced coding	**Q**	Static MIMO power save	**S**	Short GI enabled (HT40)
	W	HT40 channel width	**R**	Dynamic MIMO power save	**D**	Delayed block ACK
	P	MIMO power save enabled	**G**	Greenfield preamble	**M**	Max AMSDU size
IDLE	Current setting of the STA inactivity timer. This is the time in ms when the STA will go into power save of no activity occurs on the link.					
RATE	Current data rate of the association					
RSSI	Signal strength of the last received packet. For MIMO devices, this is an average value over all active receive chains.					
RXSEQ	Receive sequence number of the last received packet					
STATE	Current state of the STA. This is an hexadecimal value that consists of these bits:					
	0x0001	Authorized for Data Transfer	0x0010	Power Save Mode Enabled	0x0100	uAPSD SP in Progress
	0x0002	QoS enabled	0x0020	Auth Reference held	0x0200	An ATH Node
	0x0004	ERP Enabled	0x0040	uAPSD Enabled	0x0400	WDS Workaround Req.
	0x0008	HT Rates Enabled	0x0080	uAPSD Triggerable	0x0800	WDS Link
TXSEQ	Transmit sequence number of the last received packet					
(No Header)	All information elements (IE) for the attached STA are printed. They have the values:					
	WPA	WPA IE	**ATH**	Qualcomm Vendor IE	**RSN**	RSN IE
	WME	WMM IE	**VEN**	Vendor-Specific IE	**???**	Unknown IE

6.4 Captive Portal Management

- ✓ ***ps |grep eag*** ***// To check if the process of "eag" is running well.***

  Example:

```
support@ AP-70:20:~$ ps |grep eag
 5325 root      6228 S    /usr/sbin/eag_app -c
10526 root      1304 S    grep eag
```

- ✓ ***eag_cli show user all/list*** ***// To list the clients authenticated by captive portal***

- ✓ ***eag_cli kick user index 1*** ***// To delete a user from Portal authenticated user list.***
- ✓ ***tail -f /tmp/log/eag.log***
  cat /proc/kes_syslog |grep eag
  cat /var/log/eag.log

// To check the related logs of portal re-direction.

6.5 Cluster Management

- ✓ ***cluster_mgt -x show=self // To check the AP Cluster role and status***

  Example:

```
support@AP1201:~$ cluster_mgt -x show=self
ClusterID   MAC                   role        priority            status
100         dc:08:56:13:70:20     PVC         003f25137020        RUN

support@AP-0E:30:~$ cluster_mgt -x show=self
ClusterID   MAC                   role        priority            status
100         34:e7:0b:00:0e:30     SVC         001704000e30        RUN
```

- ✓ ***cluster_mgt -x show=pvc // To check the PVC of the cluster***

  Example:

```
support@AP-0E:30:~$ cluster_mgt -x show=pvc
IP                    MAC                   priority            status
172.16.10.106         dc:08:56:13:70:20     003f25137020        RUN
```

- ✓ ***show_cluster // To check all the AP members in the cluster***

  Example:

```
support@AP-0E:30:~$ show_cluster
mac                   ip                                prio        state       role      auth
ptype       version
dc:08:56:1b:d4:b0     172.16.10.101         0           4           3           1           22
4.0.0.3076
34:e7:0b:00:0e:30     172.16.10.100         0           3           2           1           23
4.0.0.3076
dc:08:56:13:70:20     172.16.10.106         0           3           1           1           63
4.0.0.3076
```

  Note: below are the definition for the role in cluster:

  1- PVC
  2- SVC
  3- VC

- ✓ ***ps |grep cluster // To check if "cluster" process is working normally***

6.6 Network Management

- ✓ ***cat /etc/resolv.conf // To check the DNS server information***
- ✓ ***cat /tmp/TZ // To check the Timezone configuration***
- ✓ ***cat /proc/kes_syslog |grep ntp // To check the NTP logs***
- ✓ ***cat /etc/config/rogueap // To check the "Rogue AP" configuration***
- ✓ ***cat /tmp/config/wids.conf***
- ✓ ***ps|grep light // To check if the WEB service is running***
- ✓ ***cat /etc/cert/serial // To check the serial of the certificate***
- ✓ ***ifconfig br-wan // To check the IP address configuration of AP***
- ✓ ***ssudo ping // To check the network connectivity***
- ✓ ***ssudo traceroute // To check the network trace route***

7 Stellar Hardware/Software limitations

Application support matrix:

AP1101	AP1101	AP1201	AP1201H AP1201L AP1261-RW-B AP1201HL	AP1220 Series	AP1230 Series	AP1251	AP1320 Series	AP1360 Series	AP1311	AP1301	AP1301H	AP1351
Application Visibility (DPI)	N	Y	N	Y	Y	Y	Y	Y	N(2)	N(2)	Y	Y
IoT Profiling	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
mDNS Edge	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Mesh/Bridge	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
WCF	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y

DPI is not supported for AP1311/AP1301 models

Restrictions on Mesh / Bridge AP

We support up to 8 slave APs, and the chain is up to 4 hops and the max AP number is up to 16 APs in a mesh network.
The WLAN limits is 5 with single frequency on mesh AP.
If AP works in bridge mode, it will not broadcast wireless signals.
Users can only change the channel of root A

Hardware Limit:

Hardware Limitation:												
	AP1101	AP1201	AP1201H AP1201L AP1201HL AP1261-RW-B	AP1220 Series	AP1230 Series	AP1251	AP1320 Series	AP1360 Series	AP1311	AP1351	AP1301	AP1301H
No of SSID max	7	7	7	7	7	7	7	7	7	7	7	7
No of VLANs max	16 VLAN	32 VLAN	16 VLAN	64 VLAN	64 VLAN	64 VLAN	64 VLAN	64 VLAN	64 VLAN	64 VLAN	64 VLAN	64 VLAN
No of Policy max	64	128	64	256	256	256	256	256	256	256	256	256
BLE Gw	N	Y	N	N	Y	N	Y	Y	Y	Y	Y	Y
Zigbee Gw	N	Y	N	N	N	N	Y	Y	Y	Y	Y	Y
LinkAgg	N	N	N	N	Y	N	Y	N	Y	Y	Y	N
WPA3	Y(1)	Y	Y(1)	Y	Y	Y	Y	Y	Y	Y	Y	Y

(1): AP1101 does not support WPA3_AES256 full band and AP1201H(L) does not support WPA3_AES256 on 2.4GHz band

Best practice recommendations:

Best practice recommendations:												
	AP1101	AP1201	AP1201H AP1201L AP1201HL AP1261-RW-B	AP1220 Series	AP1230 Series	AP1251	AP1320 Series	AP1360 Series	AP1351	AP1311	AP1301	AP1301H
No of SSID	4	5	4	5	5	5	5	5	5	5	5	5
No of VLANs	4	16	4	32	32	32	32	32	32	32	32	32
No of ARP	8	32	8	64	64	64	64	64	64	64	64	64
No of Policy	32	64	32	64	64	64	64	64	64	64	64	64
Multicast traffic (Mbps)	1Mbps	2Mbps	1Mbps 20Mbps for wired port	2Mbps	2Mbps	2Mbps	2Mbps	2Mbps	2Mbps	2Mbps	2Mbps	2Mbps

Note: the multicast traffic depends on interface in AP and it is recommended to enable the IGMP Snooping function incase of multicast scenario

8 Troubleshooting tips

8.1 AP PoE Powered and maximum consumption

AP Model	PoE Powered	Maximum power consumption (excluding USB, PoE PSE)
AP1101	802.3af	11.6W
AP1220	802.3at	15.6W,USB no load
AP1230	30.4W+/802.3at	27.6W,USB no load
AP1251	802.3af	11.8W
AP1201	802.3af	11W, Idle:4.1W
AP1201H	802.3af	11W,

8.2 LED behavior

AP has LED that is enabled and disabled by OS. Below is the reference definition:

Red	Blue	Green	Time Line	Status
ON			Power on	
ON			Bootloader-OS loading	System start up
Flash			System running	Network abnormal or connect management platform abnormal
		Flash	System running	Network normal, without SSIDcreated.
		ON	System running	Network normal, single band working, either 2.4Ghz or 5Ghzworking.
	ON		System running	Network normal, dual bands working, both 2.4Ghz and 5Ghz are working.
Flash	Flash		System running	Red and Blue LED alternate flashing; OS is upgrading.
Flash	Flash	Flash	System running	3 LEDs alternate flashing; Used for locating an AP.

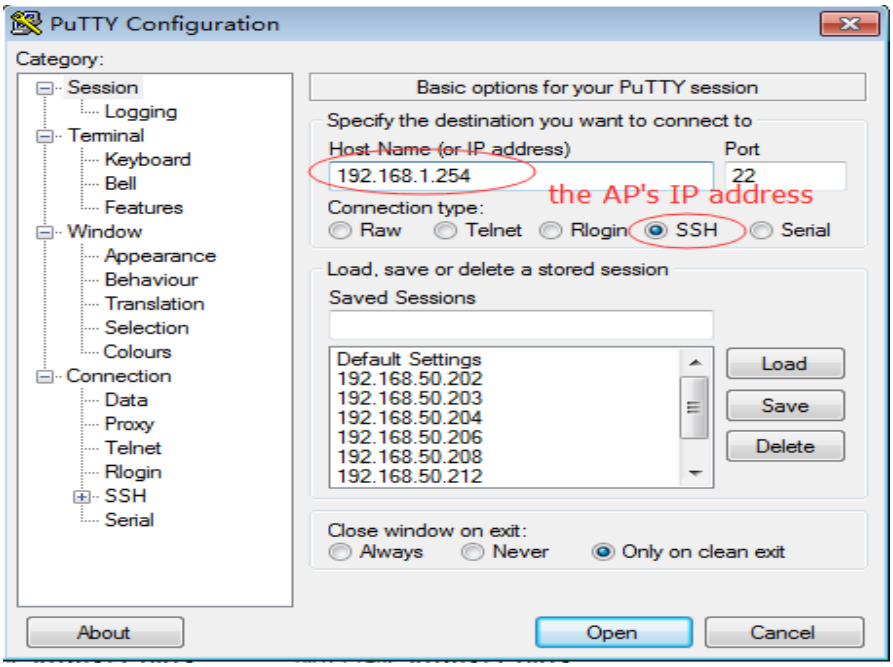
For AP1251:

SYS	2.4G	5G	ENET 0	ENET 1	RSRV 0	RSRV 1	Time Line	Status
ON							Power on	
ON							Bootloader-OS loading	System startup
Flash							System running	Bootloader-OS loading or upgrading
	ON						System running	2.4GHz SSID created and running
		ON					System running	5GHz SSID created and running
			ON				System running	Ethernet0 linkup
				ON			System running	Ethernet1 linkup
					Flash		System running	AP location
						Flash	System running	AP location

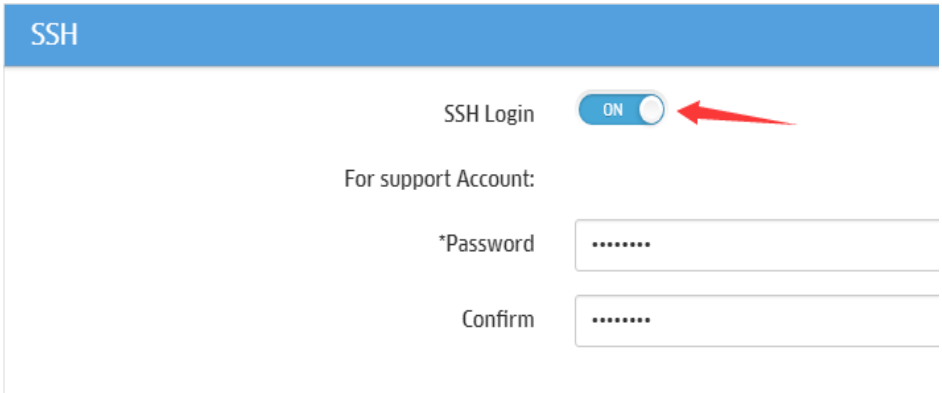
8.3 AP can not use ssh or console

Please refer to the following troubleshooting steps:

- Step1- If can't access AP by using SSH, please check the link according to the above steps, and check if the input IP address is correct.



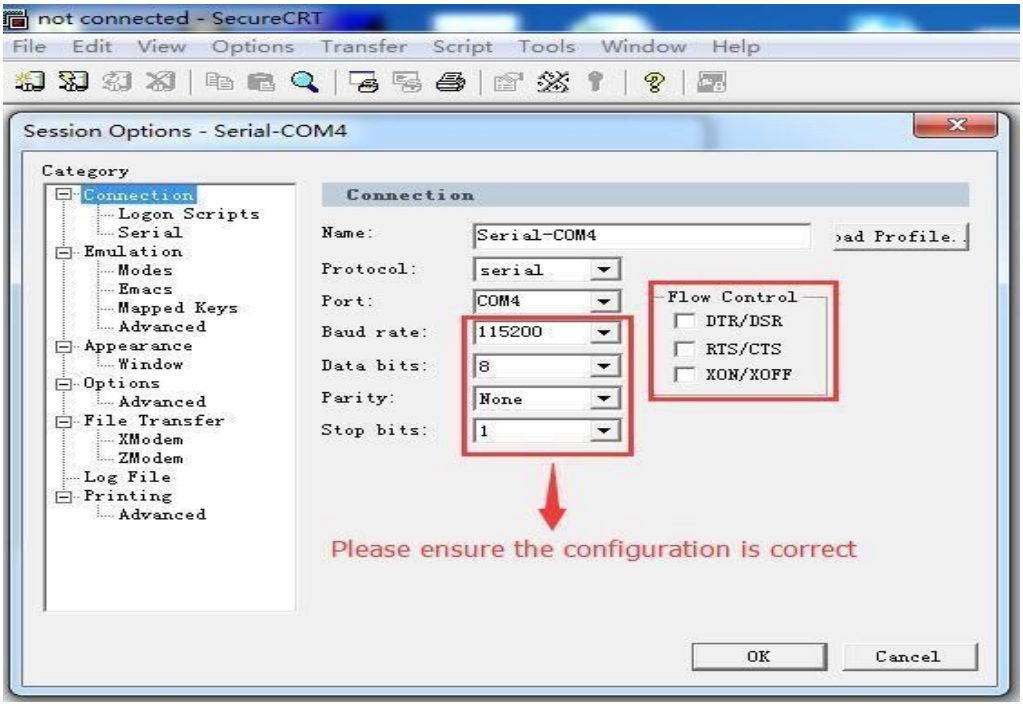
- Step2- login OV page, Home -> Network -> AP Registration -> AP Group, Check whether have configured the SSH enable for the ap group on OV



- Step3- If you can Login AP via console, please cat file /var/config/public_group.conf as below, check whether configuration applied to AP successfully.

```
support@AP-D1:40:~$ cat /var/config/public_group.conf
{
        "Public_group":{
                "rootpasswd":"e06adf968d90e16c81116abd43637b2a",
                "hanlet_enable":"1",
                "passwd":"29748b46859953c153c7533582ce41b5",
                "ssh_connect":"1"    //1 means ssh connection are enabled
        }
}
```

- Step4- If can't access AP using console, please check if the serial port and serial port line is intact, and check the configuration.



8.4 AP fails to get IP Address

Stellar AP supports from the DHCP server to obtain an IP address or manually configure a static IP address, The DHCP server can be normal DHCP server, if AP cannot get an IP address successfully, please troubleshoot by the following steps:

- Step1- Please login AP via console, and using command "cat /etc/config/network" to check the "option proto", AP will not get IP address from DHCP server if the proto is "static", there are 2 ways to resolve this case:
    a. Reset AP to factory settings by Reset button or command "ssudo firstboot & ssudo reboot"
    b. Login AP GUI by default IP (192.168.1.254) or it's static IP and change the IP address to "dhcp" from "static".

```
support@AP-C1:30:~$
support@AP-C1:30:~$ cat /etc/config/network

config interface 'loopback'
        option ifname 'lo'
        option proto 'static'
        option ipaddr '127.0.0.1'
        option netmask '255.0.0.0'

config globals 'globals'
        option ula_prefix 'fd66:ce37:fd0b::/48'

config interface 'wan'
        option ifname 'eth0'
        option type 'bridge'
        option proto 'dhcp'
support@AP-C1:30:~$
```

- Step2- If AP is still cannot get an IP from DHCP server after step1, please capture the DHCP messages on uplink port and check the DHCP process,

  Below are the right DHCP messages:

72	16.632951	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover
75	17.641445	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer
79	18.644668	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request
80	18.655769	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK

  If the DHCP messages are shown in the following picture, please check the link between the AP and DHCP server and the configuration of DHCP server:

595	7.235257	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover
854	10.236261	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover
1111	13.236666	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover
1364	16.239761	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover
1604	19.241430	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover
1860	22.242980	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover
2128	25.244693	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover
2384	28.245439	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover

- Step3- Please also check if DHCP server send DHCP-NAK packet in case of AP request an IP address that out of DHCP pool.

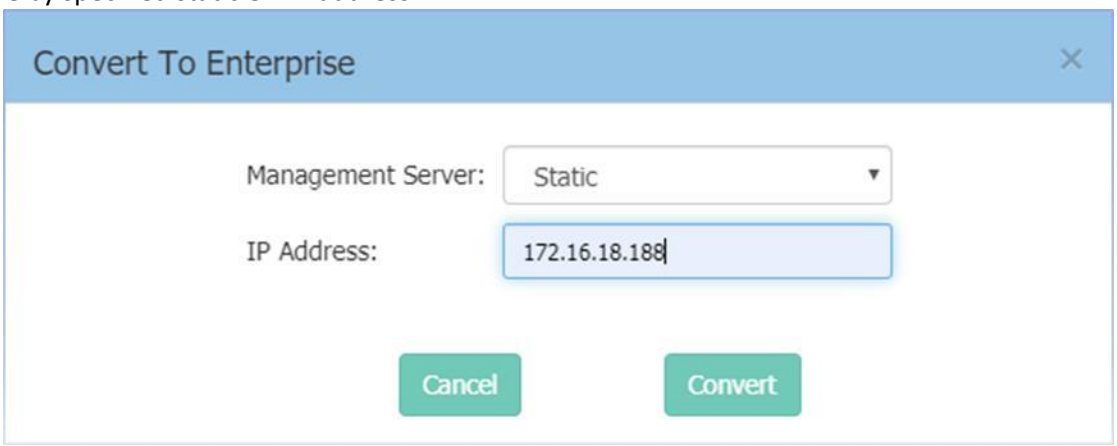
3	2.404003	0.0.0.0	255.255.255.255	DHCP	367	DHCP Request
4	2.411379	192.168.0.1	255.255.255.255	DHCP	590	DHCP NAK
5	3.422078	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover
6	3.429311	192.168.0.1	255.255.255.255	DHCP	590	DHCP Offer
7	3.429628	0.0.0.0	255.255.255.255	DHCP	373	DHCP Request
8	3.441291	192.168.0.1	255.255.255.255	DHCP	590	DHCP ACK

8.5 AP cannot register to OV 2500

There are 2 ways to let AP register to local OV

a) AP get OV ip address through option 138/43 field of DHCP and register to OV

b) On cluster mode ,there is an option “Convert To Enterprise” under AP configuration page ,AP can be convertto OV mode by specified static OV IP address



If AP cannot register to local OV successfully ,please do the troubleshooting by the follow steps:

- Step1- please using the “getmode” command to check if AP worked on “OV” mode. If it displayed as “CLUSTER”, please configure OV IP address in the option 138/43 field of DHCP server and then “firstboot” & “reboot” the AP. If it displayed as “OV”, please go to step2.

```
support@AP-C4:50:~$
support@AP-C4:50:~$
support@AP-C4:50:~$ getmode
CLUSTER
support@AP-C4:50:~$
support@AP-C4:50:~$
```

It should be “OV” mode

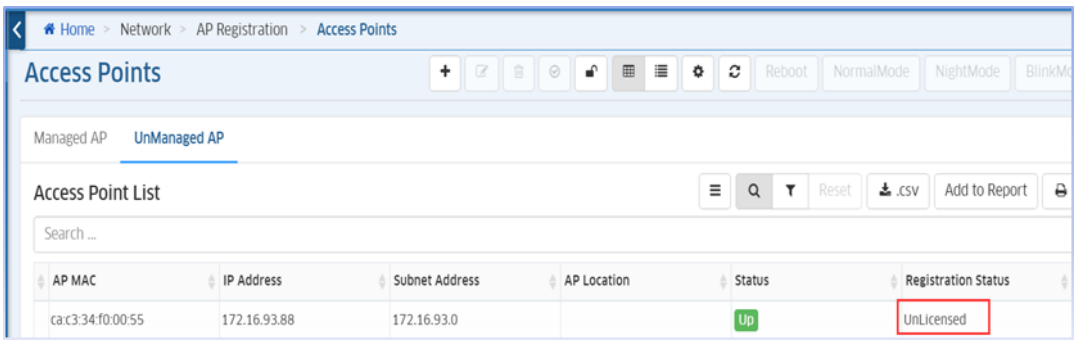
- Step2- Please using the “getovinfo” command to check whether OV IP is right. If the OV IP is't right, please update OV IP address in the option 138/43 field of DHCP server and then reboot AP.If the OV IP is correct, please go to setp3.

```
support@AP-C4:50:~$
support@AP-C4:50:~$ getovinfo
172.16.18.188
support@AP-C4:50:~$
support@AP-C4:50:~$
support@AP-C4:50:~$
```

- Step3- Please be make sure the route between AP IP and OV IP is reachable.

```
support@AP-C4:50:~$
support@AP-C4:50:~$ ssudo ping 172.16.18.188
PING 172.16.18.188 (172.16.18.188): 56 data bytes
64 bytes from 192.168.10.6: seq=0 ttl=63 time=1.601 ms
64 bytes from 192.168.10.6: seq=1 ttl=63 time=1.317 ms
64 bytes from 192.168.10.6: seq=2 ttl=63 time=1.349 ms
64 bytes from 192.168.10.6: seq=3 ttl=63 time=1.372 ms
64 bytes from 192.168.10.6: seq=4 ttl=63 time=1.327 ms
^C
--- 172.16.18.188 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.317/1.393/1.601 ms
support@AP-C4:50:~$
```

- Step4- If the Registration Status displays “unLicensed”.please check license count. If license count full, please import new sufficient license and then reboot AP



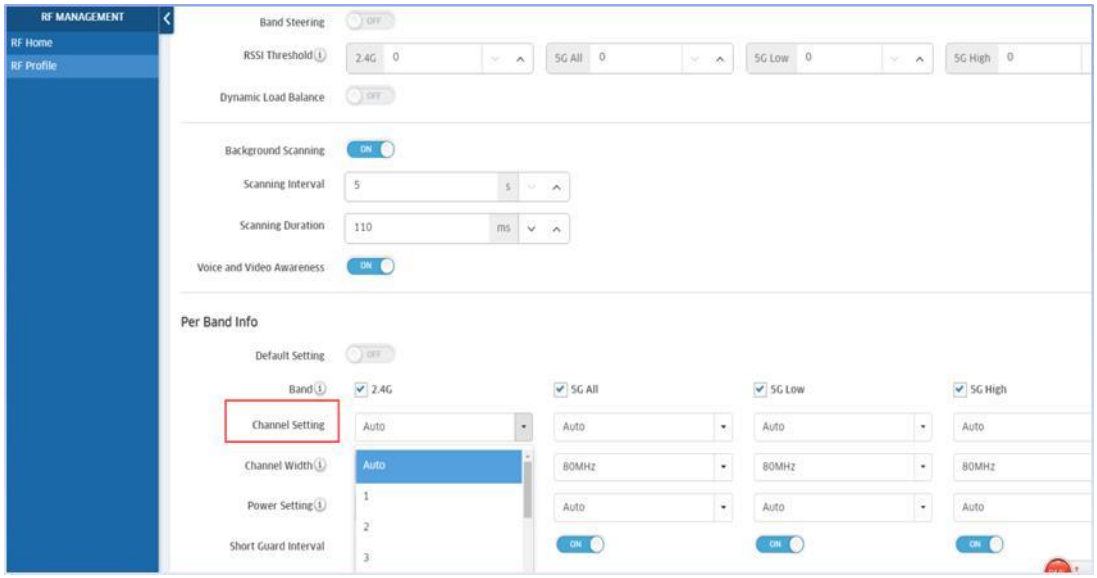
8.6 Client does not see the SSID Broadcasted

APs support broadcasting SSID on 2.4G and 5G bands. The WLAN signal can be scanned by clients, if the client cannot see the configured SSID, please check as below steps:

- Step1-Please check the wireless interface status on AP by using command “iwconfig”, if there is no corresponding interface, it may be caused by the wrong configuration, please check whether the WLAN configuration is applied successfully or the RF/SSID configuration is disabled.

```
root@AP-57:40:~# iwconfig
gre0      no wireless extensions.

ath11-untag  no wireless extensions.

br-wan    no wireless extensions.

wifi0     no wireless extensions.

ath02-untag  no wireless extensions.

ath02     IEEE 802.11ng  ESSID:"Test-SSID"
          Mode:Master  Frequency:2.462 GHz  Access Point: 34:E7:0B:10:57:42
          Bit Rate:192 Mb/s   Tx-Power=17 dBm
          RTS thr:off   Fragment thr:off
          Encryption key:8B37-CC5C-4B7B-B3D6-2C6C-CE0B-BFB2-E34D-50FC-DDBE-77A0-54AA-39BE-A330-
          Power Management:off
          Link Quality=34/94  Signal level=-81 dBm  Noise level=-95 dBm
          Rx invalid nwid:5  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

- Step2- If all the configuration is correct, it might be the AP works on a channel which clients do not supported, for example, the client only worked on 2.4G band and the AP only worked on 5G band ,
- Step3- The clients don’t support the channel that AP worked on, please check if AP configured incorrect Country Code which clients do not supported. Also, if the client do not support the channel if the country code iscorrect, the workaround is to set the channel manually on AP.



8.7 Client fails to get IP Address

Wireless clients can get IP address from DHCP server or manually configure a static IP address, Stellar AP will forward the DHCP packets also it can be a DHCP server, if AP cannot get an IP address successfully, please troubleshoot by the following steps:

- Step1- Please capture DHCP messages on the client and AP. Please use “cd /tmp” and “tcpdump -i eth0 - s0 -w X.pcap” command to capture the DHCP messages,and send the “X.pcap” to the tftp server using “tftp -pl X.pcap xx.xx.xx.xx(tftp server IP address)”,then open the “X.pcap” using tools wireshark.

  Below are the right DHCP messages:

413	34.714286	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x43630c33
414	34.715614	192.168.10.254	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x43630c33
415	34.767082	0.0.0.0	255.255.255.255	DHCP	354	DHCP Request - Transaction ID 0x43630c33
416	34.768528	192.168.10.254	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x43630c33

- Step2- If the DHCP messages were incomplete, and if the DHCP messages captured on the AP is same as the DHCP messages of client. Please log in AP and run command “ssudo sta_list”, check the access role and vlanid as below, whether the wrong role or vlanID configured.

```
support@AP-57:40:~$
support@AP-57:40:~$ ssudo sta_list
SSID:Test-SSID
STA_MAC                IP            OnlineTime    RX        TX       FREQ   AUTH    Final_role        VLANID
SSID:Test-SSID
STA_MAC                IP            OnlineTime    RX        TX       FREQ   AUTH    Final_role        VLANID
34:f3:9a:ab:79:30   172.16.108.108      32        137829   246457    5GHz   PSK       v108            108
```

- Step3- Run cmd “brctl show”,check if the ath interface in the correct br-vlan as below:

```
support@AP-57:40:~$ brctl show
bridge name     bridge id               STP enabled     interfaces
br-wan          7fff.34e70b105740       no              eth0
                                                        ath01-untag
                                                        ath11-untag
                                                        ath02-untag
                                                        ath12-untag
br-vlan108              7fff.34e70b105740       no              ath01-108
                                                        ath02-108
                                                        ath11-108
                                                        ath12-108
                                                        eth0-108
support@AP-57:40:~$
```

8.8 Syslog messages are not received on the Syslog server

OV can configure the AP to send the syslog to remote syslog server. If the server does not receive any syslog, pleasecheck as below steps:

- Step1- :Login AP, and check if the configuration applied to AP correctly ,by using command /var/config/syslog.conf as below:

```
support@AP-57:40:~$
support@AP-57:40:~$ cat /var/config/syslog.conf
{
        "SysLog":{
                "log_remote":1,
                "log_ip":"172.16.10.174",
                "log_port":514,
                "log_priority":"LOG_NOTICE"
        }
}
support@AP-57:40:~$
```

- Step2- Run cmd “ps |grep SYSLOG SERVER IP” to check if the process works, as below:

```
support@AP-57:40:~$
support@AP-57:40:~$
support@AP-57:40:~$ ps |grep 172.16.10.174
  911 root      1156 S    /sbin/logread -f -r 172.16.10.174 514 -p /var/run/lo
18462 support   1352 S    grep 172.16.10.174
support@AP-57:40:~$
support@AP-57:40:~$
```

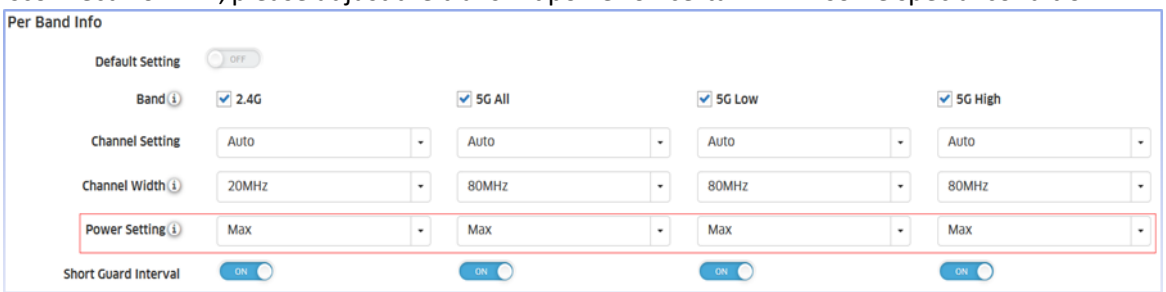
- Step3- Use the command: logger -p emerg “_GOLSOH_Just for test!” , this command will send a syslog packet to syslog remote server at once, and you can confirm whether the process is working

```
support@AP-57:40:~$
support@AP-57:40:~$
support@AP-57:40:~$ logger -p emerg  "_GOLSOH_Just for test!"
support@AP-57:40:~$
```

8.9 Wireless client frequently disconnects from the AP

If users frequently disconnect WLAN, please check the following steps:

- Step1- SSH or Console to AP check whether the transmit power is too low on AP, Generally, the transmit power of the clients is lower than AP, if there is a large attenuation between AP and clients , this may cause clients disconnect from AP, please adjust the transmit power on certain AP in some special condition.



- Step2- Please check if higher RSSI Threshold was configured, if the RSSI Threshold is too high, it may cause the clients disconnection which far away from AP, please adjust the RSSI Threshold(Home>WLAN>RF Management>RF Profile)on OV management page.

```
support@AP-BB:60:~$ cat /tmp/config/rfprofile.conf
{
        "RFService":[
                {
                        "bandSteering":"disable",
                        "LoadBalance":"disable",
                        "backgroundScanning":"enable",
                        "countryCode":"CN",
                        "scanningInterval":5,
                        "scanningDuration":110,
                        "voiceVedioAwareness":"enable",
                        "perBandInfo":{
                                "2.4G":{
                                        "band":"enable",
                                        "channelSetting":"AUTO",
                                        "channelWidth":20,
                                        "powerSetting":"30",
                                        "shortGuardInterval":"enable",
                                        "signalStrengthThreshold":80,
                                        "channelLists":[],
                                        "powerValMax":-1,
                                        "powerValMin":-1
                                },
                                "5G_high":{
                                        "band":"enable",
                                        "channelSetting":"AUTO",
                                        "channelWidth":80,
                                        "powerSetting":"AUTO",
                                        "shortGuardInterval":"enable",
                                        "signalStrengthThreshold":80,
                                        "channelLists":[],
                                        "powerValMax":-1,
                                        "powerValMin":-1
                                },
```

- Step3- If all the configurations are correct, please capture the wireless packets and check if AP deny the clients or client send deauth/disassociation to AP, meanwhile ,please collect the logs on AP to see the specific information.

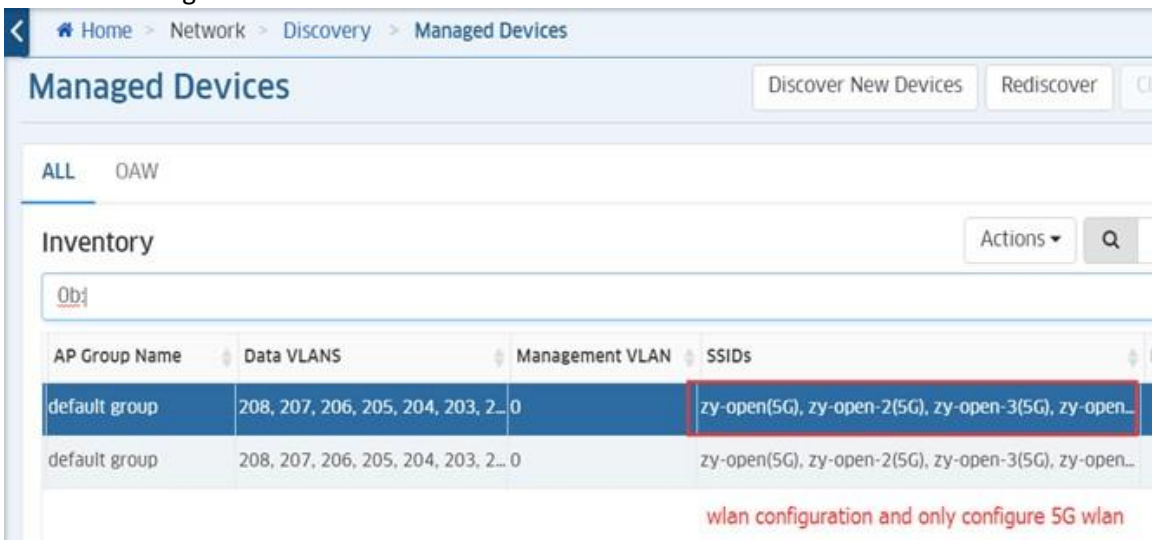
8.10 AP is not seen in the OV Heatmap

If AP has Wireless interface, AP can transmit signal and then generate the heat-map on OV, if there is no HEAT-MAP displayed on OV, please check as following steps:

- Step1-If there is no wireless interface on AP, it will not generate HEAT-MAP correctly, please using command “iwconfig” to check whether AP has Wireless interface.

```
support@AP-57:40:~$
support@AP-57:40:~$ iwconfig
gre0      no wireless extensions.

eth0-108  no wireless extensions.

ath02-108  no wireless extensions.

br-wan    no wireless extensions.

wifi0     no wireless extensions.

ath02-untag  no wireless extensions.

ath02     IEEE 802.11ng  ESSID:"Test-SSID"
          Mode:Master  Frequency:2.462 GHz  Access Point: 34:E7:0B:10:57:42
          Bit Rate:192 Mb/s   Tx-Power=17 dBm
          RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality=15/94  Signal level=-87 dBm  Noise level=-95 dBm
          Rx invalid nwid:4918  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

- Step2- If AP RF configuration or WLAN configuration only configure the 5G, but heat-map page select only 2.4G,it can't generate heat-map, vice versa, please check AP whether WLAN configuration correspond to signal option of heat-map.
  - Check AP wlan configuration



  - Check the signal option of heat-map

8.11 Troubleshooting Mesh AP and Bridge AP

If you have problems forming a mesh, please refer to the following limitation factor:

- ✓ All AP can only work in 2.4G or 5G. If you want to establish a mesh network between APs, you must ensure that the two APs work in the same frequency band. The SSID must be the same and the encryption passwords must be the same.
- ✓ The mesh AP directly connects to 8 slave AP, and the chain is up to 4 hops in the mesh network, supports up to16 AP in a mesh network.
- ✓ The WLAN limits is 5 with single frequency on mesh AP. If work in bridge mode, do not broadcast wireless signals.
- ✓ User can only change the channel of root AP
- ✓ Mesh AP in a group, you can see the topology. If in different groups, there will be an external flag and see thetopology in the physical topology.

The command about MESH as the following:

- ✓ Check the mesh configuration, root AP and slave AP are same. Via the command: cat /etc/config/mesh

```
        "mesh":[
                {
                        "enable":"Yes",
                        "meshMode":"Mesh",
                        "is_root":"Yes",
                        "essid":"lln-mesh-5G",
                        "band":"5G",
                        "passphrase":"a83f6faa547f31ac983de7a6f0970961"
                }
        ]
}
support@AP-C1:20:~$
```

- ✓ Check the uplink interface of the root AP. Via the command : iwconfig athap1(If it is 2.4G with athap0, if it is 5G with aathap1)

```
support@AP-C1:20:~$ iwconfig athap1
athap1    IEEE 802.11ac  ESSID:"lln-mesh-5G"
          Mode:Master  Frequency:5.825 GHz  Access Point: 34:E7:0B:03:C1:2A
          Bit Rate:312 Mb/s   Tx-Power=23 dBm
          RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality=94/94  Signal level=-44 dBm  Noise level=-95 dBm
          Rx invalid nwid:91594  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

support@AP-C1:20:~$
```

- ✓ Check the downlink interface of the slave AP. Via the command : iwconfig athsta1(If it is 2.4G with athsta0, if it is 5G with aathsta1)

```
support@AP-30:D0:~$ iwconfig athsta2
athsta2   IEEE 802.11ac  ESSID:"lln-mesh-5G"
          Mode:Managed  Frequency:5.825 GHz  Access Point: 34:E7:0B:03:C1:2A
          Bit Rate:156 Mb/s   Tx-Power=3 dBm
          RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality=94/94  Signal level=-20 dBm  Noise level=-95 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

support@AP-30:D0:~$
```

- ✓ Further check the scan log from the AP. Via the command: cat /tmp/wpa.log

```
1562315193.171322: driver_atheros_event_wireless: scan result event - SIOCGIWSCAN
1562315199.956115: driver_atheros_event_wireless: scan result event - SIOCGIWSCAN
1562315201.852957: driver_atheros_event_wireless: scan result event - SIOCGIWSCAN
1562315206.606240: driver_atheros_event_wireless: scan result event - SIOCGIWSCAN
1562315206.606816: athsta1: Trying to associate with 34:e7:0b:03:ce:39 (SSID='SYY-MESH-C' freq=5280 MHz)
1562315209.119119: athsta1: Associated with 34:e7:0b:03:ce:39
1562315209.143157: athsta1: WPA: Key negotiation completed with 34:e7:0b:03:ce:39 [PTK=CCMP GTK=TKIP]
1562315209.143295: athsta1: CTRL-EVENT-CONNECTED - Connection to 34:e7:0b:03:ce:39 completed [id=0 id_str=]
1562315213.745792: driver_atheros_event_wireless: scan result event - SIOCGIWSCAN
support@AP-34:90:~$
```

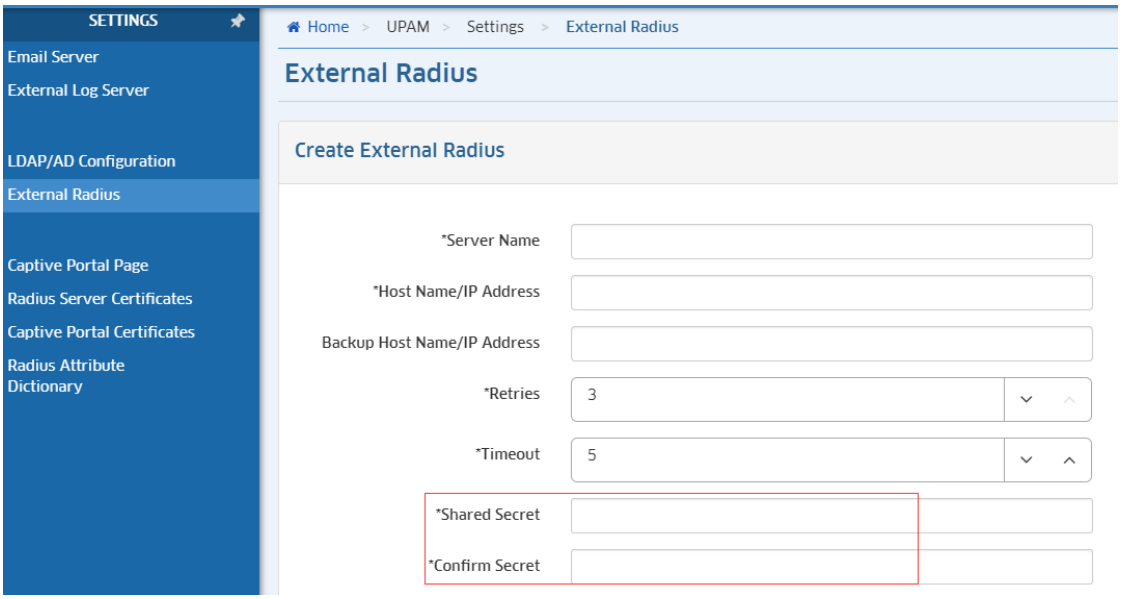
- ✓ You can check the AP connected in the ssudo sta_list and determine whether it is a downlink AP or a wireless client based on the MAC address

```
support@AP-CE:30:~$ ssudo sta_list
SSID:SYY-MESH-C
STA_MAC                IPv4            IPv6                    OnlineTime        RX        TX
ELID  FARENDIP
dc:08:56:00:34:a1  0.0.0.0                                       170041          81422591
34:e7:0b:02:be:79  0.0.0.0                                       170131          94441878
support@AP-CE:30:~$
```

8.12 Troubleshooting multiple external Radius Servers

Multiple External Radius is a new feature of UPAM, users can add 8 external radius at the most, if users select external radius as authentication server and auth failed, please check as the following steps:

- ✓ Step1- AP in OV or OVC mode, user can set external radius as the following link (shown as the picture). Users shouldkeep the secret same as user external radius server.

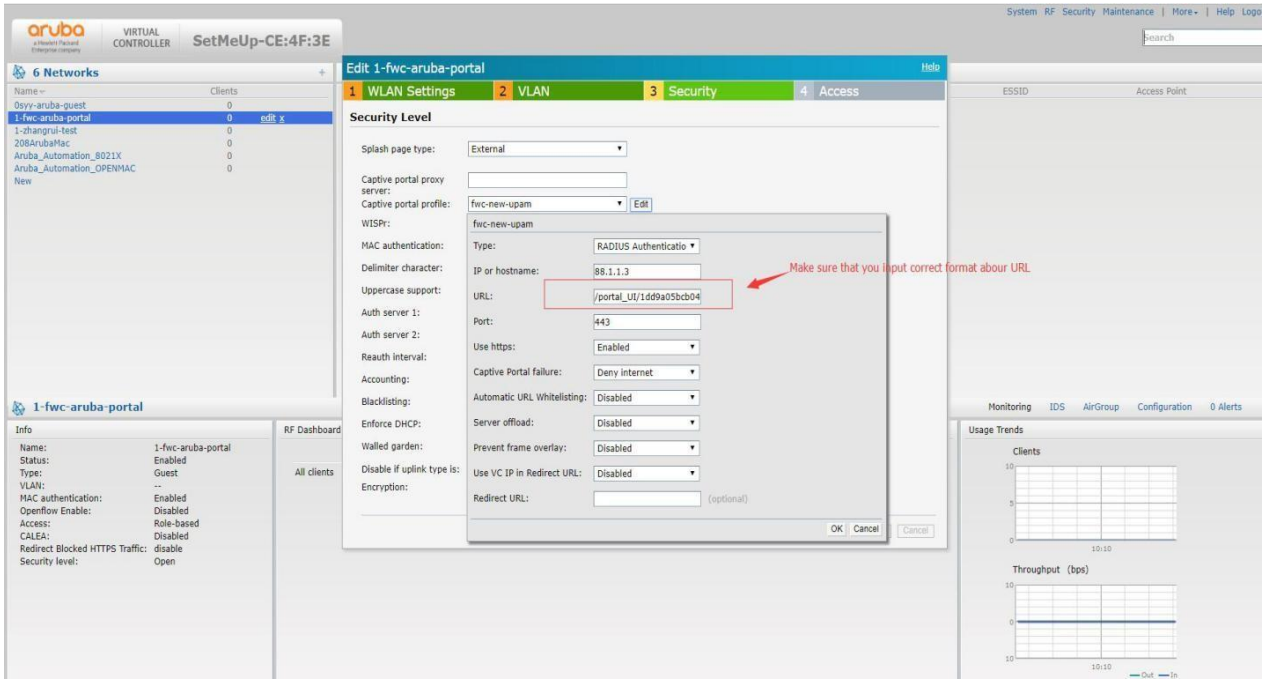


- ✓ Step2- Keep the network between AP and the external radius is reachable. For example, if users use free radius as the external radius, users should add the AP’s IP in client of free radius.
- ✓ Step3- AS for username, UPAM is case insensitive. But for freeradius is case sensitive.

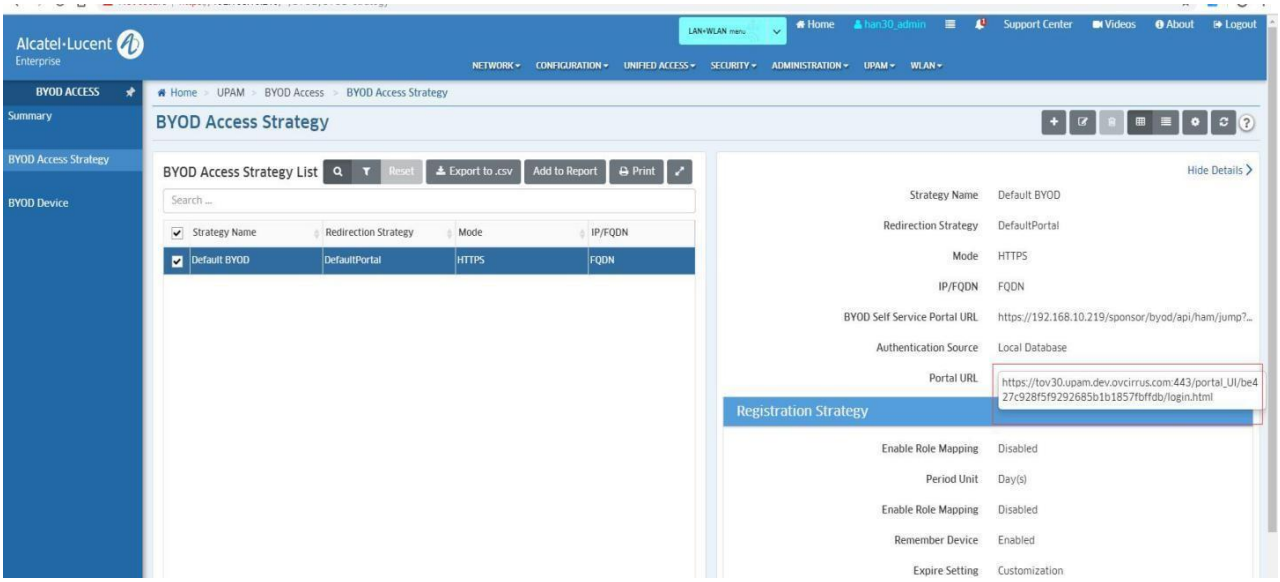
8.13 Captive Portal is not accessible

- ✓ Step1- Please make sure your client can ping successfully to portal IP.
- ✓ Step2- If it is OK, please check your client’ IP configuration. Whether it has DNS IP address, if not, please set it.
- ✓ Step3- If everything is OK as above, every Guest/BYOD access strategy from UPAM has unique portal URL. When configure portal authentication for Aruba AP, please ensure your portal URL whether is right. If change different Guest/BYOD access strategy from UPAM, then you need to input corresponding portal URL to Aruba configuration.

Aruba configuration about URL as below:



You can copy the URL from UPAM which you configured strategy as below:
https://ov2500-upam-cportal.al-enterprise.com:443/portal_UI/be427c928f5f9292685b1b1857fbffdb/login.html
Just copy red part from it.



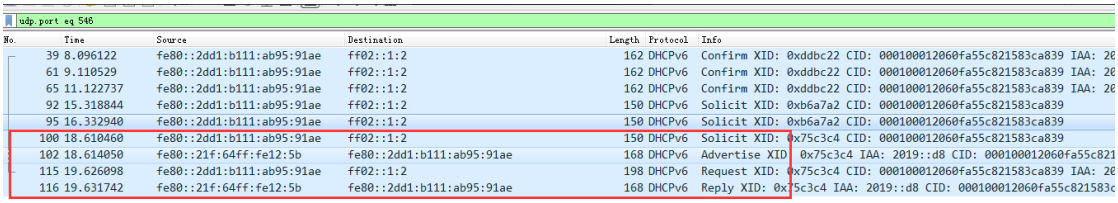
8.14 UPAM Guest Strategy

The account you created is not available. Please note whether the OVC or OVE has configured the time zone and time when installing. If the configured time does not correspond to the actual time, the account you created will be expired.

8.15 IPv6 clients can't launch Captive Portal page

- ✓ Step1- The OVE mode should configure a IPv6 address for UPAM. The IPv6 address should be reachable with the client address.
- ✓ Step2- Whether the client get the ipv6 address. If not, you should check your network environment. Capture thepackage on the side of the client. Check whether the client receive the reply.

  The DHCPv6 include four packages: Solicit、Advertise、Request、Reply



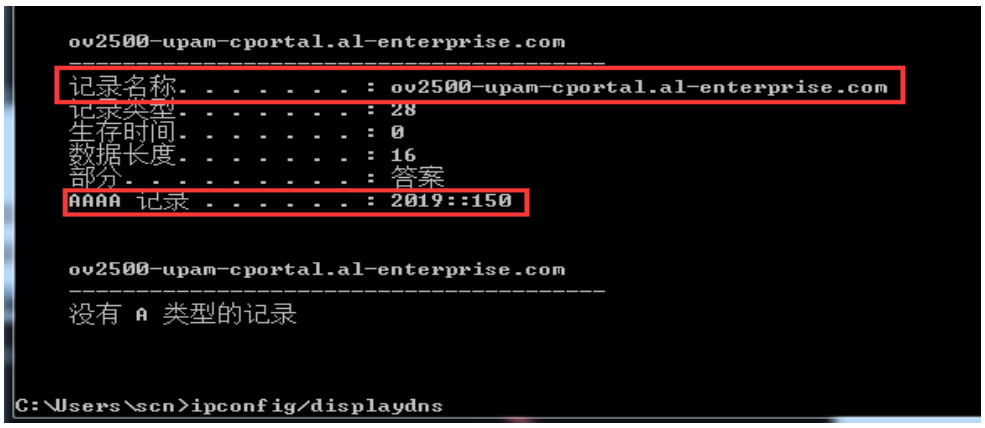
udp.port eq 546

No.	Time	Source	Destination	Length	Protocol	Info
39	8.096122	fe80::2dd1:b111:ab95:91ae	ff02::1:2	162	DHCPv6	Confirm XID: 0xddbc22 CID: 000100012060fa55c821583ca839 IAA: 20
61	9.110529	fe80::2dd1:b111:ab95:91ae	ff02::1:2	162	DHCPv6	Confirm XID: 0xddbc22 CID: 000100012060fa55c821583ca839 IAA: 20
65	11.122737	fe80::2dd1:b111:ab95:91ae	ff02::1:2	162	DHCPv6	Confirm XID: 0xddbc22 CID: 000100012060fa55c821583ca839 IAA: 20
92	15.318844	fe80::2dd1:b111:ab95:91ae	ff02::1:2	150	DHCPv6	Solicit XID: 0xb6a7a2 CID: 000100012060fa55c821583ca839
95	16.332940	fe80::2dd1:b111:ab95:91ae	ff02::1:2	150	DHCPv6	Solicit XID: 0xb6a7a2 CID: 000100012060fa55c821583ca839
100	18.610460	fe80::2dd1:b111:ab95:91ae	ff02::1:2	150	DHCPv6	Solicit XID: 0x75c3c4 CID: 000100012060fa55c821583ca839
102	18.614050	fe80::21f:64ff:fe12:5b	fe80::2dd1:b111:ab95:91ae	168	DHCPv6	Advertise XID: 0x75c3c4 IAA: 2019::d8 CID: 000100012060fa55c821
115	19.626098	fe80::2dd1:b111:ab95:91ae	ff02::1:2	198	DHCPv6	Request XID: 0x75c3c4 CID: 000100012060fa55c821583ca839 IAA: 20
116	19.631742	fe80::21f:64ff:fe12:5b	fe80::2dd1:b111:ab95:91ae	168	DHCPv6	Reply XID: 0x75c3c4 IAA: 2019::d8 CID: 000100012060fa55c821583c

- ✓ Step3- Check the URL on the AP. The command is 'ssudo wam_debug sta_list'.If the URL is right, then turn to thenext step.


```
"iface": "ath13",
"ssid": "scn-guest",
"freq": "5GHz",
"security": "Open",
"wlanService": "scn-guest",
"staData": [
    {
        "staMAC": "c8:21:58:3c:a8:39",
        "staIP": "172.16.53.10",
        "staGlobalIPv6": "2019::38",
        "staLocalIPv6": "fe80::2dd1:b111:ab95:91ae",
        "associationTime": 18,
        "mappingType": 0,
        "assignedVLAN": 0,
        "assignedAR": "__scn-guest",
        "assignedPL": "",
        "macAuthResult": "SUCCESS",
        "ARFromMACAuth": "",
        "PLFromMACAuth": "",
        "redirectURLFromMACAuth": "https:\/\/ov2500-upam-cportal.al-enterprise.com:443\/portal_UI\/b8c7fb2450b6e8ff9946a07f0fabc23e\/l
gin.html?mac=C821583CA839",
        "ARFrom8021xAuth": "",
        "PLFrom8021xAuth": "",
        "redirectURLFrom8021xAuth": "",
        "CPAuthResult": "FAILED",
        "ARFromCPAuth": "",
        "PLFromCPAuth": "",
        "ARFromRoaming": "",
        "PLFromRoaming": "",
        "redirectURLFromRoaming": "",
        "classificationMatched": "none"
    }
```

✓ Step4- Check the DNS on the client-side. If the URL and IPV6 address is right, then turn to next step. If not, then thereare some problems about the DNS on AP.

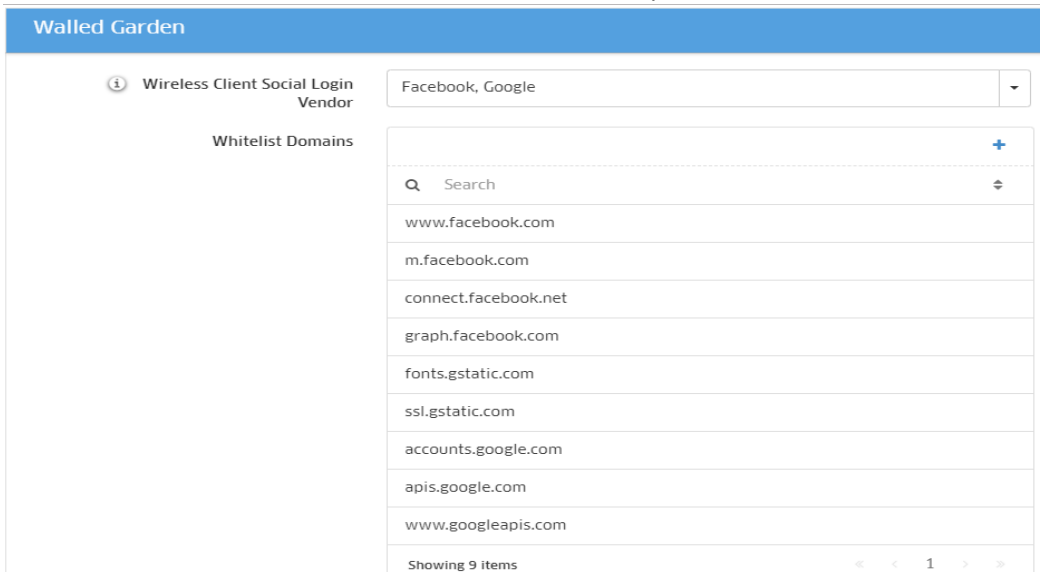


Step5- Manually enter the URL to see if it can push out the portal page. If it cannot launch, then there are some problemson the OV-UPAM.

8.16 The Google or Facebook login page cannot be loaded

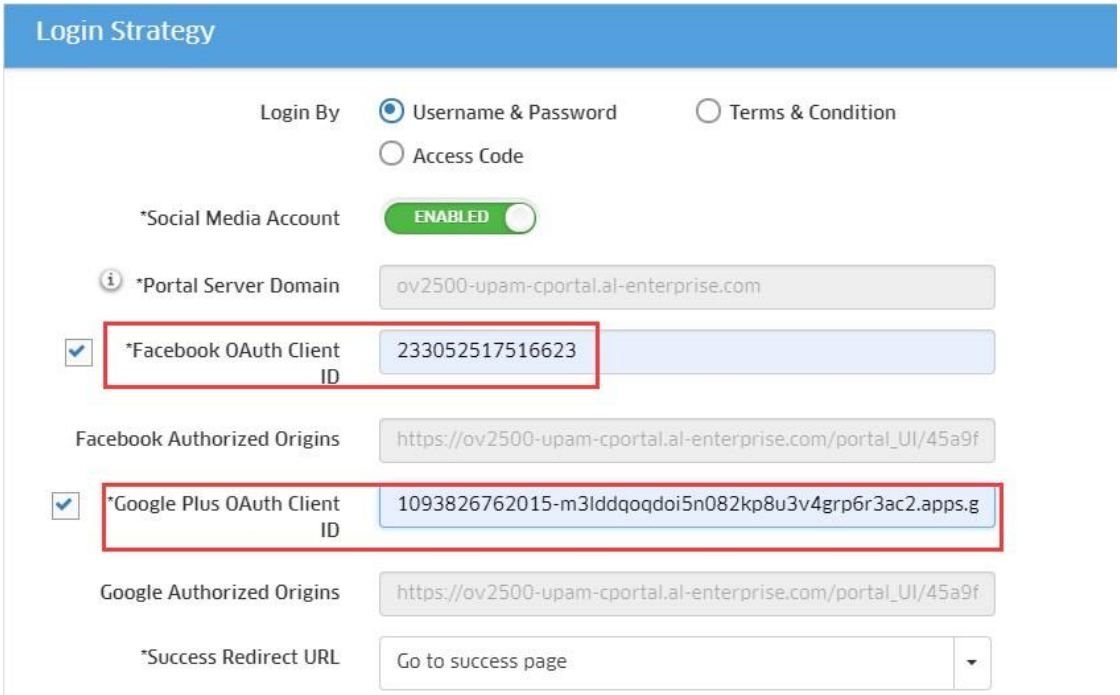
✓ Step1- First check if the domains of Google and Facebook had been added to Walled garden.

Path: Home -> Unified Access -> Unified Profile -> Template -> Access Role Profile



There are 9 default domains of Google and Facebook. When the domains change, you can press F12 or capture the package of client-side to view the domains cannot be loaded. Then adding them to the Walled garden.

✓ Step2- Then check the OAuth Client ID



There are detailed configuration steps in the help information. Checking whether the fill information on Google or Facebook API is consistent with the OV environment.

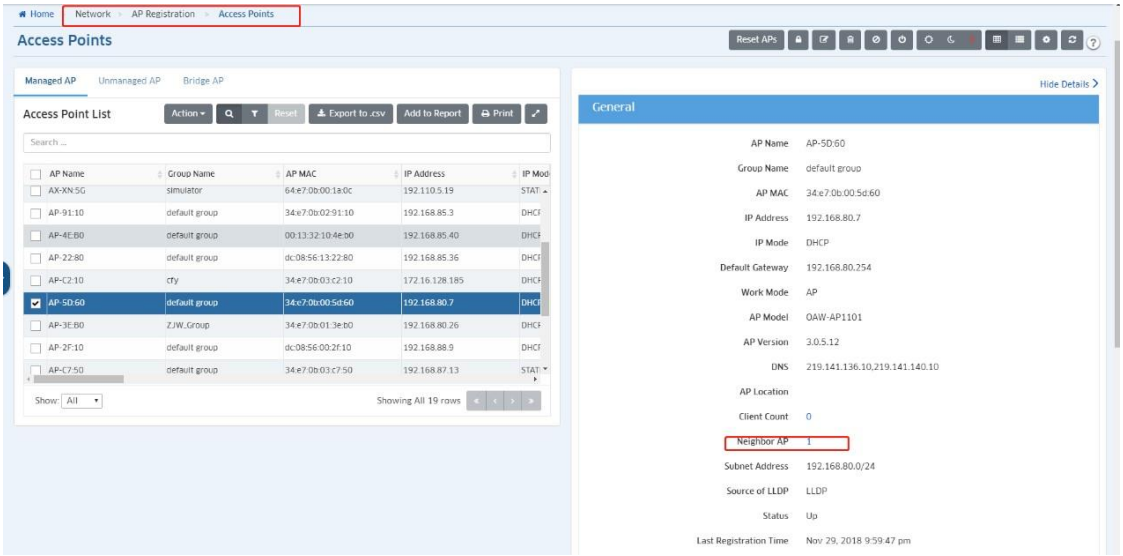
8.17 Reasons for roaming failure

L2 Roaming

- ✓ The L2 OKC roaming/L2 802.11r roaming/L2 portal roaming/L3 roaming need APs are neighbors with each other.
- ✓ Our AP do not support roaming from untagged VLAN to tagged VLAN.
- ✓ RSSI is too low when you are roaming between source AP and destination AP.

L3 Roaming

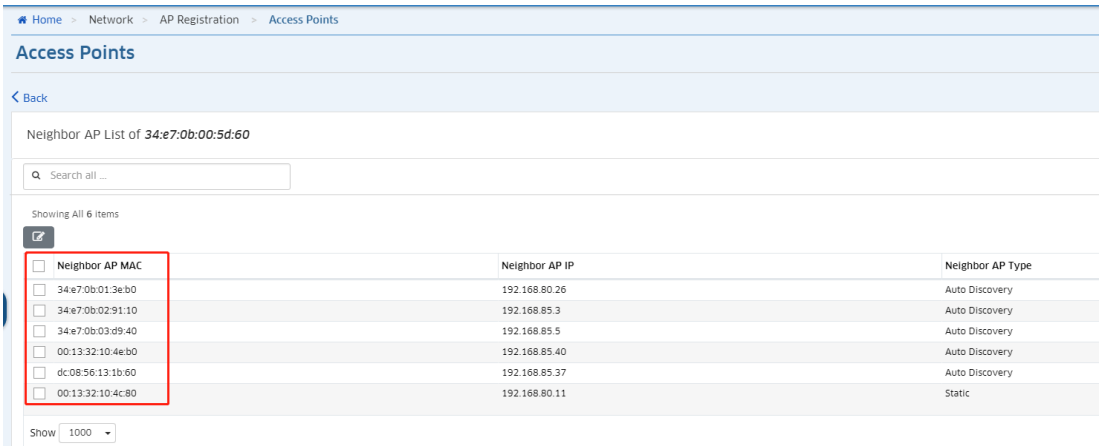
- ✓ Step1- Go to the Unified Access->Unified Profile->Device Config ->Access Role Profile. Click add AP Group and check your source AP and destination AP to make sure which one is “Untagged VLAN”.



If your source AP is configured with untagged VLAN, you will not connect to network after L3 roaming. It is normally

because of safety assurance. When clients roaming from untagged VLAN to tagged VLAN, we do not want clients to visit the management VLAN on source AP from destination AP.

✓ Step2- If your source AP and destination AP all with tagged VLAN, please check your source AP and destination AP whether they are neighbors with each other like below:



8.18 How to check roaming is successful

You can check your roaming whether succeed like below:

✓ Step1- Check your wam.log

1. OKC roaming you can get log like below. If log OKC passed is printed, the roaming is successful.

```
1552887466.535022: _GOLSOH_[ lina-K3-OKC roaming-wlan @ ath11 ]: STA 00:01:3e:3d:4a:e8 - L3 roaming - start, home ap 172.16.23.100
1552887466.536933: _GOLSOH_[ lina-K3-OKC roaming-wlan @ ath11 ]: found STA <00:01:3e:3d:4a:e8> roaming context in current AP, home AP MAC dc:08:56:44:45:60, ip address 172.16.23.100, access role lina-roaming, origin VLAN ID 208,porta
Auth not pass
1552887466.547683: Custom wireless event: 'Manage.assoc_req 184'
1552887466.547963: atheros_raw_receive: subtype 0x2 len 184
1552887466.548345: ath11: Event ASSOC (0) received
1552887466.549544: _GOLSOH_[ lina-K3-OKC roaming-wlan @ ath11 ]: Receive STA <00:01:3e:3d:4a:e8> 80211 reassoc event
1552887466.550652: _GOLSOH_[ lina-K3-OKC roaming-wlan @ ath11 ]: STA <00:01:3e:3d:4a:e8> included RSN IE in (Re)AssocReq frame
1552887466.550835: ieee8021x acct stop syslog not configured
1552887466.551627: [ lina-K3-OKC roaming-wlan @ ath11 ]: recv sta assoc frame, reassoc 1
1552887466.551832: RSN IE: STA PMKID - hexdump(len=16): 37 f1 d3 1f b7 e3 72 f1 bd 06 eb fa 6b d0 bf 7a
1552887466.552780: RSN IE: STA PMKID - hexdump(len=16): cc 60 f3 b2 50 38 93 f4 66 e4 e8 ae 13 3e ca 5d
1552887466.554792: _GOLSOH_[ lina-K3-OKC roaming-wlan @ ath11 ]: STA <00:01:3e:3d:4a:e8> carried 2 PMKID in RSN IE
1552887466.555003: find index 52
1552887466.555184: find arp_node: find name =lina-roaming
1552887466.556096: pmksa_cache_get_okc, key mgmt 0, len 32
1552887466.556351: ##RSN: calc->pmkid - hexdump(len=16): cc 60 f3 b2 50 38 93 f4 66 e4 e8 ae 13 3e ca 5d
1552887466.557258: ##RSN: data->pmkid - hexdump(len=16): 37 f1 d3 1f b7 e3 72 f1 bd 06 eb fa 6b d0 bf 7a
1552887466.558884: pmksa_cache_get_okc, key mgmt 0, len 32
1552887466.559141: ##RSN: calc->pmkid - hexdump(len=16): cc 60 f3 b2 50 38 93 f4 66 e4 e8 ae 13 3e ca 5d
1552887466.560186: ##RSN: data->pmkid - hexdump(len=16): cc 60 f3 b2 50 38 93 f4 66 e4 e8 ae 13 3e ca 5d
1552887466.562209: _GOLSOH_[ lina-K3-OKC roaming-wlan @ ath11 ]: The pmkid carried by the STA <00:01:3e:3d:4a:e8> matched with the pmkid calculated on the AP, okc passes.
1552887466.563583: _GOLSOH_[ lina-K3-OKC roaming-wlan @ ath11 ]: STA 00:01:3e:3d:4a:e8 - L3 roaming - OKC matched, home ap 172.16.23.100
1552887466.563927: PMKID found from PMKSA cache eap_type=0 vlan_id=0
1552887466.564838: ##RSN: final pmkid - hexdump(len=16): cc 60 f3 b2 50 38 93 f4 66 e4 e8 ae 13 3e ca 5d
1552887466.565855: atheros_sta_assoc: addr=00:01:3e:3d:4a:e8 status_code=0 reassoc 1
1552887466.566845: atheros_del_key: addr=00:01:3e:3d:4a:e8 key_idx=0
1552887466.567946: cmd=ubus call wmaagent sendtrap '{"contents":"{\"trapType\":\"apStationAssociation\",\"apUptime\":\"9330\",\"apTraptime\":\"Mon Mar 18 13:37:46 2019
\",\"apMac\":\"34:e7:0b:03:c1:20\",\"apSSID\":\"lina-K3-OKC roaming-wlan\",\"apEncryptType\":\"3\",\"apAuthType\":\"1\",\"apStaMAC\":\"00:01:3e:3d:4a:e8\",\"apStaRSSI\":\"56\"}"}'
1552887466.601923: EAP: Server state machine created
1552887466.602152: IEEE 802.1X: 00:01:3e:3d:4a:e8 BE_AUTH entering state IDLE
1552887466.602583: IEEE 802.1X: 00:01:3e:3d:4a:e8 CTRL_DIR entering state FORCE_BOTH
1552887466.603302: WPA: 00:01:3e:3d:4a:e8 WPA_PTK entering state INITIALIZE
1552887466.603817: atheros_del_key: addr=00:01:3e:3d:4a:e8 key_idx=0
1552887466.604164: WPA: 00:01:3e:3d:4a:e8 WPA_PTK_GROUP entering state IDLE
1552887466.604609: WPA: 00:01:3e:3d:4a:e8 WPA_PTK entering state AUTHENTICATION
1552887466.605192: WPA: 00:01:3e:3d:4a:e8 WPA_PTK entering state AUTHENTICATION2
1552887466.605627: WPA: Re-initialize GMK/Counter on first station
1552887466.606490: GMK - hexdump(len=32): [REMOVED]
1552887466.607540: Key Counter - hexdump(len=32): [REMOVED]
1552887466.608298: GTK - hexdump(len=16): [REMOVED]
1552887466.608626: atheros_set_key: alg=3 addr=ff:ff:ff:ff:ff:ff key_idx=1
1552887466.609819: WPA: Assign ANonce - hexdump(len=32): ad f0 49 1a 16 bc 33 89 40 00 d7 c8 dc 48 87 29 5b 52 0f eb 6d c0 83 ae 6a 4c 7b ab ce 53 08 76
1552887466.611649: WPA: 00:01:3e:3d:4a:e8 WPA_PTK entering state INITPMK
1552887466.612081: WPA: PMK from PMKSA cache
1552887466.612240: WPA: 00:01:3e:3d:4a:e8 WPA_PTK entering state PTKSTART
1552887466.612814: WPA: Send EAPOL(version=2 secure=0 mic=0 ack=1 install=0 pairwise=1 kde_len=22 keyidx=0 encr=0)
1552887466.613362: WPA: Replay Counter - hexdump(len=8): 00 00 00 00 00 00 00 01
1552887466.624296: WPA: Use EAPOL-Key timeout of 1000 ms (retry counter 1)
1552887466.624645: wam_new_assoc_sta: reschedule ap_handle_timer timeout for 00:01:3e:3d:4a:e8 (300 seconds - ap_max_inactivity)
1552887466.625489: IEEE 802.1X: 00:01:3e:3d:4a:e8 BE_AUTH entering state IDLE
1552887466.633479: l2_packet_receive: src=00:01:3e:3d:4a:e8 len=169
1552887466.634101: ath11: Event EAPOL_RX (24) received
1552887466.634302: IEEE 802.1X: 155 bytes from 00:01:3e:3d:4a:e8
1552887466.634952:     IEEE 802.1X: version=1 type=3 length=151
1552887466.635225: WPA: Received EAPOL-Key from 00:01:3e:3d:4a:e8 key_info=0x10a type=2 key_data_length=56
1552887466.635753: WPA: Received Key Nonce - hexdump(len=32): 55 13 79 0d 2b 41 7b c5 e2 b4 17 bc 87 8a d0 5e 3d 38 90 f1 18 7a 71 21 b0 61 e9 c4 7b 34 76 0c
1552887466.637404: WPA: Received Replay Counter - hexdump(len=8): 00 00 00 00 00 00 00 01
1552887466.638317: WPA: 00:01:3e:3d:4a:e8 WPA_PTK entering state PTKCALCNEGOTIATING
1552887466.639011: WPA: PTK derivation - A1=34:e7:0b:03:c1:29 A2=00:01:3e:3d:4a:e8
1552887466.639700: WPA: Nonce1 - hexdump(len=32): ad f0 49 1a 16 bc 33 89 40 00 d7 c8 dc 48 87 29 5b 52 0f eb 6d c0 83 ae 6a 4c 7b ab ce 53 08 76
1552887466.641353: WPA: Nonce2 - hexdump(len=32): 55 13 79 0d 2b 41 7b c5 e2 b4 17 bc 87 8a d0 5e 3d 38 90 f1 18 7a 71 21 b0 61 e9 c4 7b 34 76 0c
1552887466.642978: WPA: PMK - hexdump(len=32): [REMOVED]
1552887466.643215: WPA: PTK - hexdump(len=48): [REMOVED]
1552887466.643457: WPA: KCK - hexdump(len=16): [REMOVED]
1552887466.643694: WPA: KEK - hexdump(len=16): [REMOVED]
1552887466.643929: WPA: TK - hexdump(len=16): [REMOVED]
1552887466.644282: WPA: 00:01:3e:3d:4a:e8 WPA_PTK entering state PTKCALCNEGOTIATING2
1552887466.645146: WPA: 00:01:3e:3d:4a:e8 WPA_PTK entering state PTKINITNEGOTIATING
1552887466.645646: atheros_get_seqnum: addr=00:00:00:00:00:00 idx=1
1552887466.646101: WPA: Send EAPOL(version=2 secure=1 mic=1 ack=1 install=1 pairwise=1 kde_len=46 keyidx=1 encr=1)
1552887466.646661: WPA: Replay Counter - hexdump(len=8): 00 00 00 00 00 00 00 02
1552887466.647369: Plaintext EAPOL-Key Key Data - hexdump(len=56): [REMOVED]
1552887466.658170: WPA: Use EAPOL-Key timeout of 1000 ms (retry counter 1)
1552887466.667698: l2_packet_receive: src=00:01:3e:3d:4a:e8 len=113
1552887466.668325: ath11: Event EAPOL_RX (24) received
1552887466.668528: IEEE 802.1X: 99 bytes from 00:01:3e:3d:4a:e8
1552887466.668976:     IEEE 802.1X: version=1 type=3 length=95
1552887466.669237: WPA: Received EAPOL-Key from 00:01:3e:3d:4a:e8 key_info=0x30a type=2 key_data_length=0
1552887466.669763: WPA: Received Key Nonce - hexdump(len=32): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1552887466.671841: WPA: Received Replay Counter - hexdump(len=8): 00 00 00 00 00 00 00 02
1552887466.672829: WPA: 00:01:3e:3d:4a:e8 WPA_PTK entering state PTKINITDONE
1552887466.673338: atheros_set_key: alg=3 addr=00:01:3e:3d:4a:e8 key_idx=0
1552887466.675145: 1552887466.675306: ath11: STA 00:01:3e:3d:4a:e8 WPA: pairwise key handshake completed (RSN)
1552887466.676743: _GOLSOH_[ lina-K3-OKC roaming-wlan @ ath11 ]: STA 00:01:3e:3d:4a:e8 - pairwise key handshake completed
1552887466.677048: IEEE 802.1X: 00:01:3e:3d:4a:e8 AUTH_PAE entering state AUTHENTICATED
1552887466.677617: ath11: AP-STA-CONNECTED 00:01:3e:3d:4a:e8
1552887466.678723: _GOLSOH_[ lina-K3-OKC roaming-wlan @ ath11 ]: AP-STA-CONNECTED 00:01:3e:3d:4a:e8
1552887466.678946: atheros_set_sta_authorized: addr=00:01:3e:3d:4a:e8 authorized=1
1552887466.681070: ieee802_1x_set_sta_authorized()
1552887466.681767: cmd=ubus call wmaagent sendtrap '{"contents":"{\"trapType\":\"apStationAuthenticationSuccessful\",\"apUptime\":\"9330\",\"apTraptime\":\"Mon Mar 18 13:37:46 2019
\",\"apMac\":\"34:e7:0b:03:c1:20\",\"apSSID\":\"lina-K3-OKC roaming-wlan\",\"apEncryptType\":\"3\",\"apAuthType\":\"1\",\"apStaMAC\":\"00:01:3e:3d:4a:e8\",\"apStaIP\":\"192.168.92.89\",\"apUserName\":\"\"}"}'
1552887466.715013: wam_authfail_start start
1552887466.715294: wam_getroam_authorinfo, cp success 0
1552887466.715499: wam_ov_author_proc, auth_flag 9, auth_step 9, mac-auth status 4
1552887466.716989: roaming client, auth step complete after ignore mac-auth
1552887466.717151: find index 52
1552887466.717329: find arp_node: find name =lina-roaming
1552887466.718488: _GOLSOH_[ lina-K3-OKC roaming-wlan @ ath11 ]: Access Role lina-roaming  from STA <00:01:3e:3d:4a:e8> roaming context will be applied
1552887466.718717: wam_ov_author_proc :apply_arp,redirect_enable:0, sta->mac_auth_result:4, apply_arp,ExternalCaptivePortal_flag:0,
1552887466.719033: wam_ov_author_proc :sta->cp_auth_success= 0,sta->applied_redirect_url=, sta->roam_flag =33
1552887466.720479: ap_check_some_conditions_value: all conditions isn't satisfied
1552887466.720640: wam_ov_ApplyARP, L3 roaming, cur arp vlanid 206, homeap vlanid 208, skip add macvlan
1552887466.720914: send_ovmode_homeap_l3roaming, homeap 172.16.23.100, vlan 208, ssid lina-K3-OKC roaming-wlan, sta 00:01:3e:3d:4a:e8, ipaddr 192.168.92.89, rolename lina-roaming
1552887466.723650: send_user_sync_msg, len 126
1552887466.724268: after send sync info to 172.16.23.100 time 9329--s,439610--us
1552887466.724904: send_user_sync_msg to 172.16.23.100,type 20, msglen 164.
1552887466.727760: _GOLSOH_[ lina-K3-OKC roaming-wlan @ ath11 ]: Create a tunnel between APs:name: [444560], vlanID: [0], localIP: [172.16.23.102], remote_ip: [172.16.23.100]
1552887466.930372: AddTunneluser ubus msg: ubus call gretap add_user '{"name":"444560","macAddress":"00:01:3e:3d:4a:e8","vlanID":0}'
1552887466.981474: check policylist .
1552887466.981807: wam_ov_add_policylist, policylist :
1552887466.982322: set policylist ubus msg: ubus call policy set_user_policy '{"macAddress":"00:01:3e:3d:4a:e8","arpName":"lina-roaming","policyListName":"","ifName":"ath11","ssid":"lina-K3-OKC roaming-
wlan","gwMacAddr":"","isolateEnable":0,"wlanSvcName":"lina-K3-OKC roaming-wlan"}'
1552887467.045138: _GOLSOH_[ lina-K3-OKC roaming-wlan @ ath11 ]: Set the PolicyList:[] from Access Role for STA <00:01:3e:3d:4a:e8>
1552887467.045398: wam_ov_ApplyARP : ARP(lina-roaming) applied successful.

1552887467.047991: wam_ov_author_proc,sta roaming, sta->sta_gateway = 0.0.0.0
1552887467.048378: gateway_mgr ubus msg: ubus call gateway_mgr adduser '{"userMac":"00:01:3e:3d:4a:e8","gwIp":"0.0.0.0"}'
1552887467.084054: cmd=ubus send sta_info_notify '{"on_line":true,"sta_mac":"00:01:3e:3d:4a:e8","proc":"wam","portal_username":"","security":"802.1X","sta_ip":-1062708135,"arp":"lina-roaming","vlanid":208,"ssid":"lina-K3-OKC roaming-
wlan"}'
1552887467.136506: send_add_user_sync_info enter
1552887467.136903: enter send time 9329--s,852245--us
1552887467.137329: send_ovmode_user_sync_info sta sync size 804
1552887467.137689: send_ovmode_user_sync_info, send cp success 0, mac-au success 0
1552887467.138037: send_ovmode_user_sync_info, append arp name lina-roaming
1552887467.138429: send user sync info 34:e7:0b:03:c1:29iface ath11,00:01:3e:3d:4a:e8, ssid lina-K3-OKC roaming-wlan, ipaddr 192.168.92.89, wlan lina-K3-OKC roaming-wlan, arp lina-roaming
1552887467.142145: sta->sync_type 2, cnt 66
1552887467.143544: _GOLSOH_delete STA <00:01:3e:3d:4a:e8> roaming context in current AP
1552887467.143725: sta_add_UserInfoToOtherbss, iface ath11
1552887467.143943: sta_add_UserInfoToOtherbss, find other bss ifname ath01, 34:e7:0b:03:c1:21, own ifname ath11, 34:e7:0b:03:c1:29
1552887467.147435: _GOLSOH_[ lina-K3-OKC roaming-wlan @ ath01 ]: receive STA <00:01:3e:3d:4a:e8> roaming context, ip 192.168.92.89, portal Auth success 0, roam flag 2, Sta applied access role lina-roaming, home ap 172.16.23.100
1552887467.147752: find index 52
1552887467.148024: find arp_node: find name =lina-roaming
1552887467.148274: SYNC_PMKSA_OKC,PMKID - hexdump(len=16): ed a4 4e 77 e6 e4 6e dc 24 a9 2b a8 39 47 bc 81
1552887467.149262: RSN: added PMKSA cache entry for 00:01:3e:3d:4a:e8
1552887467.150843: RSN: added PMKID - hexdump(len=16): ed a4 4e 77 e6 e4 6e dc 24 a9 2b a8 39 47 bc 81
1552887467.152802: _GOLSOH_save STA <00:01:3e:3d:4a:e8> roaming context in current AP
1552887467.155048: _GOLSOH_[ lina-K3-OKC roaming-wlan @ ath11 ]: send SYNC_ADD message to neighbors, STA <00:01:3e:3d:4a:e8> applied access role lina-roaming, sync_type 2, portal Auth fail
1552887467.155299: before nblist time 9329--s,870641--us
1552887467.155611: encap payload time 9329--s,870953--us
1552887467.156130: send sync info to 172.16.23.100 time 9329--s,871471--us
1552887467.156697: send_user_sync_msg, len 126
1552887467.157275: after send sync info to 172.16.23.100 time 9329--s,872616--us
1552887467.158061: send_user_sync_msg to 172.16.23.100,type 11, msglen 872.
1552887467.161757: _GOLSOH_[ lina-K3-OKC roaming-wlan @ ath11 ]: send STA <00:01:3e:3d:4a:e8> SYNC_ADD msg to neighbor AP:172.16.23.100, msglen 872,success 0
1552887467.161946: encap payload time 9329--s,877290--us
1552887467.162248: send sync info to 172.16.23.101 time 9329--s,877591--us
1552887467.162866: send_user_sync_msg, len 126
1552887467.163984: after send sync info to 172.16.23.101 time 9329--s,879325--us
1552887467.164609: send_user_sync_msg to 172.16.23.101,type 11, msglen 872.
1552887467.168008: _GOLSOH_[ lina-K3-OKC roaming-wlan @ ath11 ]: send STA <00:01:3e:3d:4a:e8> SYNC_ADD msg to neighbor AP:172.16.23.101, msglen 872,success 0
1552887467.168817: cmd=ubus call wmaagent sendtrap '{"contents":"{\"trapType\":\"apStationRoamingSuccessful\",\"apUptime\":\"9330\",\"apTraptime\":\"Mon Mar 18 13:37:47 2019
\",\"apMac\":\"34:e7:0b:03:c1:20\",\"apSSID\":\"lina-K3-OKC roaming-wlan\",\"apEncryptType\":\"3\",\"apAuthType\":\"1\",\"apRoamingType\":\"L3Roaming\",\"apStaMAC\":\"00:01:3e:3d:4a:e8\",\"apStaIP\":\"192.168.92.89\",\"apUserName\":
\"\"}"}'
1552887467.205724: _GOLSOH_[ lina-K3-OKC roaming-wlan @ ath11 ]: STA 00:01:3e:3d:4a:e8 - L3 roaming - success, home ap 172.16.23.100
```

2. Roaming without OKC and 802.11r, you can get apRoamingType and the roaming is success or failed like below:

```
1553161183.470170: _GOLSOH_[ 11r-cfy @ ath12 ]: Receive STA <e4:b2:fb:74:51:61> 80211 reassoc event
1553161183.470758: _GOLSOH_[ 11r-cfy @ ath12 ]: STA <e4:b2:fb:74:51:61> included RSN IE in (Re)AssocReq frame
1553161183.471222: [ 11r-cfy @ ath12 ]: recv sta assoc frame, reassoc 1
1553161183.471815: _GOLSOH_[ 11r-cfy @ ath12 ]: STA <e4:b2:fb:74:51:61> carried 0 PMKID in RSN IE
1553161183.472062: find index 71
1553161183.472131: find arp_node: find name =1553155430098arp
1553161183.472223: atheros_sta_assoc: addr=e4:b2:fb:74:51:61 status_code=0 reassoc 1
1553161183.472768: atheros_del_key: addr=e4:b2:fb:74:51:61 key_idx=0
1553161183.473141: cmd=ubus call wmaagent sendtrap '{"contents":"{\"trapType\":\"apStationAssociation\",\"apUptime\":\"5559\",\"apTraptime\":\"Thu Mar 21 17:39:43 2019
\",\"apMAC\":\"34:e7:0b:03:c2:10\",\"apSSID\":\"11r-cfy\",\"apEncryptType\":\"4\",\"apAuthType\":\"2\",\"apStaMAC\":\"e4:b2:fb:74:51:61\",\"apStaRSSI\":\"60\"}"}'
1553161183.506542: IEEE 802.1X: Ignore STA - 802.1X not enabled or forced for WPS
1553161183.506697: WPA: e4:b2:fb:74:51:61 WPA_PTK entering state INITIALIZE
1553161183.506876: atheros_del_key: addr=e4:b2:fb:74:51:61 key_idx=0
1553161183.507051: atheros_set_sta_authorized: addr=e4:b2:fb:74:51:61 authorized=0
1553161183.507257: WPA: e4:b2:fb:74:51:61 WPA_PTK_GROUP entering state IDLE
1553161183.507418: WPA: e4:b2:fb:74:51:61 WPA_PTK entering state AUTHENTICATION
1553161183.507567: WPA: e4:b2:fb:74:51:61 WPA_PTK entering state AUTHENTICATION2
1553161183.507713: WPA: Re-initialize GMK/Counter on first station
1553161183.508091: GMK - hexdump(len=32): [REMOVED]
1553161183.508504: Key Counter - hexdump(len=32): [REMOVED]
1553161183.508982: GTK - hexdump(len=32): [REMOVED]
1553161183.509098: atheros_set_key: alg=2 addr=ff:ff:ff:ff:ff:ff key_idx=2
1553161183.509571: WPA: Assign ANonce - hexdump(len=32): e2 f7 b2 86 a6 6d cb 63 7a 44 30 8b 9e c3 1b bd 5b d8 33 fe 97 78 b0 f0 68 da dc 73 77 53 28 38
1553161183.510187: WPA: e4:b2:fb:74:51:61 WPA_PTK entering state INITPSK
1553161183.510336: Searching a PSK for e4:b2:fb:74:51:61 prev_psk=(nil)
1553161183.510491: Searching a PSK for e4:b2:fb:74:51:61 prev_psk=(nil)
1553161183.510645: WPA: e4:b2:fb:74:51:61 WPA_PTK entering state PTKSTART
1553161183.510835: WPA: Send EAPOL(version=2 secure=0 mic=0 ack=1 install=0 pairwise=1 kde_len=0 keyidx=0 encr=0)
1553161183.511036: WPA: Replay Counter - hexdump(len=8): 00 00 00 00 00 00 00 01
1553161183.521390: WPA: Use EAPOL-Key timeout of 1000 ms (retry counter 1)
1553161183.521535: ath12: hostapd_new_assoc_sta: reschedule ap_handle_timer timeout for e4:b2:fb:74:51:61 (300 seconds - ap_max_inactivity)
1553161183.529066: l2_packet_receive: src=e4:b2:fb:74:51:61 len=135
1553161183.529298: ath12: Event EAPOL_RX (23) received
1553161183.529373: IEEE 802.1X: 121 bytes from e4:b2:fb:74:51:61
1553161183.529591:    IEEE 802.1X: version=2 type=3 length=117
1553161183.529695: WPA: Received EAPOL-Key from e4:b2:fb:74:51:61 key_info=0x10a type=2 mic_len=16 key_data_length=22
1553161183.529900: WPA: Received Key Nonce - hexdump(len=32): b5 e6 28 67 a1 9c 0c e5 33 97 31 a2 8d 14 34 53 d1 4f ba c2 eb 08 53 dc 61 1b 84 6d ee 49 b9 27
1553161183.530504: WPA: Received Replay Counter - hexdump(len=8): 00 00 00 00 00 00 00 01
1553161183.530826: WPA: e4:b2:fb:74:51:61 WPA_PTK entering state PTKCALCNEGOTIATING
1553161183.530982: Searching a PSK for e4:b2:fb:74:51:61 prev_psk=(nil)
1553161183.531143: WPA: PTK derivation using PRF(SHA1)
1553161183.531327: WPA: PTK derivation - A1=34:e7:0b:03:c2:1a A2=e4:b2:fb:74:51:61
1553161183.531569: WPA: Nonce1 - hexdump(len=32): e2 f7 b2 86 a6 6d cb 63 7a 44 30 8b 9e c3 1b bd 5b d8 33 fe 97 78 b0 f0 68 da dc 73 77 53 28 38
1553161183.532154: WPA: Nonce2 - hexdump(len=32): b5 e6 28 67 a1 9c 0c e5 33 97 31 a2 8d 14 34 53 d1 4f ba c2 eb 08 53 dc 61 1b 84 6d ee 49 b9 27
1553161183.532825: WPA: PMK - hexdump(len=32): [REMOVED]
1553161183.532918: WPA: PTK - hexdump(len=48): [REMOVED]
1553161183.533005: WPA: KCK - hexdump(len=16): [REMOVED]
1553161183.533090: WPA: KEK - hexdump(len=16): [REMOVED]
1553161183.533175: WPA: TK - hexdump(len=16): [REMOVED]
1553161183.533262: WPA: EAPOL-Key MIC using HMAC-SHA1
1553161183.533380: WPA: e4:b2:fb:74:51:61 WPA_PTK entering state PTKCALCNEGOTIATING2
1553161183.533536: WPA: e4:b2:fb:74:51:61 WPA_PTK entering state PTKINITNEGOTIATING
1553161183.533700: atheros_get_seqnum: addr=00:00:00:00:00:00 idx=2
1553161183.533901: WPA: Send EAPOL(version=2 secure=1 mic=1 ack=1 install=1 pairwise=1 kde_len=94 keyidx=2 encr=1)
1553161183.534115: WPA: Replay Counter - hexdump(len=8): 00 00 00 00 00 00 00 02
1553161183.534375: Plaintext EAPOL-Key Key Data - hexdump(len=104): [REMOVED]
1553161183.534463: WPA: Encrypt Key Data using AES-WRAP (KEK length 16)
1553161183.534656: WPA: EAPOL-Key MIC using HMAC-SHA1
1553161183.544864: WPA: Use EAPOL-Key timeout of 1000 ms (retry counter 1)
1553161183.549788: l2_packet_receive: src=e4:b2:fb:74:51:61 len=113
1553161183.550000: ath12: Event EAPOL_RX (23) received
1553161183.550073: IEEE 802.1X: 99 bytes from e4:b2:fb:74:51:61
1553161183.550227:    IEEE 802.1X: version=2 type=3 length=95
1553161183.550325: WPA: Received EAPOL-Key from e4:b2:fb:74:51:61 key_info=0x30a type=2 mic_len=16 key_data_length=0
1553161183.550524: WPA: Received Key Nonce - hexdump(len=32): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1553161183.551302: WPA: Received Replay Counter - hexdump(len=8): 00 00 00 00 00 00 00 02
1553161183.551612: WPA: EAPOL-Key MIC using HMAC-SHA1
1553161183.551733: WPA: e4:b2:fb:74:51:61 WPA_PTK entering state PTKINITDONE
1553161183.551905: atheros_set_key: alg=3 addr=e4:b2:fb:74:51:61 key_idx=0
1553161183.552192: ath12: AP-STA-CONNECTED e4:b2:fb:74:51:61
1553161183.552825: _GOLSOH_[ 11r-cfy @ ath12 ]: AP-STA-CONNECTED e4:b2:fb:74:51:61
1553161183.553080: atheros_set_sta_authorized: addr=e4:b2:fb:74:51:61 authorized=1
1553161183.553247: ieee802_1x_set_sta_authorized()
1553161183.553462: cmd=ubus call wmaagent sendtrap '{"contents":"{\"trapType\":\"apStationAuthenticationSuccessful\",\"apUptime\":\"5559\",\"apTraptime\":\"Thu Mar 21 17:39:43 2019
\",\"apMAC\":\"34:e7:0b:03:c2:10\",\"apSSID\":\"11r-cfy\",\"apEncryptType\":\"4\",\"apAuthType\":\"2\",\"apStaMAC\":\"e4:b2:fb:74:51:61\",\"apStaIP\":\"172.16.50.16\",\"apUserName\":\"\"}"}'
1553161183.626363: wam_getroam_authorinfo, cp success 0
1553161183.626478: wam_ov_author_proc, auth_flag 5, auth_step 5, mac-auth status 1
1553161183.627037: roaming client, auth step complete after ignore mac-auth
1553161183.627107: find index 71
1553161183.627174: find arp_node: find name =1553155430098arp
1553161183.627618: _GOLSOH_[ 11r-cfy @ ath12 ]: Access Role 1553155430098arp  from STA <e4:b2:fb:74:51:61> roaming context will be applied
1553161183.627892: wam_ov_author_proc :apply_arp.redirect_enable:0, sta->mac_auth_result:1, apply_arp.ExternalCaptivePortal_flag:0,
1553161183.628007: wam_ov_author_proc :sta->cp_auth_success= 0,sta->applied_redirect_url=, sta->roam_flag =1
1553161183.628540: ap_check_some_conditions_value: all conditions isn't satisfied
1553161183.628599: wam_check_send_conditions: all conditions don't match

1553161183.628682: set add macvlan ubus msg: ubus call network.macvlan add_user '{"macAddress":"e4:b2:fb:74:51:61","vlanID":0}'
1553161183.649244: _GOLSOH_[ 11r-cfy @ ath12 ]: Set MAC-vlan, Vlan-ID=[0] for STA <e4:b2:fb:74:51:61>
1553161183.649501: check policylist .
1553161183.649571: wam_ov_add_policylist, policylist :
1553161183.649680: set policylist ubus msg: ubus call policy set_user_policy '{"macAddress":"e4:b2:fb:74:51:61","arpName":"1553155430098arp","policyListName":"","ifName":"ath12","ssid":"11r-
cfy","gwMacAddr":"","isolateEnable":0,"wlanSvcName":"1553155430098"}'
1553161183.667897: _GOLSOH_[ 11r-cfy @ ath12 ]: Set the PolicyList:[] from Access Role for STA <e4:b2:fb:74:51:61>
1553161183.668178: wam_ov_ApplyARP : ARP(1553155430098arp) applied successful.

1553161183.668688: get vlan iface name br-wan, vlan id : 0
1553161183.668783: wam_ov_author_proc, will delete old sta's route : 172.16.50.16, ifname br-wan
1553161183.668886: sta_route_set: will set route for IPv4 address 172.16.50.16/-1
1553161183.669054: route_set failed: DST[172.16.50.16] SUBNET_MASK[255.255.255.255] RtMode[1] RtOp[1], No such process
1553161183.669481: wam_ov_author_proc, will add sta's route for its ip : 172.16.50.16, ifname br-wan
1553161183.669585: sta_route_set: will set route for IPv4 address 172.16.50.16/-1
1553161183.669831: route_set success: DST[172.16.50.16] SUBNET_MASK[255.255.255.255] RtMode[1] RtOp[0]
1553161183.670009: wam_ov_author_proc,sta roaming, sta->sta_gateway = 172.16.50.1
1553161183.670125: gateway_mgr ubus msg: ubus call gateway_mgr adduser '{"userMac":"e4:b2:fb:74:51:61","gwIp":"172.16.50.1"}'
1553161184.440074: cmd=ubus send sta_info_notify '{"on_line":true,"sta_mac":"e4:b2:fb:74:51:61","proc":"wam","portal_username":"","security":"PSK","sta_ip":-1408224752,"arp":"1553155430098arp","vlanid":0,"ssid":"11r-cfy"}'
1553161184.455317: send_add_user_sync_info enter
1553161184.455429: enter send time 5559--s,241613--us
1553161184.455525: send_ovmode_user_sync_info sta sync size 804
1553161184.455604: send_ovmode_user_sync_info, send cp success 0, mac-au success 0
1553161184.455716: send_ovmode_user_sync_info, append arp name 1553155430098arp
1553161184.455793: send user sync info 34:e7:0b:03:c2:1aiface ath12,e4:b2:fb:74:51:61, ssid 11r-cfy, ipaddr 172.16.50.16, wlan 1553155430098, arp 1553155430098arp
1553161184.456797: sta->sync_type 0, cnt 65
1553161184.457303: _GOLSOH_delete STA <e4:b2:fb:74:51:61> roaming context in current AP
1553161184.457654: sta_add_UserInfoToOtherbss, iface ath12
1553161184.457770: sta_add_UserInfoToOtherbss, find other bss ifname ath03, 34:e7:0b:03:c2:13, own ifname ath12, 34:e7:0b:03:c2:1a
1553161184.459367: _GOLSOH_[ 11r-cfy @ ath03 ]: receive STA <e4:b2:fb:74:51:61> roaming context, ip 172.16.50.16, portal Auth success 0, roam flag 0, Sta applied access role 1553155430098arp, home ap 172.16.50.13
1553161184.459802: find index 71
1553161184.459885: find arp_node: find name =1553155430098arp
1553161184.460494: _GOLSOH_save STA <e4:b2:fb:74:51:61> roaming context in current AP
1553161184.461401: _GOLSOH_[ 11r-cfy @ ath12 ]: send SYNC_ADD message to neighbors, STA <e4:b2:fb:74:51:61> applied access role 1553155430098arp, sync_type 0, portal Auth fail
1553161184.461845: before nblist time 5559--s,248026--us
1553161184.461959: encap payload time 5559--s,248143--us
1553161184.462074: send sync info to 172.16.50.11 time 5559--s,248256--us
1553161184.462291: send_user_sync_msg, len 126
1553161184.462809: after send sync info to 172.16.50.11 time 5559--s,248988--us
1553161184.463086: send_user_sync_msg to 172.16.50.11,type 11, msglen 804.
1553161184.464570: _GOLSOH_[ 11r-cfy @ ath12 ]: send STA <e4:b2:fb:74:51:61> SYNC_ADD msg to neighbor AP:172.16.50.11, msglen 804,success 0
1553161184.464874: encap payload time 5559--s,251058--us
1553161184.464974: send sync info to 172.16.50.10 time 5559--s,251159--us
1553161184.465138: send_user_sync_msg, len 126
1553161184.465460: after send sync info to 172.16.50.10 time 5559--s,251642--us
1553161184.465703: send_user_sync_msg to 172.16.50.10,type 11, msglen 804.
1553161184.466947: _GOLSOH_[ 11r-cfy @ ath12 ]: send STA <e4:b2:fb:74:51:61> SYNC_ADD msg to neighbor AP:172.16.50.10, msglen 804,success 0
1553161184.467379: cmd=ubus call wmaagent sendtrap '{"contents":"{\"trapType\":\"apStationRoamingSuccessful\",\"apUptime\":\"5560\",\"apTraptime\":\"Thu Mar 21 17:39:44 2019
\",\"apMAC\":\"34:e7:0b:03:c2:10\",\"apSSID\":\"11r-cfy\",\"apEncryptType\":\"4\",\"apAuthType\":\"2\",\"apRoamingType\":\"L2Roaming\",\"apStaMAC\":\"e4:b2:fb:74:51:61\",\"apStaIP\":\"172.16.50.16\",\"apUserName\":\"\"}"}'
1553161184.486737: _GOLSOH_[ 11r-cfy @ ath12 ]: STA e4:b2:fb:74:51:61 - L2 roaming - success  home ap 172.16.50.10
1553161184.487117: send message to track successful
1553161184.487255: 1553161184.487311: ath12: STA e4:b2:fb:74:51:61 WPA: pairwise key handshake completed (RSN)
```

3. Roaming with 802.11r, you can get log like below, you can judge whether succeed like the word in redcircle:

```
[2018-06-16 16:02:22]: _GOLSOH_[ personal-11r-cfy @ ath01 ]: STA <1c:5c:f2:26:07:37> carried 1 PMKID in RSN IE
[2018-06-16 16:02:22]: find index 110
[2018-06-16 16:02:22]: find arp_node: find name =cfy_arp
[2018-06-16 16:02:22]: FT: Reassoc Req IEs - hexdump(len=275): 00 10 70 65 72 73 6f 6e 61 6c 2d 31 31 72 2d 63 66 79 01 08 82 84 8b 96 24 30 48 6c 32 04 0c 12 18 60 21 02 02 12 24 02 01 0d 30 26 01 00 00 0f ac 04 01 00 00
00 0f ac 04 0c 00 01 00 02 1c a4 85 38 db 13 aa cb 08 cc 8b bc 36 2c fc 36 03 a1 b2 00 37 73 00 03 7f 43 92 7c 09 68 c8 c7 75 b6 9a da 96 ce 19 29 fd a5 8f 08 78 eb 04 48 10 98 a5 1f 51 ba bd e3 16 77 7b be 64 de e9 a0 21
4d 8b 7c 0a ec 2b 9e a2 7a 8b d4 5f 51 7e 74 1e d0 7a be 14 f8 50 e1 41 7a f9 14 1b 50 6d be 4b 06 d3 01 06 34 e7 0b 00 0c 31 03 17 30 30 30 63 33 39 2e 68 61 6e 2d 6e 65 74 77 6f 72 6b 73 2e 63 6f 6d 2d 1a 2d 40 17 ff ff
00 00 00 00 00 00 00 00 00 00 00 00 7f 08 04 00 00 00 00 00 00 40 dd 0b 00 17 f2 0a 00 01 04 00 00 00 00 dd 09 00 10 18 02 01 00 10 00 00 dd 07 00 50 f2 02 00 01 00
[2018-06-16 16:02:22]: atheros_get_seqnum: addr=00:00:00:00:00:00 idx=1
[2018-06-16 16:02:22]: atheros_sta_assoc: addr=1c:5c:f2:26:07:37 status_code=0 reassoc 1
[2018-06-16 16:02:22]: ath01: AP-STA-CONNECTED 1c:5c:f2:26:07:37
[2018-06-16 16:02:22]: _GOLSOH_[ personal-11r-cfy @ ath01 ]: AP-STA-CONNECTED 1c:5c:f2:26:07:37
[2018-06-16 16:02:22]: atheros_set_sta_authorized: addr=1c:5c:f2:26:07:37 authorized=1
[2018-06-16 16:02:22]: FT: Retry PTK configuration after association
[2018-06-16 16:02:22]: atheros_set_key: alg=3 addr=1c:5c:f2:26:07:37 key_idx=0
[2018-06-16 16:02:22]: wam_check_sta SSID personal-11r-cfy, ath01,find sta1c:5c:f2:26:07:37
[2018-06-16 16:02:22]: atheros_sta_deauth: addr=1c:5c:f2:26:07:37 reason_code=1
[2018-06-16 16:02:22]: cmd=ubus send sta_info_notify '{"on_line":false,"sta_mac":"1c:5c:f2:26:07:37","proc":"wam","portal_username":"","security":"PSK","sta_ip":-1408224240,"arp":"cfy_arp","vlanid":52,"ssid":"personal-11r-
[2018-06-16 16:02:22]: send message to track successful
[2018-06-16 16:02:22]: wam_ov_u
[2018-06-16 16:02:22]: wam_ov_u
[2018-06-16 16:02:22]: ath11: A
[2018-06-16 16:02:22]: _GOLSOH_
[2018-06-16 16:02:22]: get tunn
[2018-06-16 16:02:22]: ap_free_
[2018-06-16 16:02:22]: sta_rout
[2018-06-16 16:02:22]: route_se
[2018-06-16 16:02:22]: ap_free_
[2018-06-16 16:02:22]: cmd=ubus
[2018-06-16 16:02:22]: cmd=ubus
\",\"apMAC\":\"34:e7:0b:00:0c:3
[2018-06-16 16:02:22]: IEEE 802
[2018-06-16 16:02:22]: wam_ov_a
[2018-06-16 16:02:22]: roaming
[2018-06-16 16:02:22]: find inc
[2018-06-16 16:02:22]: find arp
[2018-06-16 16:02:22]: _GOLSOH_[ personal-11r-cfy @ ath01 ]: Access Role cfy_arp from STA <1c:5c:f2:26:07:37> roaming context will be applied
[2018-06-16 16:02:22]: wam_clear_old_author_info, start
[2018-06-16 16:02:22]: wam_clear_old_author_info, sta author info NULL,macaddr 1c:5c:f2:26:07:37
[2018-06-16 16:02:22]: wam_ov_author_proc :apply_arp.redirect_enable:0, sta->mac_auth_result:1, apply_arp.ExternalCaptivePortal_flag:0,
[2018-06-16 16:02:22]: wam_ov_author_proc :sta->cp_auth_success= 0,sta->applied_redirect_url=, sta->roam_flag =1
[2018-06-16 16:02:22]: ap_check_some_conditions_value: all conditions isn't satisfied
[2018-06-16 16:02:22]: check policylist ..
[2018-06-16 16:02:22]: wam_ov_add_policylist, policylist :
[2018-06-16 16:02:22]: set policylist ubus msg: ubus call policy set_user_policy '{"macAddress":"1c:5c:f2:26:07:37","arpName":"cfy_arp","policyListName":"","ifName":"ath01","ssid":"personal-11r-
cfy","gwMacAddr":"","isolateEnable":0,"WlanSvcName":"personal-11r-cfy"}'
[2018-06-16 16:02:22]: _GOLSOH_[ personal-11r-cfy @ ath01 ]: Set the PolicyList:[] from Access Role for STA <1c:5c:f2:26:07:37>
[2018-06-16 16:02:22]: set add macvlan ubus msg: ubus call network.macvlan add_user '{"macAddress":"1c:5c:f2:26:07:37","vlanID":52}'
[2018-06-16 16:02:22]: _GOLSOH_[ personal-11r-cfy @ ath01 ]: Set MAC-vlan, vlan-ID=[52] for STA <1c:5c:f2:26:07:37>
[2018-06-16 16:02:22]: wam_ov_ApplyARP : ARP(cfy_arp) applied successful.

[2018-06-16 16:02:22]: get tunnel iface name br-vlan52, vlan id : 52
[2018-06-16 16:02:22]: wam_ov_author_proc, will delete old sta's route : 172.16.52.16, ifname br-vlan52
[2018-06-16 16:02:22]: sta_route_set: will set route for IPv4 address 172.16.52.16/-1
[2018-06-16 16:02:22]: route_set failed: DST[172.16.52.16] SUBNET_MASK[255.255.255.255] RtMode[1] RtOp[1], No such process
[2018-06-16 16:02:22]: wam_ov_author_proc, will add sta's route for its ip : 172.16.52.16, ifname br-vlan52
[2018-06-16 16:02:22]: sta_route_set: will set route for IPv4 address 172.16.52.16/-1
[2018-06-16 16:02:22]: route_set success: DST[172.16.52.16] SUBNET_MASK[255.255.255.255] RtMode[1] RtOp[0]
[2018-06-16 16:02:22]: wam_ov_author_proc,sta roaming, sta->sta_gateway = 172.16.52.1
[2018-06-16 16:02:22]: gateway_mgr ubus msg: ubus call gateway_mgr adduser '{"userMac":"1c:5c:f2:26:07:37","gwIp":"172.16.52.1"}'
[2018-06-16 16:02:22]: Could not remove STA 1c:5c:f2:26:07:37 from ARP sta_list.
[2018-06-16 16:02:22]: send_add_user_sync_info enter
[2018-06-16 16:02:22]: enter send time 585--s,6329--us
[2018-06-16 16:02:22]: send_ovmode_user_sync_info sta sync size 804
[2018-06-16 16:02:22]: send_ovmode_user_sync_info, send cp success 0, mac-au success 0
[2018-06-16 16:02:22]: send_ovmode_user_sync_info, append arp name cfy_arp
[2018-06-16 16:02:22]: send user sync info 34:e7:0b:00:0c:31iface ath01,1c:5c:f2:26:07:37, ssid personal-11r-cfy, ipaddr 172.16.52.16, wlan personal-11r-cfy, arp cfy_arp
[2018-06-16 16:02:22]: sta->sync_type 1, cnt 69
[2018-06-16 16:02:22]: _GOLSOH_delete STA <1c:5c:f2:26:07:37> roaming context in current AP
[2018-06-16 16:02:22]: sta_add_UserInfoToOtherbss, iface ath01
[2018-06-16 16:02:22]: sta_add_UserInfoToOtherbss, find other bss ifname ath11, 34:e7:0b:00:0c:39, own ifname ath01, 34:e7:0b:00:0c:31
[2018-06-16 16:02:22]: sta_add_UserInfoToOtherbss, J = 0, r1kh->ap_ip 172.16.128.185, r1kh->addr 34:e7:0b:03:c2:19
[2018-06-16 16:02:22]: sta_add_UserInfoToOtherbss, J = 0, r1kh->ap_ip 172.16.128.185, r1kh->addr 34:e7:0b:03:c2:11
[2018-06-16 16:02:22]: sta_add_UserInfoToOtherbss, J = 0, r1kh->ap_ip 172.16.128.10, r1kh->addr 34:e7:0b:00:0c:39
[2018-06-16 16:02:22]: wpa_ov_generate_PmkR1Info, r1kh->ap_ip 172.16.128.10
[2018-06-16 16:02:22]: FT: R1KH-ID 34:e7:0b:00:0c:39
[2018-06-16 16:02:22]: FT: PMK-R1 - hexdump(len=32): [REMOVED]
[2018-06-16 16:02:22]: FT: PMKR1Name - hexdump(len=16): 4f f5 52 23 a7 0f e9 25 c8 8a e3 97 77 f3 0a fa
[2018-06-16 16:02:22]: sta_add_UserInfoToOtherbss, append 11r sync info.r1kh->ipaddr 172.16.128.10
[2018-06-16 16:02:22]: sta_add_UserInfoToOtherbss, SYNCFLAG 0, sendto 34:e7:0b:00:0c:39
[2018-06-16 16:02:22]: _GOLSOH_[ personal-11r-cfy @ ath11 ]: receive STA <1c:5c:f2:26:07:37> roaming context, ip 172.16.52.16, portal Auth success 0, roam flag 1, sta applied access role cfy_arp, home ap 172.16.128.10
[2018-06-16 16:02:22]: find index 110
[2018-06-16 16:02:22]: find arp_node: find name =cfy_arp
[2018-06-16 16:02:22]: sta_ovmode_sync_add, before r0 info pw 16
[2018-06-16 16:02:22]: sta_ovmode_sync_add, r0 info pw 16
[2018-06-16 16:02:22]: sta_ovmode_sync_add, recv 11r sync info from ap 34:e7:0b:00:0c:31
[2018-06-16 16:02:22]: FT: RRB received frame from remote AP 34:e7:0b:00:0c:31, ip 172.16.128.10
[2018-06-16 16:02:22]: FT: RRB frame - frame_type=1 packet_type=202 action_length=88 ap_address=34:e7:0b:00:0c:31
[2018-06-16 16:02:22]: FT: Received PMK-R1 push
[2018-06-16 16:02:22]: FT: PMK-R1 push - R1KH-ID=34:e7:0b:00:0c:39 S1KH-ID=1c:5c:f2:26:07:37 pairwise=0x10
[2018-06-16 16:02:22]: FT: PMK-R1 push - PMK-R1 - hexdump(len=32): [REMOVED]
[2018-06-16 16:02:22]: FT: PMK-R1 push - PMKR1Name - hexdump(len=16): 4f f5 52 23 a7 0f e9 25 c8 8a e3 97 77 f3 0a fa
[2018-06-16 16:02:22]: sta_ovmode_sync_add, recv invalid 11r sync info.
[2018-06-16 16:02:22]: sta_ovmode_sync_add, recv invalid 11r sync info.
[2018-06-16 16:02:22]: _GOLSOH_save STA <1c:5c:f2:26:07:37> roaming context in current AP
[2018-06-16 16:02:22]: _GOLSOH_[ personal-11r-cfy @ ath01 ]: send SYNC_ADD message to neighbors, STA <1c:5c:f2:26:07:37> applied access role cfy_arp, sync_type 1, portal Auth fail
[2018-06-16 16:02:22]: before nblist time 585--s,28979--us
[2018-06-16 16:02:22]: send_ovmode_user_sync_info, J = 0, ipaddr 172.16.128.185, r1kh->ap_ip 172.16.128.185, r1kh->addr 34:e7:0b:03:c2:19
[2018-06-16 16:02:22]: find  time 585--s,30384--us
[2018-06-16 16:02:22]: wpa_ov_generate_PmkR1Info, r1kh->ap_ip 172.16.128.185
[2018-06-16 16:02:22]: FT: R1KH-ID 34:e7:0b:03:c2:19
[2018-06-16 16:02:22]: FT: PMK-R1 - hexdump(len=32): [REMOVED]
[2018-06-16 16:02:22]: FT: PMKR1Name - hexdump(len=16): 6f e4 6c 08 a3 29 97 29 74 4e df e7 fb 0e ac fb
[2018-06-16 16:02:22]: send_ovmode_user_sync_info, append 11r sync info.r1kh->ipaddr 172.16.128.185
[2018-06-16 16:02:22]: send_ovmode_user_sync_info, SYNCFLAG 1, sendto 34:e7:0b:03:c2:19
[2018-06-16 16:02:22]: after gene R1  time 585--s,34743--us
[2018-06-16 16:02:22]: send_ovmode_user_sync_info, J = 1, ipaddr 172.16.128.185, r1kh->ap_ip 172.16.128.185, r1kh->addr 34:e7:0b:03:c2:11
[2018-06-16 16:02:22]: find  time 585--s,36013--us
[2018-06-16 16:02:22]: wpa_ov_generate_PmkR1Info, r1kh->ap_ip 172.16.128.185
[2018-06-16 16:02:22]: FT: R1KH-ID 34:e7:0b:03:c2:11
[2018-06-16 16:02:22]: FT: PMK-R1 - hexdump(len=32): [REMOVED]
[2018-06-16 16:02:22]: FT: PMKR1Name - hexdump(len=16): 7c 81 7c 08 59 91 db 57 23 02 99 27 ce ab bf 13
[2018-06-16 16:02:22]: send_ovmode_user_sync_info, append 11r sync info.r1kh->ipaddr 172.16.128.185
[2018-06-16 16:02:22]: send_ovmode_user_sync_info, SYNCFLAG 1, sendto 34:e7:0b:03:c2:11
[2018-06-16 16:02:22]: after gene R1  time 585--s,40286--us
[2018-06-16 16:02:22]: send_ovmode_user_sync_info, J = 2, ipaddr 172.16.128.185, r1kh->ap_ip 172.16.128.10, r1kh->addr 34:e7:0b:00:0c:39
[2018-06-16 16:02:22]: encap payload time 585--s,41218--us
[2018-06-16 16:02:22]: send sync info to 172.16.128.185 time 585--s,41780--us
[2018-06-16 16:02:22]: send_user_sync_msg, len 126
[2018-06-16 16:02:22]: after send sync info to 172.16.128.185 time 585--s,42817--us
[2018-06-16 16:02:22]: send_user_sync_msg to 172.16.128.185,type 11, msglen 1196.
[2018-06-16 16:02:22]: _GOLSOH_[ personal-11r-cfy @ ath01 ]: send STA <1c:5c:f2:26:07:37> SYNC_ADD msg to neighbor AP:172.16.128.185, msglen 1196,success 0
[2018-06-16 16:02:22]: cmd=ubus call wmaagent sendtrap '{"contents":"{\"trapType\":\"apStationRoamingSuccessful\",\"apUptime\":\"586\",\"apTraptime\":\"Sat Jun 16 16:02:22 2018
\",\"apMAC\":\"34:e7:0b:00:0c:30\",\"apSSID\":\"personal-11r-cfy\",\"apEncryptType\":\"3\",\"apAuthType\":\"0\",\"apRoamingType\":\"L2Roaming\",\"apStaMAC\":\"1c:5c:f2:26:07:37\",\"apStaIP\":\"172.16.52.16\",\"apUserName\"
[2018-06-16 16:02:22]: _GOLSOH_[ personal-11r-cfy @ ath01 ]: STA 1c:5c:f2:26:07:37 - L2 roaming - success, home ap 172.16.128.10
[2018-06-16 16:02:22]: send message to track successful
```

The OKC roaming is without 802.1X authentication, so you can not get the message of 802.1X authentication.

1. Roaming without OKC and 802.11r,you can get wireless packet like below:

No.	Time	Source	Destination	Protocol	Length	Info
7	251.005179747	AscomTat_3d:4a:d2	dc:08:56:13:29:09	802.11	52	Authentication, SN=56, FN=0, Flags=.....C
8	251.041718597	dc:08:56:13:29:09	AscomTat_3d:4a:d2	802.11	52	Authentication, SN=2084, FN=0, Flags=.....C
9	251.043570052	AscomTat_3d:4a:d2	dc:08:56:13:29:09	802.11	181	Reassociation Request, SN=58, FN=0, Flags=.....C, SSID=enterprise-wlan
10	251.064508474	dc:08:56:13:29:09	AscomTat_3d:4a:d2	802.11	160	Reassociation Response, SN=2085, FN=0, Flags=.....C
11	251.067792773	AscomTat_3d:4a:d2	dc:08:56:13:29:09	802.11	55	Action, SN=59, FN=0, Flags=.....C
12	251.067890761	dc:08:56:13:29:09	AscomTat_3d:4a:d2	802.11	55	Action, SN=0, FN=0, Flags=.....C
13	251.178295444	dc:08:56:13:29:09	AscomTat_3d:4a:d2	EAP	65	Request, Identity
14	251.182869635	AscomTat_3d:4a:d2	dc:08:56:13:29:09	EAP	72	Response, Identity
15	251.308680231	dc:08:56:13:29:09	AscomTat_3d:4a:d2	EAP	66	Request, Protected EAP (EAP-PEAP)
16	251.316209616	AscomTat_3d:4a:d2	dc:08:56:13:29:09	TLSv1	167	Client Hello
17	251.408815643	dc:08:56:13:29:09	AscomTat_3d:4a:d2	TLSv1	1084	Server Hello, Certificate, Server Key Exchange, Server Hello Done
18	251.415799406	AscomTat_3d:4a:d2	dc:08:56:13:29:09	EAP	69	Response, Protected EAP (EAP-PEAP)
19	251.506211836	dc:08:56:13:29:09	AscomTat_3d:4a:d2	TLSv1	1080	Server Hello, Certificate, Server Key Exchange, Server Hello Done
20	251.512130781	AscomTat_3d:4a:d2	dc:08:56:13:29:09	EAP	69	Response, Protected EAP (EAP-PEAP)
21	251.616062274	dc:08:56:13:29:09	AscomTat_3d:4a:d2	TLSv1	181	Server Hello, Certificate, Server Key Exchange, Server Hello Done
22	252.865275701	AscomTat_3d:4a:d2	dc:08:56:13:29:09	TLSv1	271	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
23	252.950128068	dc:08:56:13:29:09	AscomTat_3d:4a:d2	TLSv1	125	Change Cipher Spec, Encrypted Handshake Message
24	252.962351913	AscomTat_3d:4a:d2	dc:08:56:13:29:09	EAP	69	Response, Protected EAP (EAP-PEAP)
25	253.028583867	dc:08:56:13:29:09	AscomTat_3d:4a:d2	TLSv1	103	Application Data
26	253.038710532	AscomTat_3d:4a:d2	dc:08:56:13:29:09	TLSv1	143	Application Data, Application Data
27	253.149412197	dc:08:56:13:29:09	AscomTat_3d:4a:d2	TLSv1	119	Application Data
28	253.160013603	AscomTat_3d:4a:d2	dc:08:56:13:29:09	TLSv1	191	Application Data, Application Data
29	253.255166357	dc:08:56:13:29:09	AscomTat_3d:4a:d2	TLSv1	151	Application Data
30	253.261770134	AscomTat_3d:4a:d2	dc:08:56:13:29:09	TLSv1	143	Application Data, Application Data
31	253.364885099	dc:08:56:13:29:09	AscomTat_3d:4a:d2	TLSv1	103	Application Data
32	253.378252346	AscomTat_3d:4a:d2	dc:08:56:13:29:09	TLSv1	143	Application Data, Application Data
33	253.465143293	dc:08:56:13:29:09	AscomTat_3d:4a:d2	EAP	64	Success
34	253.483365340	dc:08:56:13:29:09	AscomTat_3d:4a:d2	EAPOL	177	Key (Message 1 of 4)
35	253.488965950	AscomTat_3d:4a:d2	dc:08:56:13:29:09	EAPOL	198	Key (Message 2 of 4)
36	253.534944575	dc:08:56:13:29:09	AscomTat_3d:4a:d2	EAPOL	211	Key (Message 3 of 4)
37	253.540216912	AscomTat_3d:4a:d2	dc:08:56:13:29:09	EAPOL	158	Key (Message 4 of 4)
38	253.550855098	AscomTat_3d:4a:d2	AscomTat_3d:4a:e8	802.11	355	QoS Data, SN=219, FN=0, Flags=.p.....TC

2. 802.11r roaming you can get wireless packet like below:

No.	Time	Source	Destination	Protocol	Length	Info
160368	203.307089400	BeijingH_00:0c:3a	e4:b2:fb:74:51:61	802.11	336	Probe Response, SN=1411, FN=0, Flags=.....C, BI=100, SSID=11r-cfy
160369	203.308210400	BeijingH_03:c2:1a	e4:b2:fb:74:51:61	802.11	337	Probe Response, SN=3414, FN=0, Flags=.....C, BI=100, SSID=11r-cfy
160528	203.410450400	e4:b2:fb:74:51:61	BeijingH_03:c2:1a	802.11	212	Authentication, SN=429, FN=0, Flags=.....C
160564	203.427819400	BeijingH_03:c2:1a	e4:b2:fb:74:51:61	802.11	204	Authentication, SN=3415, FN=0, Flags=.....C
160570	203.429373400	e4:b2:fb:74:51:61	BeijingH_03:c2:1a	802.11	335	Reassociation Request, SN=430, FN=0, Flags=.....C, SSID=11r-cfy
160593	203.442453400	BeijingH_03:c2:1a	e4:b2:fb:74:51:61	802.11	393	Reassociation Response, SN=3416, FN=0, Flags=.....C
160600	203.446203400	e4:b2:fb:74:51:61	BeijingH_03:c2:1a	802.11	40	Action, SN=431, FN=0, Flags=.....C, SSID=11r-cfy
160602	203.446218400	BeijingH_03:c2:1a	e4:b2:fb:74:51:61	802.11	54	Action, SN=0, FN=0, Flags=.....C

The 802.11r roaming is without four-way handshake, so you can not get the message of EAPOL.

8.19 WPA3 Encryption support

	Personal		Enterprise	
AP	WPA3_SAE_AES/ wpa3-personal	WPA3_PSK_SAE_AES/ Both(wa2&wpa3)	WPA3-AES/wpa3-enterprise(CNSA disable)	WPA3_AES256/wpa3-enterprise(CNSA enable)
AP1101	support	support	support	not support
AP1201H	support	support	support	only support(5G)
AP1201	support	support	support	support
AP1221	support	support	support	support
AP1231	support	support	support	support
AP1251	support	support	support	support

✓ If the AP can’t support WPA3 feature for CNSA, AP will set wpa3-enterprise CNSA disable or WPA3_AES

8.20 WPA3 roaming and PMF support

	Security Level	Encryption Type	PMF status	OKC	11r
OV	Personal	WPA3_SAE_AES	Required(Mandatory)	-	Yes
		WPA3_PSK_SAE_AES	Capable(Optional)	-	Yes
	Enterprise	WPA3_AES	Capable(Optional)	Yes	Yes
		WPA3_AES256(CNSA)	Required(Mandatory)	Yes	NO
Cluster	Personal	Wpa3-personal	Required(Mandatory)	-	Yes
		Both(wpa2&wpa3)	Capable(Optional)	-	Yes
	Enterprise	wpa3-enterprise(CNSA disable)	Capable(Optional)	Yes	Yes
		wpa3-enterprise(CNSA enable)	Required(Mandatory)	Yes	NO

WPA3_SAE_AES/wpa3-personal: support wpa3 devices to access, Required (Mandatory)
WPA3_PSK_SAE_AES/Both(wpa2&wpa3): Supports wpa3/wpa2 device access, Capable (Optional)
WPA3_AES256/wpa3-enterprise (CNSA enable): Supports wpa3 devices to access, Required (Mandatory)
WPA3_AES/wpa3-enterprise (CNSA disable): supports wpa3/wpa2 device access, Capable (Optional)

8.21 iPhone cannot access the WLAN when WPA3 is configured

Please check the system version if the iPhone, the system version before iPhone IOS12.2 does not support this encryption type.

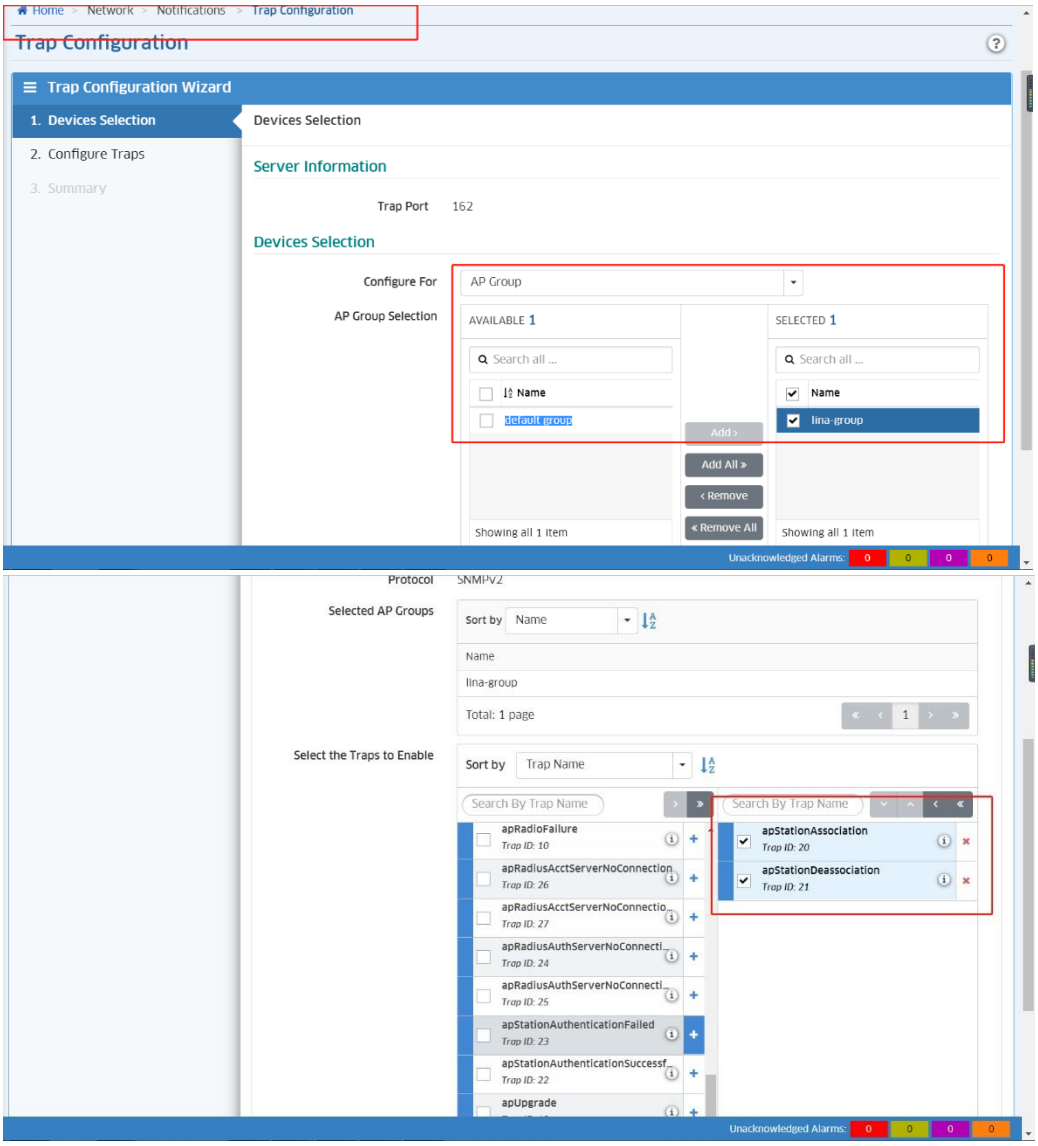
8.22 WPA3-AES / AES256 are enabled but clients are connected under WPA2

Below is the limitation by hardware regarding the key management for WPA3-AES/ AES256

AP1101 full band does not support WPA3 CNSA encryption,
AP1201H and AP1201L 2.4 GHz band does not support WPA3 CSNA encryption.
All the other APs and radio bands support CSNA encryption.
When CSNA encryption is applied to an AP that does not support it, the encryption will automatically fall back to non-CSNAmode (WPA2)

8.23 No roaming records in OVC or OVE

In OVC or OVE mode, it is necessary to turn on the trap function of corresponding AP to collect roaming information ofthe corresponding client. The configuration path is as follows:



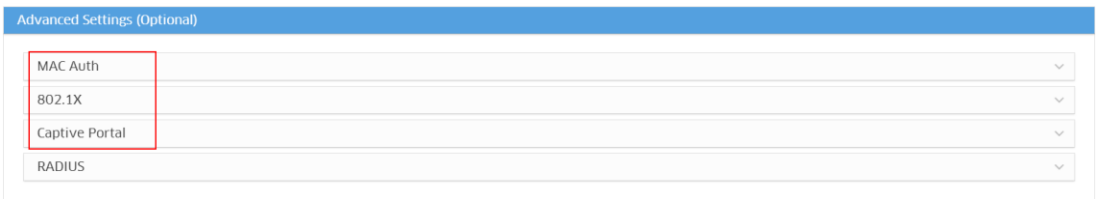
8.24 Missing or inconsistent roaming records / RSSI History

Please confirm whether the time of Cluster or OVC or OVE corresponds to the actual time. If the time does notcorrespond, records will be missing or inaccurate.

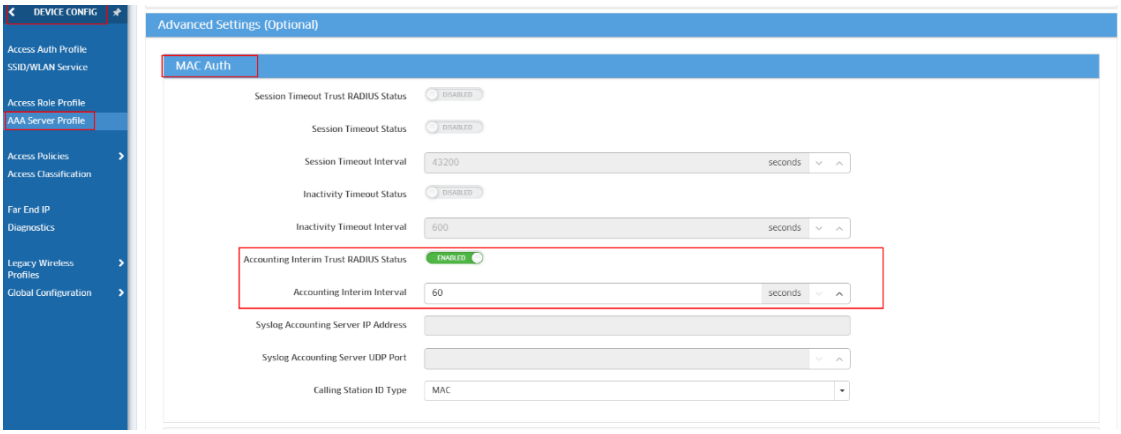
8.25 After the data quota exhausted, the client is still online

First check if the Accounting Interim Trust RADIUS Status is enabled.

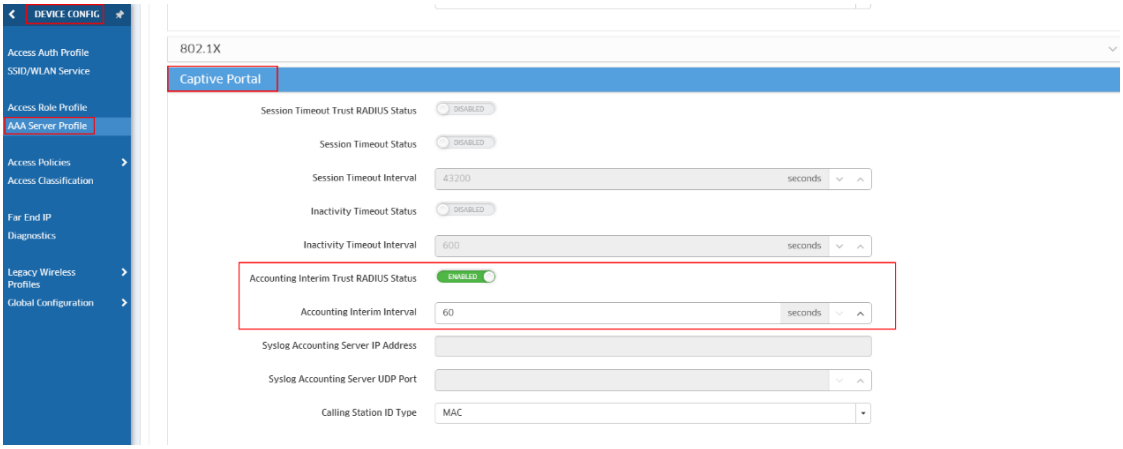
Home -> Unified Access -> Unified Profile -> Device Config -> AAA server Profile



If Authentication Strategy is MAC:

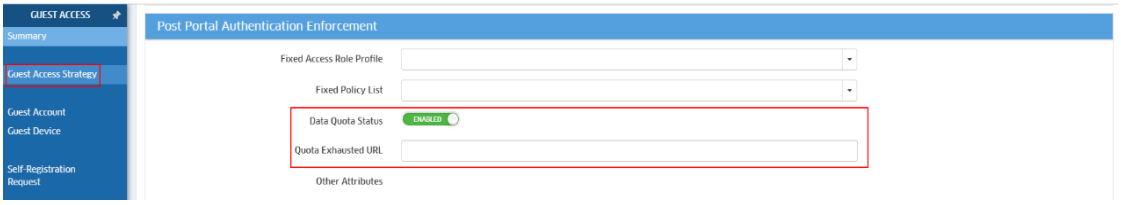


Else if Authentication Strategy is Portal:



Then check if the Data Quota Status is enabled.

Home -> UPAM -> Guest Access -> Guest Access Strategy, quota exhausted fixed URL must start with http|https.

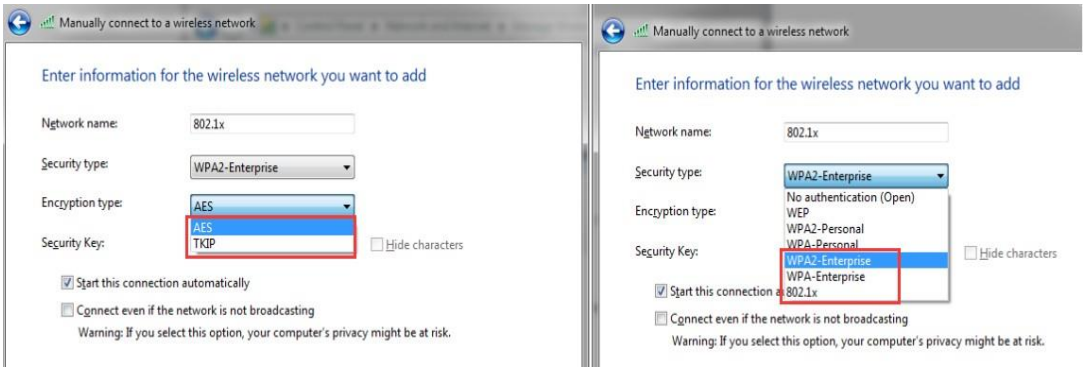


8.26 802.1x / MAC Authentication does not work

UPAM AP supports 802.1X authentication. 802.1X authentication involves the user (Access Client), the Access Point (AP, as RADIUS Client) and the RADIUS Server. If 802.1x authentications failed, please check as the following steps:

On client side, please check as following steps:

- Step1- Whether the **username** and **password** are correct and whether the security type settings match the configurationof WLAN, shown as below:

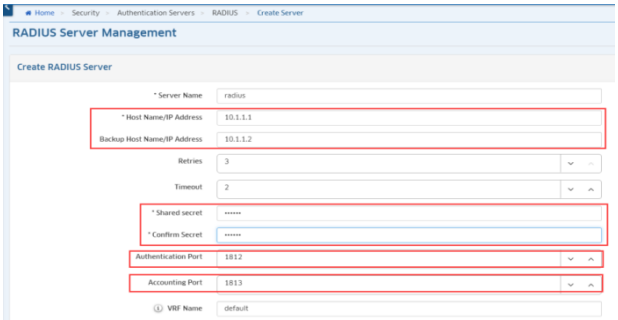


- Step2- When using a certificate to authenticate, check that the certificate used matches the radius server

On AP side, please check as following steps:

- Step1- Check the connected Radius’s configuration (AP and OV), The IP address and port number and shared secret arethe same as those configured on radius, shown as below:

```
support@AP-C1:20:~$ cat /var/config/AAA_server.conf
{
  "UnifiedAAAServer":[
    {
      "accountingPort":1813,
      "hostName":null,
      "retries":3,
      "ipAddress2":"10.1.1.2",
      "ipAddress":"10.1.1.1",
      "hostName2":null,
      "name":"radius",
      "type":"Radius",
      "timeout":2,
      "authenticationPort":1812,
      "secret":"a006a626d46117ba078e0ca9ffd5b859"
    }
  ]
```



- Step2- Check that the radius server in the selected AAA server profile in the WLAN configuration is correct and match, shown as below:

```
support@AP-C1:20:~$ cat /var/config/wlanservice.conf
{
        "WLANService":[
                {
                        "name":"radius",
                        "essid":"radius",
                        "hideSSID":"disable",
                        "ssidEnable":"enable",
                        "allowBand":"all",
                        "securityLevel":"Enterprise",
                        "encryptionType":"wpa2-aes",
                        "preSharedKey":"",
                        "passphrase":"",
                        "macAuthStatus":"disable",
                        "aaaProfile":"3A",
                        "bypassStatus":"disable",
                        "macAllowEap":"pass",
                        "classificationStatus":"disable",
```

```
support@AP-C1:20:~$ cat /var/config/AAA_profile.conf
{
  "AAAProfile":[
    {
      "e02d1xAuthServer":{
        "secondaryServer":null,
        "primaryServer":"radius",
        "thirdServer":null,
        "fourthServer":null
      },
      "name":"3A",
      "e02d1xAccServer":{
        "secondaryServer":null,
        "callingStationIdType":"MAC",
        "syslogUpdPort":null,
        "syslogIpAddress":null,
        "primaryServer":"radius",
        "thirdServer":null,
        "fourthServer":null
      },
```

```
support@AP-C1:20:~$ cat /var/config/AAA_server.conf
{
  "UnifiedAAAServer":[
    {
      "accountingPort":1813,
      "hostName":null,
      "retries":3,
      "ipAddress2":"10.1.1.2",
      "ipAddress":"10.1.1.1",
      "hostName2":null,
      "name":"radius",
      "type":"Radius",
      "timeout":2,
      "authenticationPort":1812,
      "secret":"a006a626d46117ba078e0ca9ffd5b859"
    }
  ]
```

- Step3- If above items have been done and the authentication still fail, please capture the data packets on the AP usingthe command **tcpdump -i br-wan －s 0 host radiusIP** to check the detailed authentication process.

On RADIUS Server side, please check as following steps:

- Step1- Whether the RADIUS Server Client configuration is correct, such as the username, password, shared secret, RADIUS Client IP or IP range (the IP of AP's br-wan interface), authentication and accounting port, certificate, sampleconfigurations on FreeRadius server are shown as *below:*

```
[root@bogon ~]# cat /etc/raddb/clients.conf
# -*- text -*-
##
## clients.conf -- client configuration directives
#
#  You can now specify one secret for a network of clients.
#  when a client request comes in, the BEST match is chosen.
#  i.e. The entry from the smallest possible network.
client 192.168.0.0/16 {
        secret          = testing123-2
        shortname       = private-network-2
}
client 172.16.0.0/16 {
        secret          = 123456
        shortname       = private-network-2
}

#client 10.10.10.10 {
```

```
[root@bogon ~]# vi /etc/raddb/users
steve   Cleartext-Password := "testing"
        Service-Type = Framed-User,
        Framed-Protocol = PPP,
        Framed-IP-Address = 172.16.3.33,
        Framed-IP-Netmask = 255.255.255.0,
        Framed-Routing = Broadcast-Listen,
        Framed-Filter-Id = "std.ppp",
        Framed-MTU = 1500,
#       Framed-Compression = Van-Jacobsen-TCP-IP

test    Cleartext-Password := "123456"
98-E7-F4-F6-C8-B7       Cleartext-Password :=   "98-E7-F4-F6-C8-B7"
98:E7:F4:F6:C8:B7       Cleartext-Password :=   "98:E7:F4:F6:C8:B7"
98E7F4F6C8B7    Cleartext-Password :=   "98E7F4F6C8B7"
7CB0C2BC7AA0    Cleartext-Password :=   "7CB0C2BC7AA0"
#
```

- Step2- Check whether the radius service is enabled, and whether the firewall allows authentication and account ports.
- Step3- If above items has been done; please capture the data packets on the RADIUS Server.

8.27 802.1x / MAC Authentication does not work

Client can roam between the APs of same group or the APs in different group, and if enable 802.11r switch or OKC, the client can happen fast roaming, if the client cannot roam between APs, Please check as following steps:

Step1- View the neighbor table entries and use cmd “adme show | grep IPADDR”, make sure that the AP2 is in AP1`s neighbor table and that the two AP`s OV IP is the same one , shown as below:

Notes From AP startup to get the complete neighbor information takes about 5~10 minutes:

```
support@AP-C1:30:~$
support@AP-C1:30:~$
support@AP-C1:30:~$
support@AP-C1:30:~$ adme show |grep  172.16.32.13
34:e7:0b:00:08:e0   172.16.32.13     172.16.32.5      0      AP-08:E0    3.0.0.50    2         0         1
support@AP-C1:30:~$
support@AP-C1:30:~$
support@AP-C1:30:~$                 neighbor          ov_ip
support@AP-C1:30:~$
```

Step2- If the client still cannot roam, you should capture the wireless packet to check the client whether send reassociation request to target AP, shown as below:

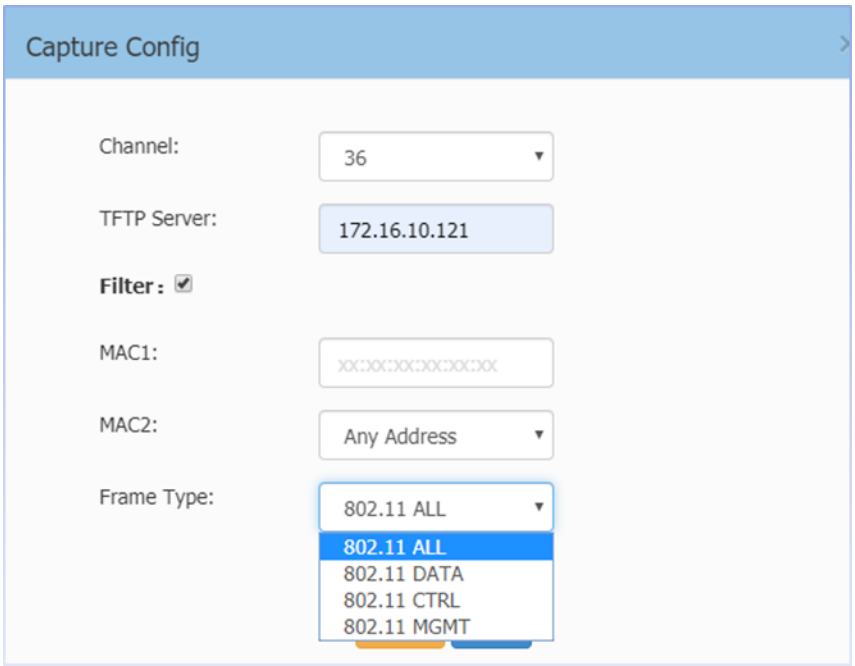
```
▷ Frame 75: 311 bytes on wire (2488 bits), 311 bytes captured (2488 bits)
▷ Radiotap Header v0, Length 18
▷ 802.11 radio information
◢ IEEE 802.11 Reassociation Request, Flags: ........
    Type/Subtype: Reassociation Request (0x0002)
  ▷ Frame Control Field: 0x2000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: BeijingH_00:0d:35 (34:e7:0b:00:0d:35)
    Destination address: BeijingH_00:0d:35 (34:e7:0b:00:0d:35)
    Transmitter address: 4c:74:bf:5f:2e:94 (4c:74:bf:5f:2e:94)
    Source address: 4c:74:bf:5f:2e:94 (4c:74:bf:5f:2e:94)
    BSS Id: BeijingH_00:0d:35 (34:e7:0b:00:0d:35)
    .... .... .... 0000 = Fragment number: 0
    1010 1011 1010 .... = Sequence number: 2746
▷ IEEE 802.11 wireless LAN management frame
```

8.28 How to perform an air-capture from Stellar AP

AP can work on capture mode and support wireless capture from 3.0.5 release, in this mode, all clients on this AP will be disconnected and wireless scanning will be stopped during packet capture period. Packet capture will be completed automatically when reaches its threshold (5minutes/10MB) or it can be stopped manually, please refer to the following steps for the capture on Stellar AP:

Step1- Please login AP UI page and go to RF Environment→ Wireless Capture Config→Start Capture, shown as below:

Step2-Please select the corresponding filters to capture ,shown as below:



After click “Start” AP will stored packet file under /tmp folder temporarily and delete it automatically after it uploaded to TFTP server.

8.29 AP fails to register to OV Cirrus

It needs to wait the next call home for the AP registration to OVC. If the AP always keeps in the incorrect status, please check according to below steps:

Check the DHCP server configuration whether there is option 43 or option138

If yes, please delete the option 43 or option138 configuration and set the AP to the default setting by pushing the reset button or executing the commands “ssudo firstboot” and “ssudo reboot” in support account.

For example:

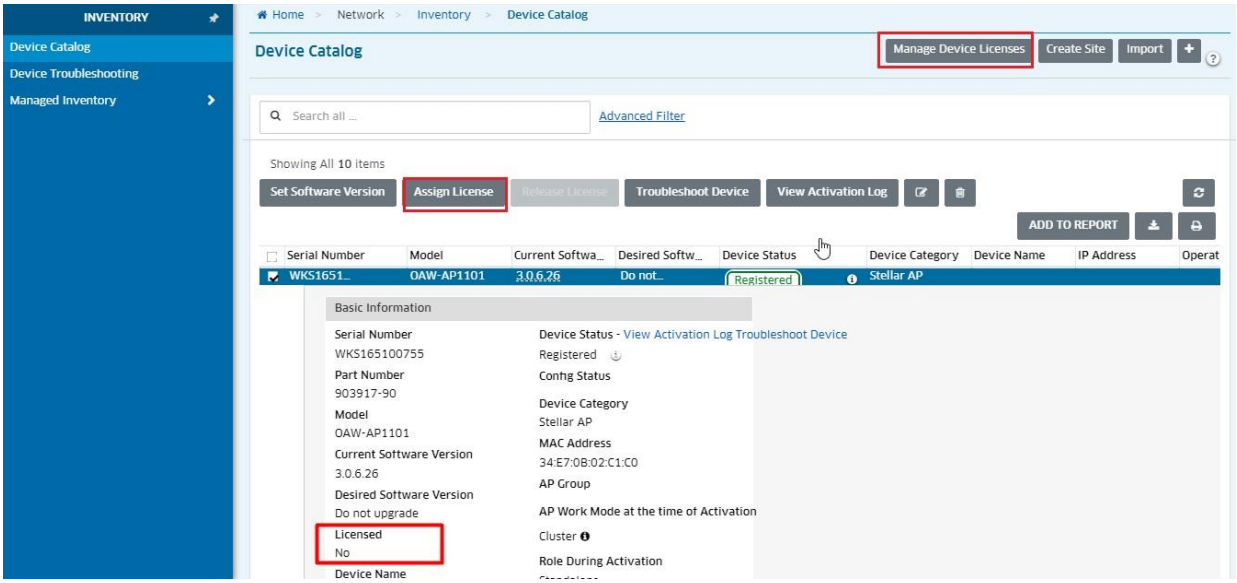
```
ip pool 88
 add range 172.16.88.100 172.16.88.200 mask 255.255.255.0
 ip dhcp server dns 192.168.10.177 219.141.136.10 219.141.140.10
 ip dhcp server option138 172.16.18.188
 ip dhcp server routers 172.16.88.1
 exit
```

```
support@AP-C1:30:~$
support@AP-C1:30:~$
support@AP-C1:30:~$ ssudo firstboot
This will erase all settings and remove any installed packages. Are you sure? [N/y]
y
/dev/ubi1_0 is mounted as /overlay, only erasing files
support@AP-C1:30:~$ ssutouch: /etc/cfm/delete_log: No such file or directory
ls: /etc/cfm/delete_log: No such file or directory
sh: 20280: unknown operand
touch: /etc/cfm/delete_log: No such file or directory
ls: /etc/cfm/delete_log: No such file or directory
sh: 20280: unknown operand

support@AP-C1:30:~$ ssudo rebootouch: /etc/cfm/delete_log: No such file or directory
ls: /etc/cfm/delete_log: No such file or directory
sh: 20280: unknown operand

support@AP-C1:30:~$ Jul 10 18:40:00 crond[2905]: USER root pid 21886 cmd /usr/sbin/fcgicheck.sh


- SIGTERM processes -
- SIGKILL processes -
- reboot -
[17108.918712] reboot: Restartin
Format: Log Type - Time(microsec) - Message - Optional Info
Log Type: B - Since Boot(Power On Reset),  D - Delta,  S - Statistic
```

If not, please check according to next step:

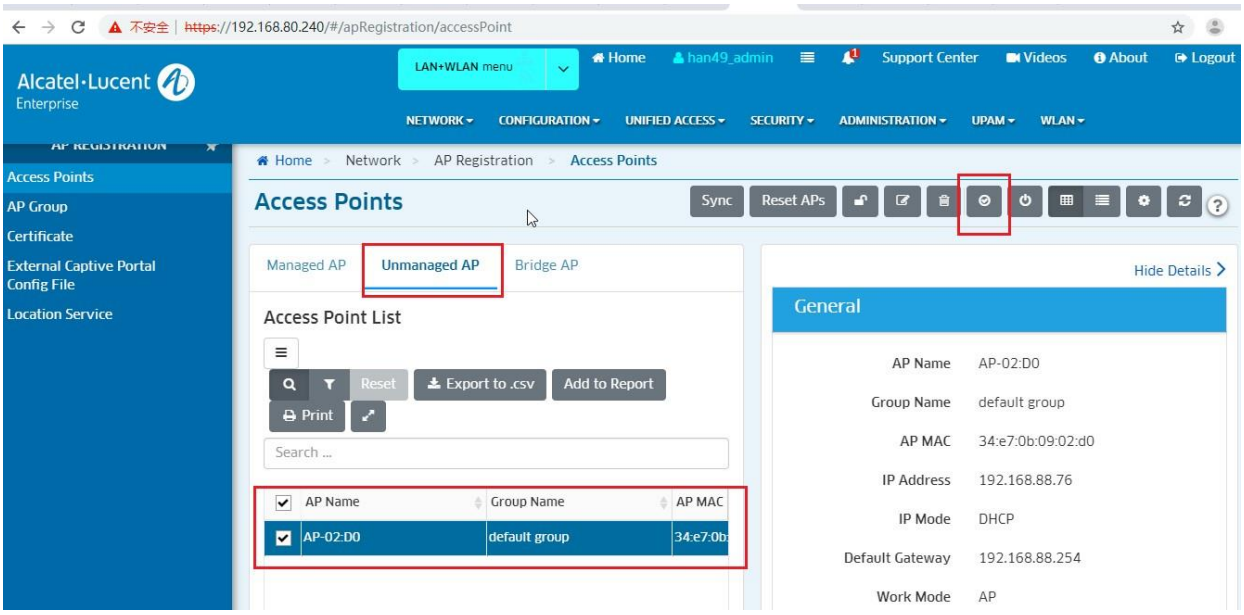
Check the AP information on the Device Catalog page whether there is the license.

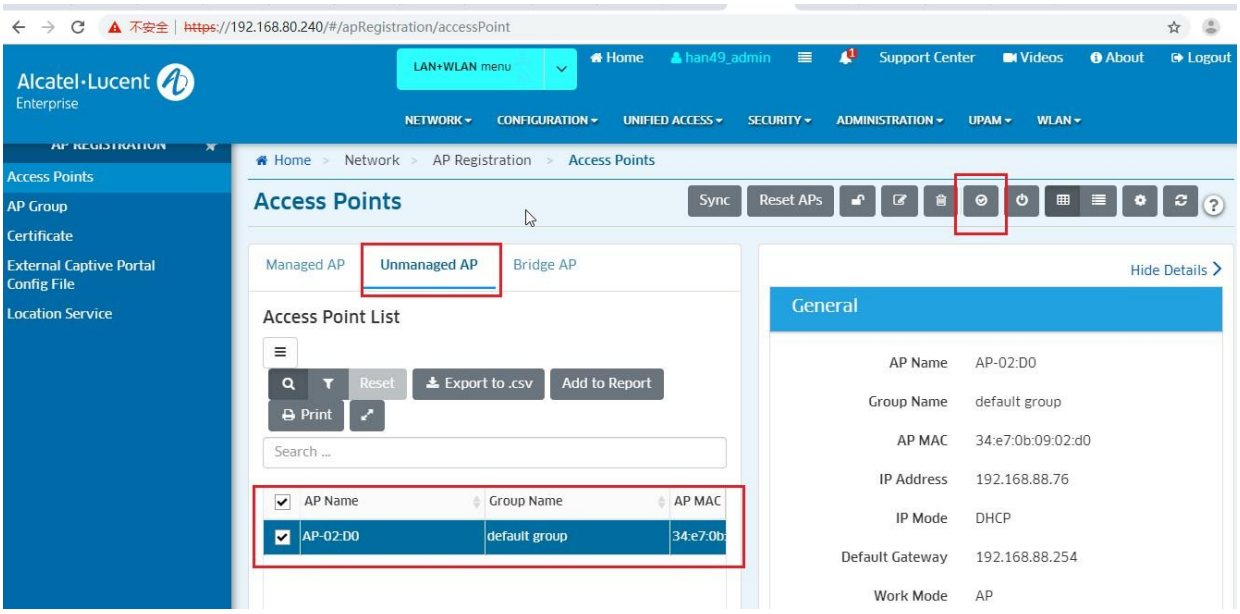
If there is no license, please add license for it by clicking the icon “Assign License” or clicking the icon “Manage Device Licenses”.



Check whether the AP is in the list of Network—Access Points—Unmanaged APs

If the Device Status in the Device Catalog, please check whether the AP is in the Unmanaged AP list. IF yes, please trust it first.





Check the ocloud_show information and the activation_client log and vpn log in CLI.

View the ocloud_show information

```
support@AP-6D:20:~$ ocloud_show
AP Work Mode:OVCLOUD
AP Date:Thu Jul 11 20:33:02 2019
AP IP:172.16.18.110
VPN Status:connected
VPN Assigned IP:10.8.0.2
VPN DPD:600
deviceCloudGroup:
cloudProcessStatus:completeOK
DHCP Server:
Activation Server: https://activation.ov.dev.ovcirrus.com
Failed to connect to ubus
NTP Server list: clock0.ovcirrus.com clock1.ovcirrus.com clock2.ovcirrus.com clock3.ovcirrus.com
echo DNS Server: 192.168.10.177
Proxy Server:
VPN Server:vpn30.ov.han.sqa.myovcloud.com
ovMqtt:private30.ov.han.sqa.myovcloud.com:1883
ovFqdn:public30.ov.han.sqa.myovcloud.com:443
Image Server:
Time to next Call Home(sec):195
support@AP-6D:20:~$
```

Check the activation_client.log

If the activation server is not reachable, please check the network.

```
support@AP-0B:40:~$ cat /tmp/log/activation_client.log
config: activation_url:https://activation.myovcloud.com proxy_url: proxy_port:0 proxy_user: proxy_pass:
2017-5-29 16:03:15 : enter into ====================> acv_upload_apinfo_with_hash
2017-5-29 16:03:15 : enter into ====================> parse_json_from_file
2017-5-29 16:03:15 : enter into ====================> acv_upload_apinfo_with_certificate
2017-5-29 16:03:15 : enter into ----------> parse_response_dCG_cPS
2017-5-29 16:03:15 : enter into ----------> parse_response
2017-5-29 16:03:15 : enter into ----------> _upload_apinfo_with_certificate
2017-5-29 16:03:15 : enter into ----------> call_home_json
2017-5-29 16:03:15 : enter into ----------> post_json_prepare
2017-5-29 16:03:15 : enter into ----------> popen_getstring
2017-5-29 16:03:16 : enter into ----------> popen_getstring
2017-5-29 16:03:16 : enter into ----------> popen_getstring
2017-5-29 16:03:17 : enter into ----------> popen_getstring
2017-5-29 16:03:18 : enter into ----------> popen_getstring
2017-5-29 16:03:19 : enter into ----------> popen_getstring
2017-5-29 16:03:19 : enter into ----------> post2acv_server
ping: bad address 'activation.myovcloud.com'
2017-5-29 16:04:49 : enter into ----------> communicate_with_server
2017-5-29 16:04:49 : url:https://activation.myovcloud.com/api/actserver/callhome post:{"data":{"devices":[{"serialNumber":"SSZ174501746","hash":"855478c4eba6ad8d5044ee
4dc49167feb4c81c660faf22803579bfd9bd44b58f","deviceMacAddress":"DC:08:56:03:0B:40","modelName":"OAW-AP1231","partNumber":"903925-90","role":"standalone","currentSoftwa
reVersion":"3.0.2.21","deviceCloudGroup":"han2","authMethod":"certificate"}]}} type:2
2017-5-29 16:04:49 : enter into ----------> popen_getstring
* name lookup timed out
* Couldn't resolve host 'activation.myovcloud.com'
2017-5-29 16:05:39 : error: curl_easy_perform() failed: Error
2017-5-29 16:05:39 : server response:  ret=13
2017-5-29 16:05:39 : enter into ====================> acv_done
2017-5-29 16:05:39 : _error_code=13, AP_mode=0
```

If “failedToGetCertificate“ is in the log, please wait 30 minutes or reboot the AP because it shall take 15 mins for the activation server to produce the certificate.

```
2017-12-16 22:49:23 : enter into ----------> communicate_with_server
2017-12-16 22:49:23 : url:https://activation.myovcloud.com/api/actserver/callhome post:{"data":{"devices":[{"serialNumber":"SSZ173200098","hash":"56659f3f5abc2fd6f8f90C
16ba084591416df500f18197602 99d5a325b1b8275","deviceMacAddress":"DC:08:56:00:34:90","modelName":"OAW-AP1231","partNumber":"903926-90","role":"standalone","currentSoftwar
eversion":"3.0.2.23","deviceCloudGroup":"unknown","authMethod":"hash"}]}} type:1
> POST /api/actserver/callhome HTTP/1.1
User-Agent: libcurl-agent/1.0
Host: activation.myovcloud.com
Accept: */*
Content-Type:application/json
Content-Length: 322

< HTTP/1.1 200 OK
< Server: nginx/1.12.0
< Date: Sun, 17 Dec 2017 06:49:35 GMT
< Content-Type: application/json
< Transfer-Encoding: chunked
< Connection: keep-alive
< Cache-Control: no-cache,no-store,must-revalidate
< Pragma: no-cache
< Expires: Thu, 01 Jan 1970 00:00:00 GMT
< X-Frame-Options: DENY
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< X-Atmosphere-first-request: true
< X-Atmosphere-tracking-id: fdcb347b-efda-4b70-8b7a-2f5ac50453c6
< Set-Cookie: JSESSIONID=CECADC90BBAC906FACEE6190F8D957FD; Path=/; HttpOnly
< Vary: Accept-Encoding
< X-Frame-Options: SAMEORIGIN
<
2017-12-16 22:49:37 : server response: {"data":{"deviceCloudGroup":"han1","cloudProcessStatus":"failedToGetCertificate","ocsp":null,"revocationUrl":null,"vpnFqdn":null,
"vpnFqdnPort":0,"ovFqdn":null,"ovFqdnPort":0,"ovInternalFqdn":null,"ovInternalFqdnPort":0,"preProvisioningFqdn":null,"preProvisioningFqdnPort":0,"dpdTime":0,"privateKey
":null,"publicKey":null,"certificateFile":null,"csr":null,"cloudCaChain":null,"cdnUrlDirectory":null,"downloadFilenameList":null,"retryCount":0}} ret=0
2017-12-16 22:49:37 : error: no certificates ready in server cloudProcessStatus:5
2017-12-16 22:49:37 : enter into ====================> acv_done
2017-12-16 22:49:37 : error_code=12, AP_mode=0
```

If the “clientCertificatePreviousluIssued” is in the log, please delete the AP information in the device catalog page and add it again and do reboot to the AP

```
Content-Type:application/json
Content-Length: 322

< HTTP/1.1 200 OK
< Server: nginx/1.12.0
< Date: Sun, 17 Dec 2017 06:20:36 GMT
< Content-Type: application/json
< Transfer-Encoding: chunked
< Connection: keep-alive
< Cache-Control: no-cache,no-store,must-revalidate
< Pragma: no-cache
< Expires: Thu, 01 Jan 1970 00:00:00 GMT
< X-Frame-Options: DENY
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< X-Atmosphere-first-request: true
< X-Atmosphere-tracking-id: c5fb1c50-4a6a-4b64-a4ae-9965c23c0394
< Set-Cookie: JSESSIONID=2ECCB0681BAE9EF4FA7BA0A5564B1EE9; Path=/; HttpOnly
< Vary: Accept-Encoding
< X-Frame-Options: SAMEORIGIN
<
2017-12-16 22:20:38 : server response: {"data":{"deviceCloudGroup":"han1","cloudProcessStatus":"clientCertificatePreviouslyIssued","ocsp":null,"revocationUrl":null,"vpr
Fqdn":null,"vpnFqdnPort":0,"ovFqdn":null,"ovFqdnPort":0,"ovInternalFqdn":null,"ovInternalFqdnPort":0,"preProvisioningFqdn":null,"preProvisioningFqdnPort":0,"dpdTime":0,
"privateKey":null,"publicKey":null,"certificateFile":null,"csr":null,"cloudCaChain":null,"cdnUrlDirectory":null,"downloadFilenameList":null,"retryCount":0}} ret=0
2017-12-16 22:20:38 : error: clientCertificatePreviouslyIssued shouldn't occur
2017-12-16 22:20:38 : enter into ====================> acv_done
2017-12-16 22:20:38 : error_code=18, AP_mode=0
```

If “vpnConfigFailed” is in the log;

```
< Pragma: no-cache
< Expires: Thu, 01 Jan 1970 00:00:00 GMT
< X-Frame-Options: DENY
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< X-Atmosphere-first-request: true
< X-Atmosphere-tracking-id: 46b75659-7add-43a4-9512-18d7ddd8e6fa
< Set-Cookie: JSESSIONID=A4BC1C1288F3A85F7B2EA67F66C34638; Path=/; HttpOnly
< Vary: Accept-Encoding
< X-Frame-Options: SAMEORIGIN
<
2017-12-15 00:04:39 : server response: {"data":{"cloudProcessStatus":"vpnConfigFailed"}} ret=0
2017-12-15 00:04:39 : error: openvpn config status upload failed
killall: openvpn: no process killed
Command failed: Not found
2017-12-15 00:04:39 : enter into ====================> acv_done
2017-12-15 00:04:39 : error_code=9, AP_mode=2
```

First check whether the DNS server works normally with the command “nslookup”, if the URL cannot be analyzed, please continue to check the configuration of DNS server

```
< X-Frame-Options: SAMEORIGIN
<
2017-12-14 03:50:10 : server response: {"data":{"deviceCloudGroup":"han1","cloudProcessStatus":"deviceCloudManaged","ocsp":null,"revocationUrl":null,"vpnFqdn":"vpn1.ov
.han.sqa.myovcloud.com","vpnFqdnPort":443,"ovFqdn":"public1.ov.han.sqa.myovcloud.com","ovFqdnPort":443,"ovInternalFqdn":null,"ovInternalFqdnPort":0,"preProvisioningFqd
n":null,"preProvisioningFqdnPort":0,"dpdTime":600,"privateKey":null,"publicKey":null,"certificateFile":null,"csr":null,"cloudCaChain":null,"cdnUrlDirectory":null,"down
loadFilenameList":null,"retryCount":0,"ovMqttFqdn":"private1.ov.han.sqa.myovcloud.com","ovMqttPort":1883}} ret=0
2017-12-14 03:50:10 : enter into ====================> acv_save_ov_info_and_start_vpn
2017-12-14 03:50:10 : enter into ----------> parse_response_dCG_cPS
```

```
support@AP-0B:40:~$ nslookup vpn1.ov.han.sqa.myovcloud.com
Server:    192.168.10.177
Address 1: 192.168.10.177

Name:      vpn1.ov.han.sqa.myovcloud.com
Address 1: 192.168.10.111 vpn2.ov.han.sqa.myovcloud.com
support@AP-0B:40:~$
```

- If the URL can be analyzed, please check whether the VPN server works normally, you can use ping command, if the URL cannot be reachable , there could be something wrong with the VPN server ,you can check it

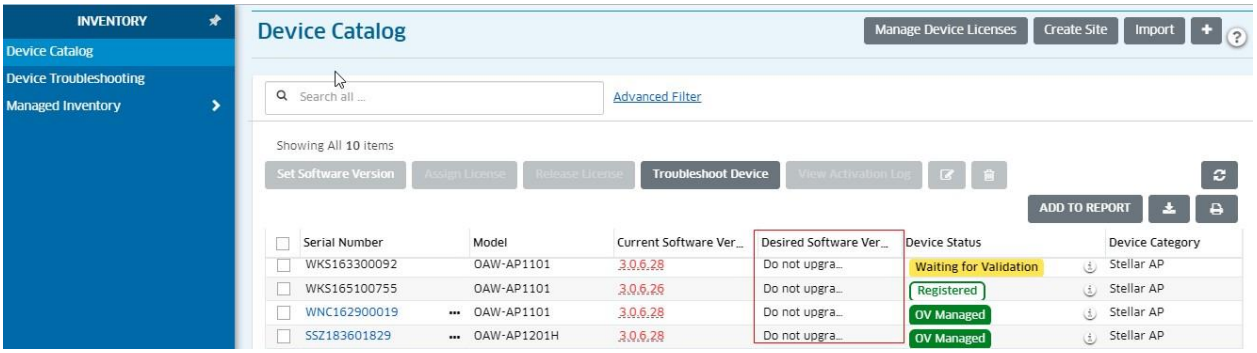
```
support@AP-0B:40:~$ nslookup vpn1.ov.han.sqa.myovcloud.com
Server:    192.168.10.177
Address 1: 192.168.10.177

Name:      vpn1.ov.han.sqa.myovcloud.com
Address 1: 192.168.10.111 vpn2.ov.han.sqa.myovcloud.com
support@AP-0B:40:~$ ping vpn1.ov.han.sqa.myovcloud.com
PING vpn1.ov.han.sqa.myovcloud.com (192.168.10.111): 56 data bytes
```

If "cloudProcessStatus":"completeOK“ is in the log but the AP still cannot register to the TOV , there could be a routing issue:

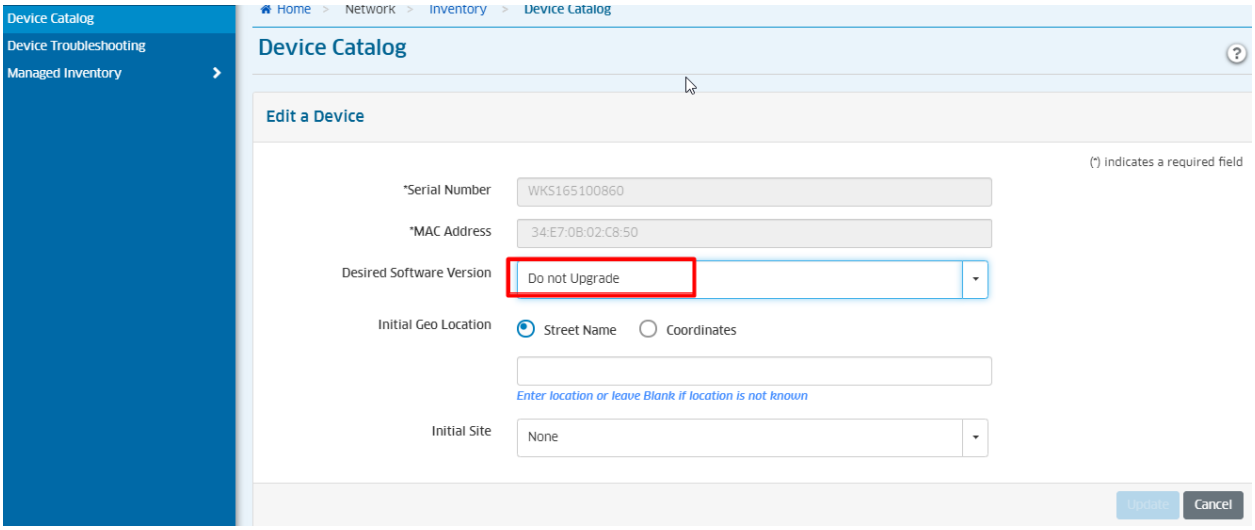
```
root@ubuntu:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.10.254  0.0.0.0         UG    0      0        0 ens33
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 ens33
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
172.18.0.0      0.0.0.0         255.255.0.0     U     0      0        0 br-12ae5fd4efa9
192.168.10.0    0.0.0.0         255.255.255.0   U     0      0        0 ens33
root@ubuntu:~#
```

If the upgrade failed is in the log, please check whether the "Desired Software Version" is “Do not upgrade” in the Device Catalog

If not, please edit it to be "Do not upgrade " , otherwise you need wait until the AP can upgrade successfully



change the AP’s software version to be "Do not upgrade"



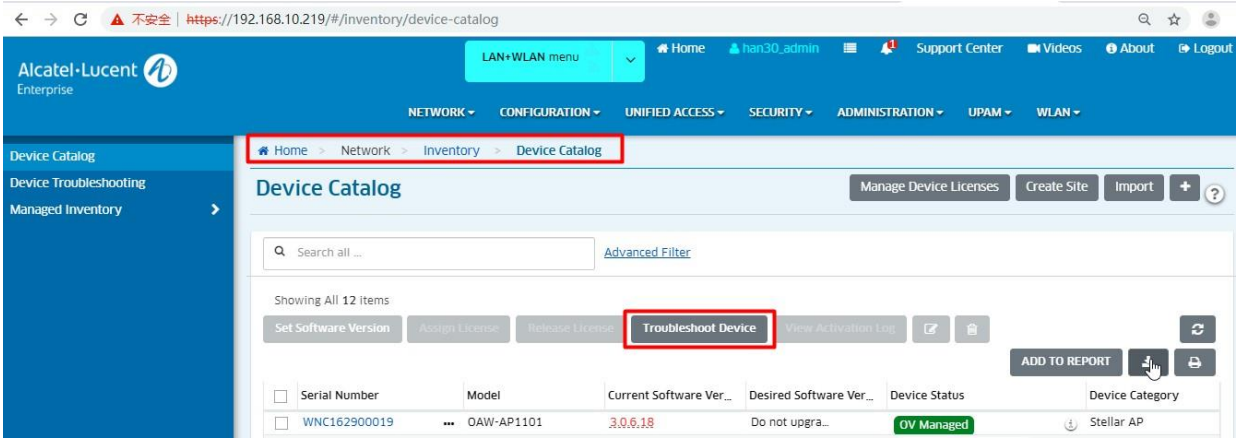
Check the vpn log in root account

```
root@AP-6D:20:/tmp/log#
root@AP-6D:20:/tmp/log# cat openvpn.log
Tue Jul  9 07:28:50 2019 OpenVPN 2.3.6 mips-openwrt-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [MH] [IPv6] built on Jul  2 2019
Tue Jul  9 07:28:50 2019 library versions: OpenSSL 1.0.2n  7 Dec 2017, LZO 2.10
Tue Jul  9 07:28:50 2019 Attempting to establish TCP connection with [AF_INET]192.168.10.218:443 [nonblock]
Tue Jul  9 07:28:51 2019 TCP connection established with [AF_INET]192.168.10.218:443
Tue Jul  9 07:28:51 2019 TCPv4_CLIENT link local: [undef]
Tue Jul  9 07:28:51 2019 TCPv4_CLIENT link remote: [AF_INET]192.168.10.218:443
Tue Jul  9 07:28:52 2019 [*.vpn.myovcloud.com] Peer Connection Initiated with [AF_INET]192.168.10.218:443
Tue Jul  9 07:28:54 2019 TUN/TAP device tun0 opened
Tue Jul  9 07:28:54 2019 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Tue Jul  9 07:28:54 2019 /sbin/ifconfig tun0 10.8.0.2 netmask 255.255.0.0 mtu 1500 broadcast 10.8.255.255
Tue Jul  9 07:28:54 2019 Initialization Sequence Completed
root@AP-6D:20:/tmp/log# cat vpn_manage.log
2019-7-9 07:28:50 : get dpdtime=600
root@AP-6D:20:/tmp/log#
```

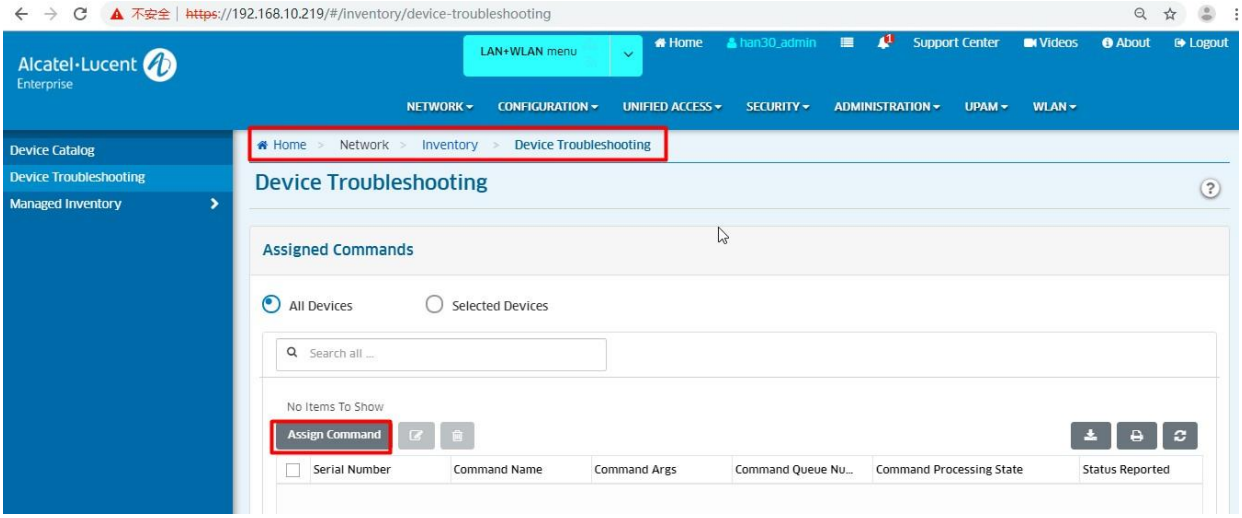
8.30 Debug AP from OV Cirrus Troubleshooting page

Enter the page of Device Selection:

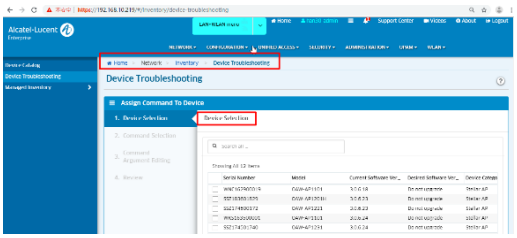
Path: Home -> NETWORK -> INVENTORY -> Device Catalog -> Troubleshoot Device



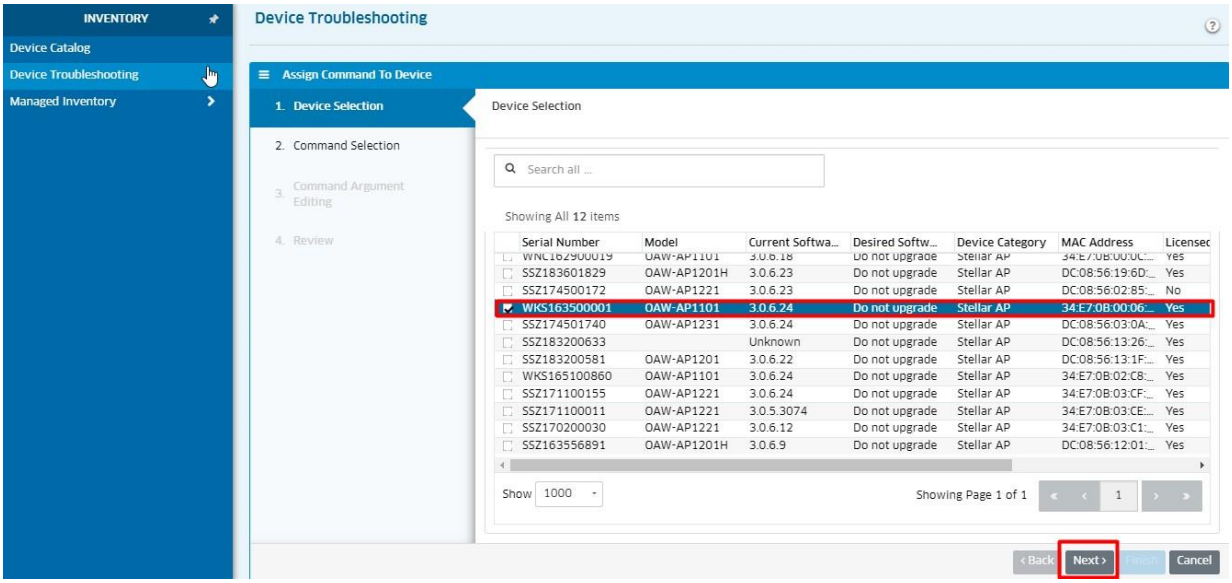
or Path: Home -> NETWORK -> INVENTORY -> Device Troubleshooting -> Troubleshoot Device -> Assign Command



Then enter the Device Selection page by above path.



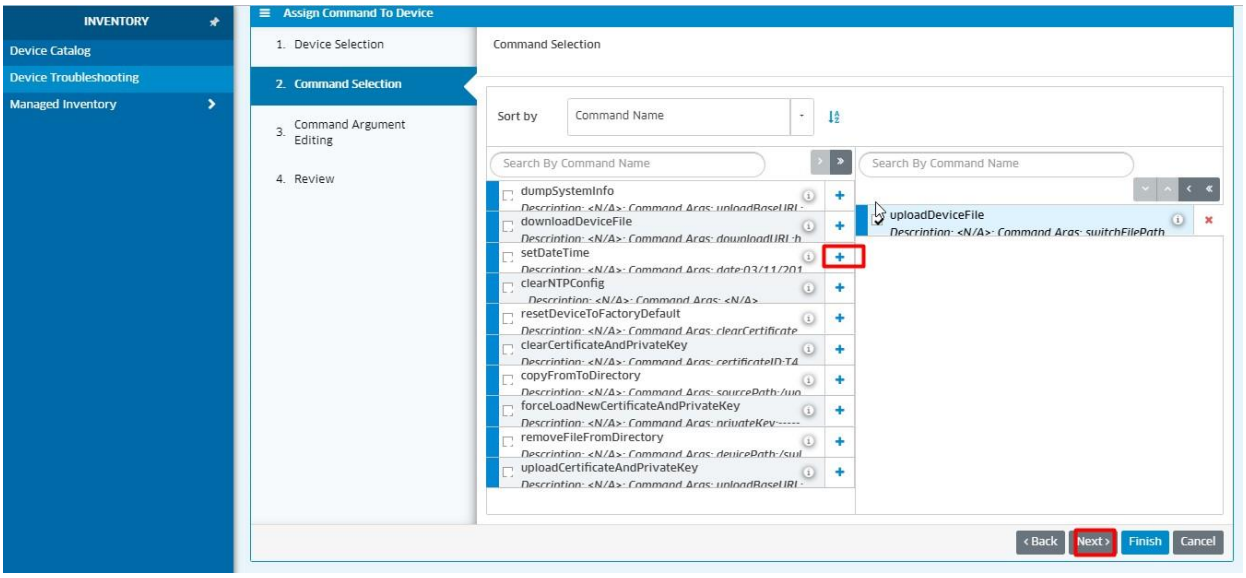
Select an AP:



Then click “Next” and enter the Command Selection page.

Command Selection

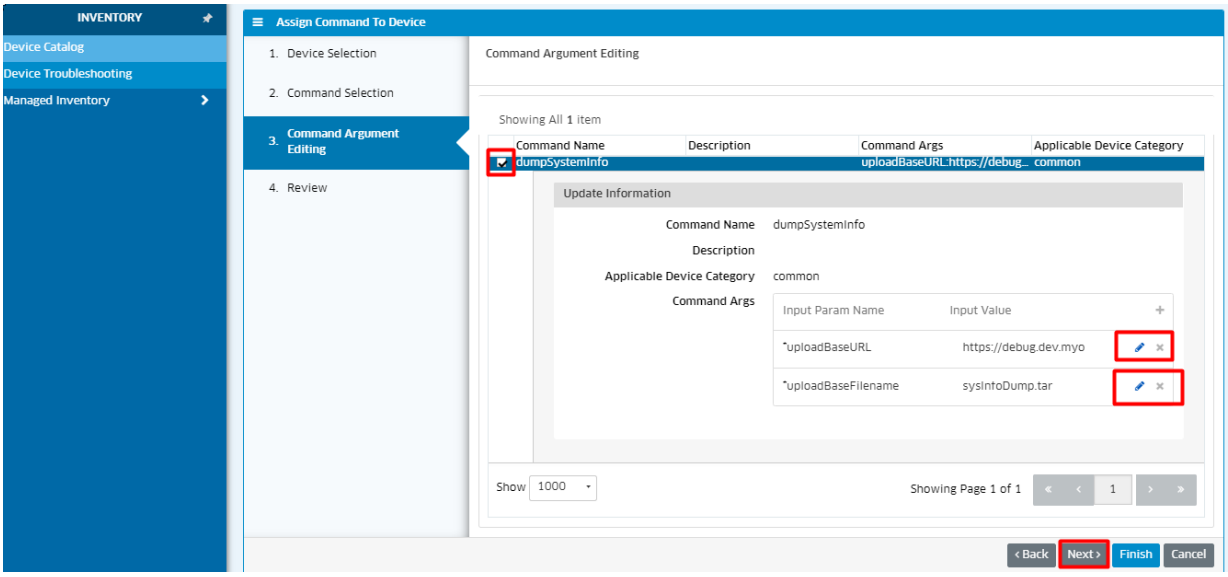
Select one command you want and click the “+” icon



Then click “Next” and enter the Command Argument Editing page.

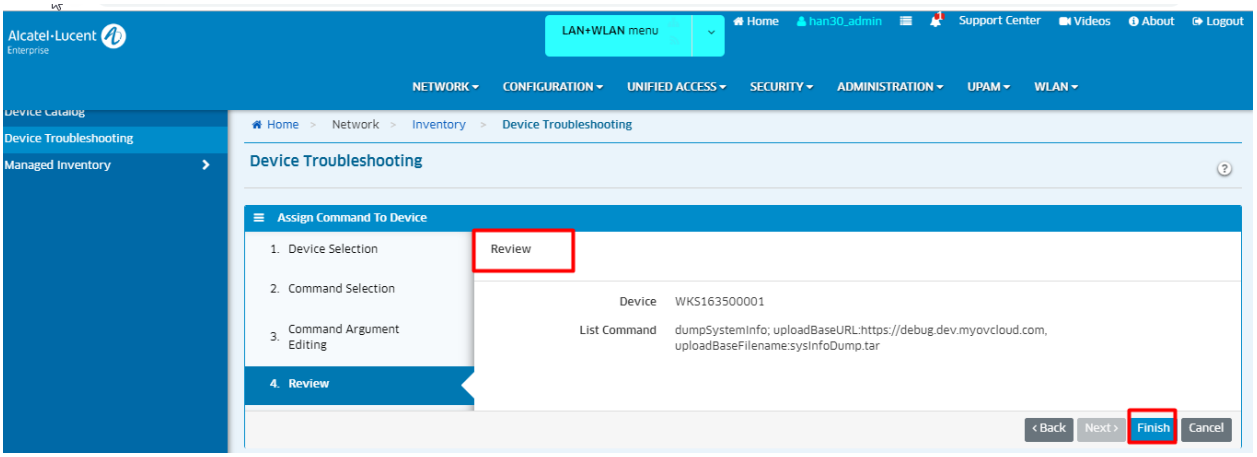
Command argument editing

There are different displays for different command, take “dumpSystemInfo” for example:

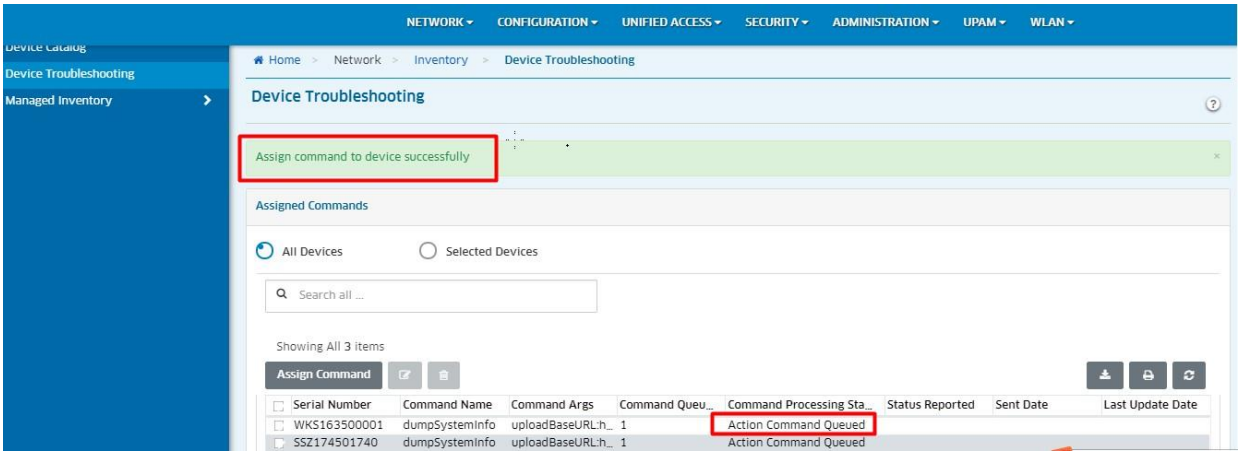


Then click “Next” and enter the Review page.

Operation review



Then click “Finish” and pop-up the tips “Assign Command to Device Successfully” and displays the Assigned Commands page, which can view the assigned commands and its processing status.



8.31 Debug AP channel change

There are 2 use cases for channel changed:

1. the ACS is disabled, and the channel will change again after the channel is fixed manually.
2. When ACS is enabled, the automatic channel is triggered to select the optimal channel, and then the channel was switched again.

The above two situations are not caused by the ACS but are caused by the drive when the radar signal detected on the current channel.

Please check if there is radar signal on channel, and use the below commands "cat / proc / kes_debug | grep Radar" or "cat / proc / kes_syslog | grep Radar" to check whether there is radar information in the log file.

How to prevent the problem from happening again:

- When ACS is disabled, do not fix the channel with radar interference.
- When ACS is enabled, all available channels are added through the channel list function. When ACS selects, only the optimal channel is selected from the channels set in the channel list.

8.32 802.11w support for WPA2

When the client cannot connect to the WLAN of type PMF: Required, please check:

That may be because the client does not support management frame encryption. You can check whether the client supports management frame encryption or force management frame encryption by capturing packets.

The specific messages are as follows:

When 802.11w Client Support is Disabled, MFPR = 0 and MFPC = 0. Indicates that management frame encryption is not supported.

```
RSN Capabilities: 0x000c
    .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
    .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
    .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STAKeySA (0x3)
    .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
    .... .... .0.. .... = Management Frame Protection Required: False
    .... .... 0... .... = Management Frame Protection Capable: False
    .... ...0 .... .... = Joint Multi-band RSNA: False
    .... ..0. .... .... = PeerKey Enabled: False
```

When 802.11w Client Support is Optional, MFPR = 0 and MFPC = 1. Supports management frame encryption.

```
Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 20
    RSN Version: 1
  > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    Pairwise Cipher Suite Count: 1
  > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
    Auth Key Management (AKM) Suite Count: 1
  > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
  v RSN Capabilities: 0x008c
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
      .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STAKeySA (0x3)
      .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
      .... .... .0.. .... = Management Frame Protection Required: False
      .... .... 1... .... = Management Frame Protection Capable: True
      .... ...0 .... .... = Joint Multi-band RSNA: False
      .... ..0. .... .... = PeerKey Enabled: False
```

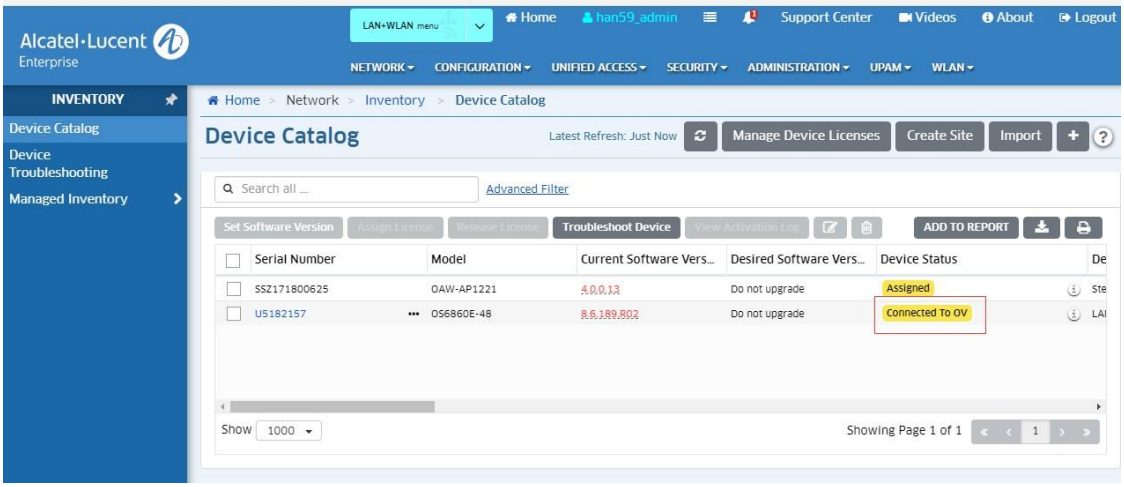
When 802.11w Client Support is Required, MFPR = 1 and MFPC = 1. Indicates mandatory support for management frame encryption.

```
Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 20
    RSN Version: 1
  > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    Pairwise Cipher Suite Count: 1
  > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
    Auth Key Management (AKM) Suite Count: 1
  > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
  v RSN Capabilities: 0x00cc
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
      .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STAKeySA (0x3)
      .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
      .... .... .1.. .... = Management Frame Protection Required: True
      .... .... 1... .... = Management Frame Protection Capable: True
      .... ...0 .... .... = Joint Multi-band RSNA: False
      .... ..0. .... .... = PeerKey Enabled: False
```

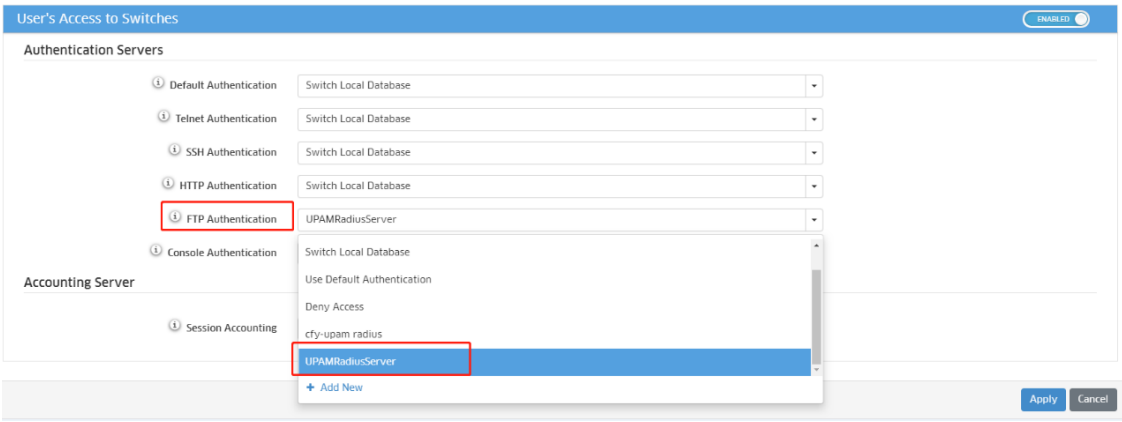
8.33 Authenticated Switch Access using UPAM Troubleshooting

Authenticated Switch Access using UPAM is a new feature of UPAM, user can use UPAM to configure and monitor all switch access ,contains FTP,SSH,TELNET,HTTP and so on. If user login the switch by FTP account failed, please check as the following steps:

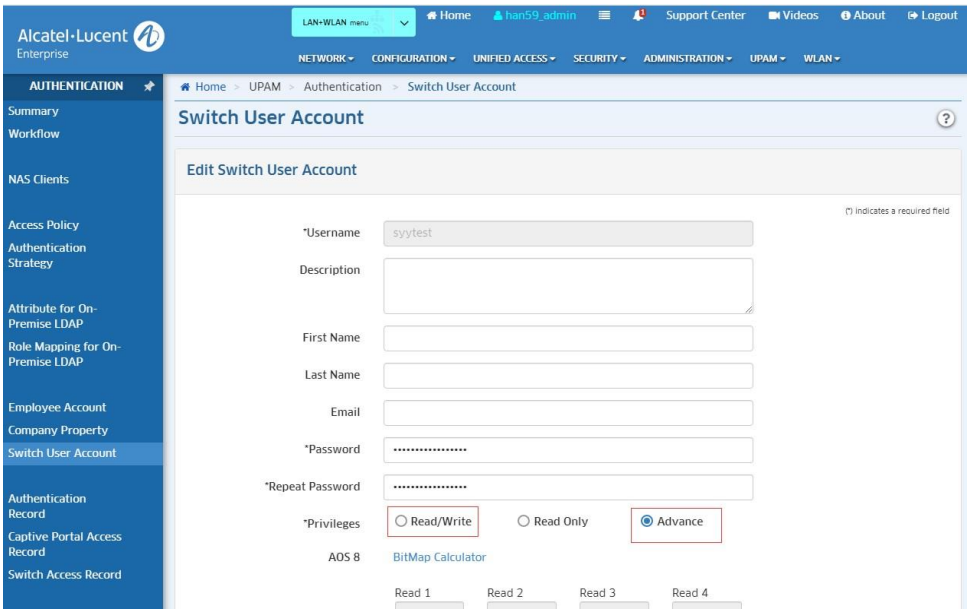
Please check whether the switch is managed by OV (shown as the picture)



If the status is OK, Please following the link: Home -> Unified Access -> Unified Profile -> Template -> Global Configuration -> AAA and check the resource of the FTP account, make sure the resource is UPAMRadiusServer (shown as the picture)



If the resource is OK. Please following the link: Home- > UPAM -> Authentication -> Switch User Account and check the privileges of the account, make sure the privileges is Read/Write or Advance, if the privileges is advance ,make sure atleast one of the family has write permission.



8.34 TCPDUMP on Wireless interface

```
support@AP-C5:70:~$ cd /tmp/
support@AP-C5:70:/tmp$ ssudo tcpdump -i ath13 -s 0 -w test1.pcap
```

capture on AP eth0 interface:

```
support@AP-C5:70:~$ cd /tmp/
support@AP-C5:70:/tmp$ ssudo tcpdump -i eth0 -s 0 -w test2.pcap
```

export/upload the capture:

`support@AP-C5:70:/tmp$ tftp -p 172.16.11.135 -l test.pcap` //172.16.11.135 is the TFTP server IP address

8.35 Troubleshooting IPv6 on Stellar AP

Check the network environment whether the DHCPv6 is configured and enabled.

On linux IPv6 server:

- ✓ Check whether the radvd and dhcpd6 process are UP

```
han@han-ThinkPad-T470p:~$ ps aux |grep radvd
han       2099  0.0  0.0  16180  1112 pts/1    S+   10:12   0:00 grep --color=auto radvd
root     12578  0.0  0.0  13056   140 ?        Ss   8月12   0:00 /usr/sbin/radvd --logmethod stderr_clean
root     12579  0.0  0.0  13056   144 ?        S    8月12   0:00 /usr/sbin/radvd --logmethod stderr_clean
han@han-ThinkPad-T470p:~$
```

```
han@han-ThinkPad-T470p:~$ ps aux  |grep dhcp
han      26605  0.0  0.0  16180  1100 pts/0    S+   14:34   0:00 grep --color=auto dhcp
dhcpd    27153  0.0  0.0  45212 15944 ?        Ss   7月31   0:25 dhcpd -user dhcpd -group dhcpd -f -6 -pf /run/dhcp-server/dhcpd6.pid -cf /etc/dhcp/dhcpd6.conf
han@han-ThinkPad-T470p:~$
```

- ✓ Check the configuration of radvd.conf.

If the AdvAutonomous is off, the AP cannot obtain any IPv6 address.

If the AdvAutonomous is on and the AdvManagedFlag is off, the AP can only obtain the stateless IPv6 address and cannot obtain the stateful IPv6 address.

If the AdvAutonomous and the AdvManagedFlag ddare both on, the AP can obtain both the stateless and stateful IPv6 address.

```
han@han-ThinkPad-T470p:~$
han@han-ThinkPad-T470p:~$ cat /etc/radvd.conf
interface enp0s31f6 {
        AdvSendAdvert on;
        AdvManagedFlag on;   stateful IPv6 switch
        AdvOtherConfigFlag on;
        prefix 2620:0:60:1480::/64 {
                AdvOnLink on;
                AdvAutonomous on;
                AdvRouterAddr on;
        };
};
```

stateless IPv6 switch

On ALE Switch OS6860:

- ✓ Check whether there is IPv6 interface with the command “show ipv6 interface”.

```
-> show ipv6 interface
Name                            IPv6 Address/Prefix Length                      Status   Device
--------------------------------+-----------------------------------------------+--------+--------------------
v6if-v55                        fe80::2efa:a2ff:fe73:15f7/64                    Active   VLAN 55
v6if-v100                       fe80::2efa:a2ff:fe73:15f7/64                    Active   VLAN 100
v6if-v200                       fe80::2efa:a2ff:fe73:15f7/64                    Active   VLAN 200
v6if-6to4                                                                       Disabled 6to4 Tunnel
loopback                        ::1/128                                         Active   Loopback
EMP-CMMA-CHAS1                  fe80::2efa:a2ff:fe73:15f6/64                    Inactive EMP

->
```

✓ Check whether the DHCPv6 service is enabled with the command “show dhcpv6-server statistics”.

```
-> show dhcpv6-server statistics
General:
  DHCPv6 Server Name            : schumacher-nt.quadritek.com,
  DHCPv6 Server Status          : Disabled,
  Total Subnets Managed         : 2,
  Total Subnets Used            : 0,
  Total Subnets Unused          : 2,
  Total Subnets Full            : 0,
  DHCPv6 Server System Up Time  : Mon Jul 20 10:28:04.445,
    Lease DB Sync time (in sec) : 60,
      Last sync time            : Tue Aug 11 10:42:26 2020,
      Next sync time            : Tue Aug 11 10:43:26 2020
```

If the AP cannot get the stateful IPv6 address, check whether the RA managed config flag is on/true with the command “show ipv6 interface v6if-interface”.

```
-> show ipv6 interface v6if-v55
v6if-v55
  IPv6 interface index          = 55(0x00000037)
  Administrative status         = Enabled
  Operational status            = Active
  Hardware address              = 2c:fa:a2:73:15:f7
  Device                        = VLAN 55
  Link-local address(es):
    fe80::2efa:a2ff:fe73:15f7/64
  Global unicast address(es):
  Anycast address(es):
  VRRP address(es):
  Joined group addresses:
    ff01::1
    ff02::1
    ff02::2
    ff02::16
    ff02::1:ff73:15f7
    ff02::1:ff00:0
  Maximum Transfer Unit (MTU)   = 1500
  Neighbor reachable time (sec) = 217
  Base reachable time (sec)     = 360
  Retransmit timer (ms)         = 1000
  Retransmit backoff            = 1
  Retransmit max                = 3
  DAD transmits                 = 1
  Send Router Advertisements    = Yes
  Maximum RA interval (sec)     = 600
  Minimum RA interval (sec)     = 198
  RA managed config flag        = False
  RA other config flag          = False
  RA reachable time (ms)        = 0
  RA retransmit timer (ms)      = 0
  RA default lifetime (sec)     = 1800
  RA hop limit                  = 64
  RA send MTU option            = No
  RA send RDNSS option          = No
  RA send DNSSL option          = No
  RA clock skew (sec)           = 600
  RA router preference          = Medium
  RA filtering                  = Disabled
  Neighbor cache limit          = None
  Local Proxy ND                = Disabled
```

- Check whether the AP version is too low.

R4.0.1 AP supports IPv4/IPv6 dual stack. R4.0.0 AP doesn't support IPv6. Check with the command "showver".

```
support@AP-28:A0:~$
support@AP-28:A0:~$ showver
4.0.0.42
support@AP-28:A0:~$ cat /etc/config/network

config interface 'loopback'
        option ifname 'lo'
        option proto 'static'
        option ipaddr '127.0.0.1'
        option netmask '255.0.0.0'

config globals 'globals'
        option ula_prefix 'fd66:ce37:fd0b::/48'

config interface 'wan'
        option ifname 'eth0'
        option type 'bridge'
        option proto 'dhcp'
        option force_link '1'
support@AP-28:A0:~$
support@AP-28:A0:~$ ifconfig br-wan
br-wan    Link encap:Ethernet  HWaddr DC:08:56:13:28:A0
          inet addr:172.16.120.72  Bcast:172.16.120.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10071 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5471 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1309041 (1.2 MiB)  TX bytes:2675671 (2.5 MiB)
```

```
support@AP-11:40:~$ showver
4.0.1.27
support@AP-11:40:~$ cat /etc/config/network

config interface 'loopback'
        option ifname 'lo'
        option proto 'static'
        option ipaddr '127.0.0.1'
        option netmask '255.0.0.0'

config globals 'globals'
        option ula_prefix 'fd66:ce37:fd0b::/48'

config interface 'wan6'
        option ifname '@wan'
        option proto 'dhcpv6'

config interface 'wan'
        option ifname 'eth0 eth1 eth2'
        option type 'bridge'
        option proto 'dhcp'
        option force_link '1'

support@AP-11:40:~$
support@AP-11:40:~$ ifconfig br-wan
br-wan    Link encap:Ethernet  HWaddr DC:08:56:51:11:40
          inet addr:172.16.120.12  Bcast:172.16.120.255  Mask:255.255.255.0
          inet6 addr: 2620:0:60:1480::2455/128 Scope:Global
          inet6 addr: 2620::60:1480:de08:56ff:fe51:1140/64 Scope:Global
          inet6 addr: fe80::de08:56ff:fe51:1140/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2032158 errors:0 dropped:1 overruns:0 frame:0
          TX packets:746798 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:299692830 (285.8 MiB)  TX bytes:235619501 (224.7 MiB)
```

Note:

Need to set the APs to be default setting after R4.0.0 APs are upgraded to R4.0.1, the upgraded APs can obtain the stateful IPv6 address. Now it needs to be optimized with PTG-1006.

```
support@AP-11:40:~$ ssudo ping -6 activation.ov.dev.ovcirrus.com
PING activation.ov.dev.ovcirrus.com (2620:0:60:1480::1802): 56 data bytes
64 bytes from 2620:0:60:1480::1802: seq=0 ttl=64 time=1.192 ms
64 bytes from 2620:0:60:1480::1802: seq=1 ttl=64 time=0.910 ms
^C
--- activation.ov.dev.ovcirrus.com ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.910/1.051/1.192 ms
support@AP-11:40:~$
support@AP-11:40:~$ ssudo ping -6 vpn40.ov.han.sqa.myovcloud.com
PING vpn40.ov.han.sqa.myovcloud.com (2620:0:60:1480::145f): 56 data bytes
64 bytes from 2620:0:60:1480::145f: seq=0 ttl=64 time=1.201 ms
64 bytes from 2620:0:60:1480::145f: seq=1 ttl=64 time=1.596 ms
64 bytes from 2620:0:60:1480::145f: seq=2 ttl=64 time=1.223 ms
^C
--- vpn40.ov.han.sqa.myovcloud.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.201/1.340/1.596 ms
support@AP-11:40:~$
support@AP-11:40:~$
support@AP-11:40:~$ ssudo ping -6 2620:0:60:1480::1100   IPv6 DNS Server
PING 2620:0:60:1480::1100 (2620:0:60:1480::1100): 56 data bytes
64 bytes from 2620:0:60:1480::1100: seq=0 ttl=64 time=1.540 ms
64 bytes from 2620:0:60:1480::1100: seq=1 ttl=64 time=1.694 ms
^C
--- 2620:0:60:1480::1100 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 1.540/1.617/1.694 ms
support@AP-11:40:~$
support@AP-11:40:~$
support@AP-11:40:~$ ssudo ping -6 private40.ov.han.sqa.myovcloud.com
PING private40.ov.han.sqa.myovcloud.com (2620:0:60:1480::2000): 56 data bytes
64 bytes from 2620:0:60:1480::2000: seq=0 ttl=64 time=1.198 ms
64 bytes from 2620:0:60:1480::2000: seq=1 ttl=64 time=1.661 ms
64 bytes from 2620:0:60:1480::2000: seq=2 ttl=64 time=1.923 ms
^C
--- private40.ov.han.sqa.myovcloud.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
```

or like below on linux DNS server:

```
                    ? MobaXterm 10.2 ?
          (SSH client, X-server and networking tools)

  ➢ SSH session to han@172.16.120.101
    ? SSH compression : ✔
    ? SSH-browser     : ✔
    ? X11-forwarding  : ✔  (remote display is forwarded through SSH)
    ? DISPLAY         : ✔  (automatically set on remote server)

  ➢ For more info, ctrl+click on help or visit our website

Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


Last login: Wed Aug 12 15:26:20 2020 from 172.16.120.109
han@han-ThinkPad-T470p:~$
han@han-ThinkPad-T470p:~$
han@han-ThinkPad-T470p:~$ cd /var/c
cache/ crash/
han@han-ThinkPad-T470p:~$ cd /var/cache/bind
han@han-ThinkPad-T470p:/var/cache/bind$ ls
db.activation.ov.dev.ovcirrus.com      db.private9.ov.han.sqa.myovcloud.com  db.vpn9.ov.han.sqa.myovcloud.com  managed-keys.bind.jnl
db.private40.ov.han.sqa.myovcloud.com  db.vpn40.ov.han.sqa.myovcloud.com     managed-keys.bind
han@han-ThinkPad-T470p:/var/cache/bind$
han@han-ThinkPad-T470p:/var/cache/bind$
han@han-ThinkPad-T470p:/var/cache/bind$ cat db.activation.ov.dev.ovcirrus.com
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
;@      IN      A       127.0.0.1
;@      IN      AAAA    ::1
@       IN      A       172.16.120.105
@       IN      AAAA    2620:0:60:1480::1802
han@han-ThinkPad-T470p:/var/cache/bind$
han@han-ThinkPad-T470p:/var/cache/bind$ cat db.private40.ov.han.sqa.myovcloud.com
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
;@      IN      A       127.0.0.1
;@      IN      AAAA    ::1
@       IN      A       172.16.120.102
@       IN      AAAA    2620:0:60:1480::2000
;@       IN      AAAA    2620:0:60:1480::2200
han@han-ThinkPad-T470p:/var/cache/bind$
han@han-ThinkPad-T470p:/var/cache/bind$ cat db.vpn40.ov.han.sqa.myovcloud.com
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
;@      IN      A       127.0.0.1
;@      IN      AAAA    ::1
@       IN      A       172.16.120.103
@       IN      AAAA    2620:0:60:1480::145f
;@       IN      AAAA    2620:0:60:1480::1450
han@han-ThinkPad-T470p:/var/cache/bind$
han@han-ThinkPad-T470p:/var/cache/bind$
han@han-ThinkPad-T470p:/var/cache/bind$
```

Check the AP information on the Device Catalog page whether the license has been assigned.

If not, please add license for it by clicking the icon “Assign License” or Clicking the icon “Manage Device Licenses”.
Check whether the AP is in the list of Network—Access Points—Unmanaged APs
If the Device Status in the Device Catalog is “provisioning Failed”, please check whether the AP is in the Unmanaged AP list. IF yes, please trust it first.
Check the ocloud_show information and the activation_client log and vpn log in CLI.
View the ocloud_show information

```
support@AP-11:40:~$ ocloud_show
AP Work Mode:OVCLOUD
AP Date:Thu Aug 13 15:13:49 2020
AP IP:172.16.120.12
VPN Status:connected
VPN Assigned IP:10.8.0.6
VPN DPD:600
deviceCloudGroup:
cloudProcessStatus:completeOK
DHCP Server:
Activation Server: https://activation.ov.dev.ovcirrus.com
Failed to connect to ubus
NTP Server list: clock0.ovcirrus.com clock1.ovcirrus.com clock2.ovcirrus.com clock3.ovcirrus.com
echo DNS Server: 2620:0:60:1480::1100
Proxy Server:
VPN Server:vpn40.ov.han.sqa.myovcloud.com
ovMqtt:private40.ov.han.sqa.myovcloud.com:1883
ovFqdn:public40.ov.han.sqa.myovcloud.com:443
Image Server:
Time to next Call Home(sec):285
```

Check the activation_client.log

If the activation server is not reachable, please check the network.

- If “failedToGetCertificate“ is in the log, please wait 30 minutes or reboot the AP because it shall take 15 mins for the activation server to produce the certificate.
- If the “clientCertificatePreviousIuIssued” is in the log, please delete the AP information in the device catalog page and add it again and do reboot to the AP
- If “vpnConfigFailed” is in the log

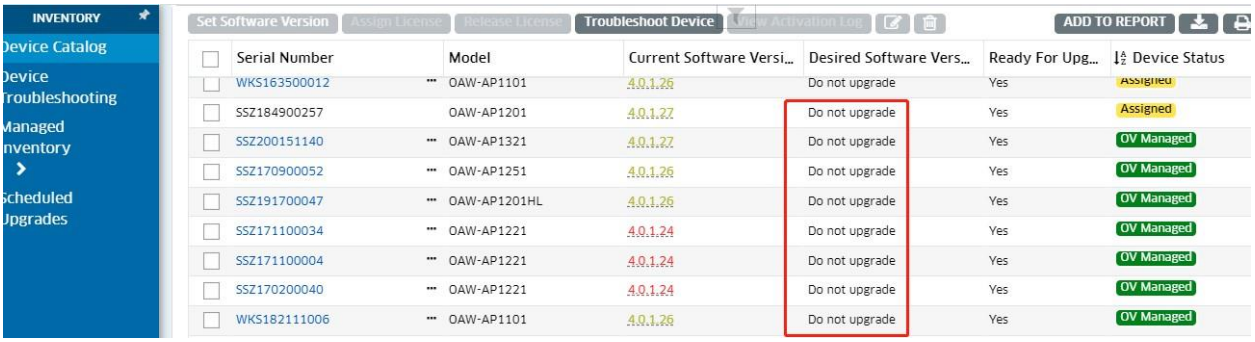
First check whether the DNS server works normally, Execute the operation of nslookup if the URL cannot be analyzed, please continue to check the configuration of DNS server

- If the URL can be analyzed , please check whether the VPN server works normally, you can use ping, if the URL cannot be reachable , there maybe something wrong with the VPN server ,you can check it
- If "cloudProcessStatus":"completeOK“ is in the log but the AP still cannot register to the TOV , there maybe loss an route in TOV , please check it.

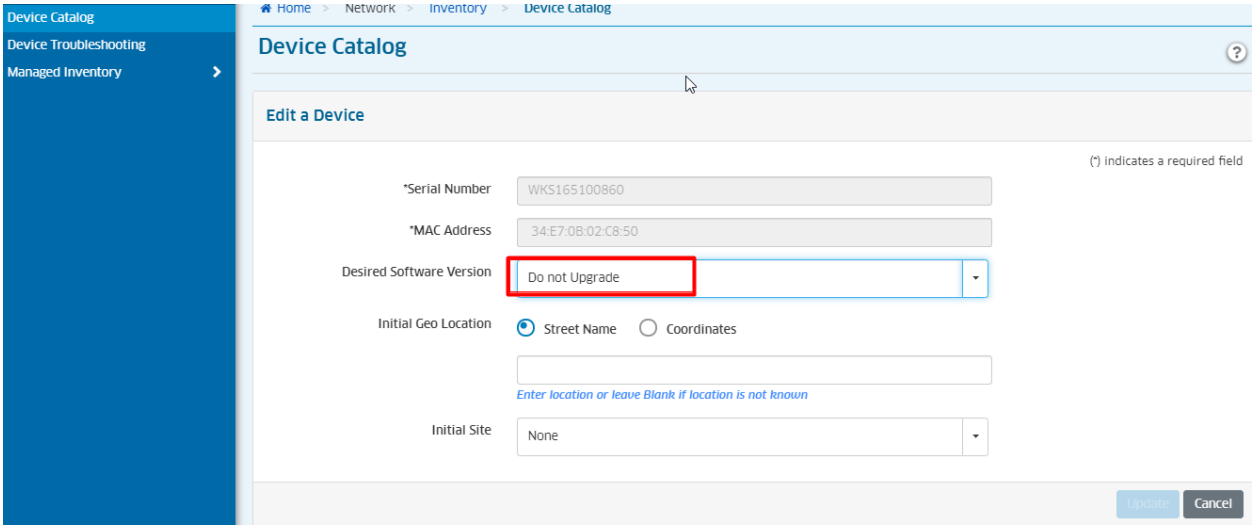
```
root@luqiuyin-VirtualBox:~# route -n
内核 IP 路由表
目标            网关            子网掩码        标志  跃点   引用  使用 接口
0.0.0.0         172.16.120.1    0.0.0.0         UG    0      0        0 ens33
10.8.0.0        172.16.120.103  255.255.0.0     UG    0      0        0 ens33
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 ens33
172.16.120.0    0.0.0.0         255.255.255.0   U     0      0        0 ens33
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
172.18.0.0      0.0.0.0         255.255.0.0     U     0      0        0 br-da6a3876a1a2
```

If the upgrade failed is in the log, please check whether the "Desired Software Version" is “Do not upgrade” in the Device Catalog

If not, please edit it to be "Do not upgrade " , otherwise you need wait until the AP can upgrade successfully



change the AP’s software version to be "Do not upgrade.»

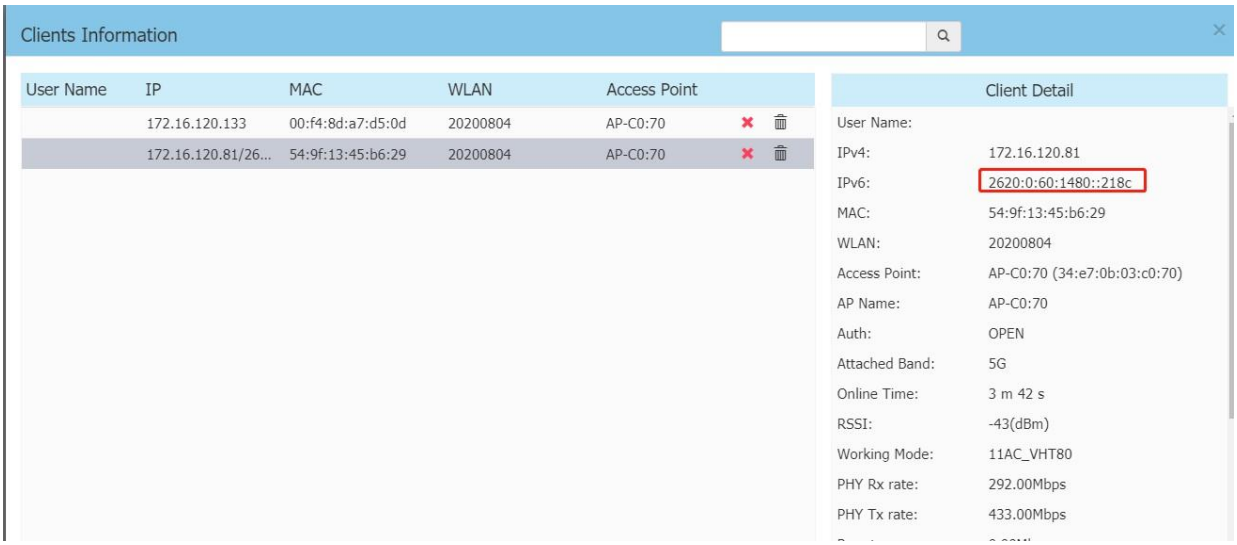


Check the vpn log in root account with the command "cat /tmp/log/vpn_manage.log "
If the clients' IPv6 address cannot be displayed on cluster/OVC web UI.
Only the stateful IPv6 address can be displayed for IPv6 client now as shown in below screenshots. The stateless IPv6 address for the IPv6 client won't be displayed.

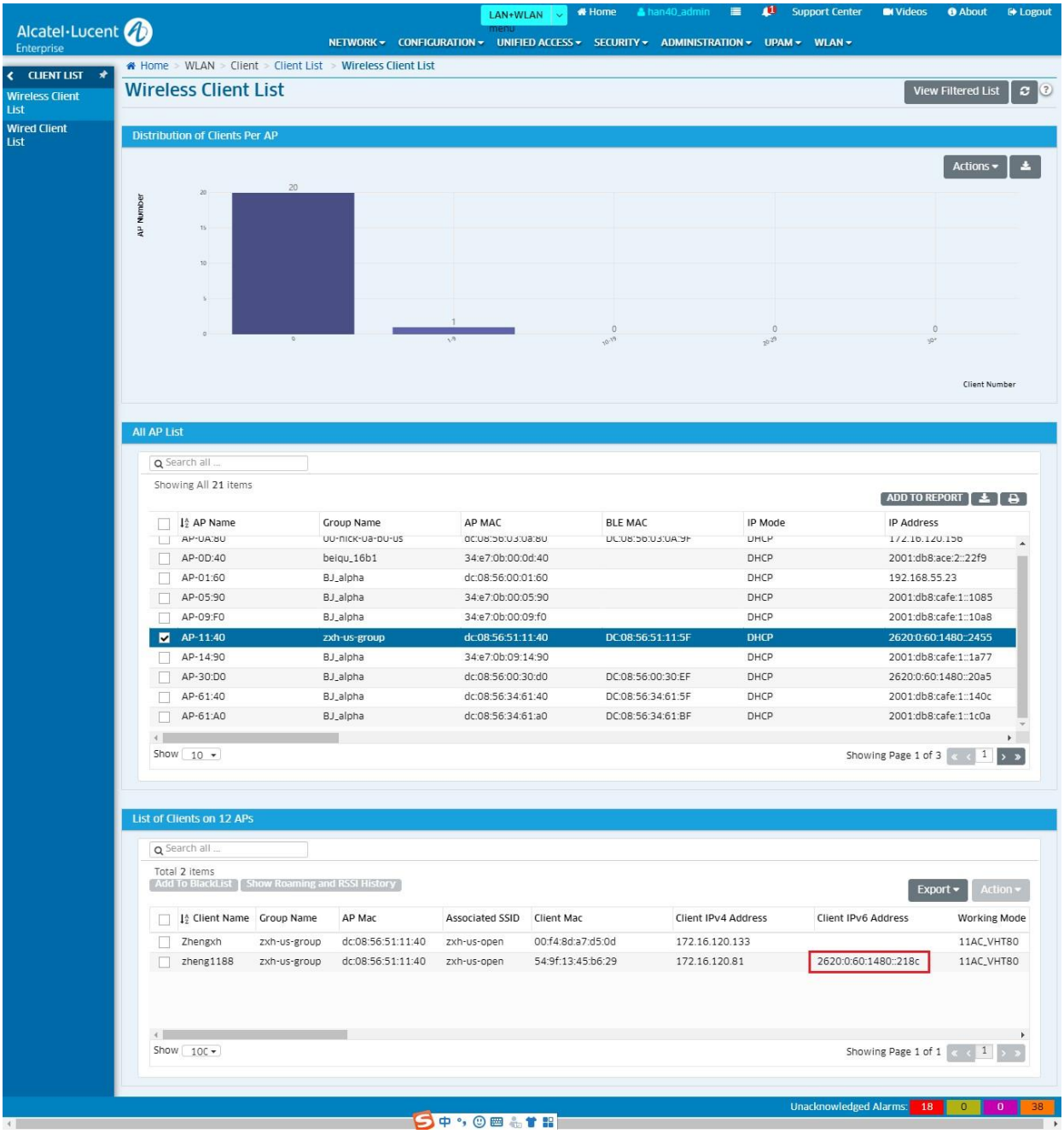
The result of sta_list:

```
support@AP-C0:70:~$ ssudo sta_list
SSID:20200804
STA_MAC              IPv4            IPv6                    OnlineTime      RX      TX          FREQ    AUTH    Final_role                  VLANID  TUNNE
LID  FARENDIP
SSID:20200804
STA_MAC              IPv4            IPv6                    OnlineTime      RX      TX          FREQ    AUTH    Final_role                  VLANID  TUNNE
LID  FARENDIP
00:f4:8d:a7:d5:0d  172.16.120.133                              27            171088        9862     5GHz OPEN    1596511743649arp            0     0
54:9f:13:45:b6:29  172.16.120.81     2620:0:60:1480::218c      929           90070         42860    5GHz OPEN    1596511743649arp            0     0
support@AP-C0:70:~$
support@AP-C0:70:~$
```

Clients Information on cluster web UI.



Clients Information on OVC web UI.



Note:
When the IPv6 clients are Windows type, its stateful IPv6 address cannot be displayed now though they have obtained both stateful and stateless IPv6 address.
Android clients cannot obtain the stateful IPv6 address. Stateless IPv6 address is OK.

8.36 Troubleshooting Zigbee application

- Wmaagent log.

  Command : tail -f /tmp/log/wmaagent.log

  For Example: OV set Zigbee configuration to AP

```
[2020-11-04 10:38:39]Main Receive from WMA msgtype=zigbee-manager.zigbee_config ,message={"version":"3.0","messageID":"d10abafd-6713-4456-87aa-
8c07f0478454","method":"zigbee-manager.zigbee_config","macAddress":"dc:08:56:34:7b:00","contents":{"ZigbeeParams":{"mgmt":{"stype":"OVE","sn":"
","region":"tenant.group","tenant":"","group":"mdns_duxn2"},"ZigbeeBeacon":{"ExpanidList":"00:17:7A:01:02:03:04:05","DiscoveryDuration":120,"Ch
annel":0,"Panid":31488,"Txpower":16,"DiscoverySwitch":"On"},"IotParams":{"RadioMode":"Zigbee"},"ZigbeeConfig":{"ZigbeeSwitch":"On","VendorOuiSw
itch":"Off","NetworkType":"Specific","FilterMode":"FilterOui","Prefix":"Door","VendorOui":"","Workmode":"Coordinator","Expanid":"Specific"},"Ou
iList":[]}}}
[2020-11-04 10:38:39]Main Send to WMA msgtype=zigbee-manager.zigbee_config,message={ "version": "3.0", "messageID": "d10abafd-6713-4456-87aa-8c
07f0478454", "method": "zigbee-manager.zigbee_config", "macAddress": "DC:08:56:34:7B:00", "contents": { "success": true, "error": { "errorCode"
: 0, "errorMessage": "" } } }
[2020-11-04 10:39:48]Main Receive from WMA msgtype=zigbee-manager.get_gateway_info ,message={"version":"3.0","messageID":"","method":"zigbee-ma
nager.get_gateway_info","macAddress":"DC:08:56:34:7B:00","contents":{}}
[2020-11-04 10:39:48]Main Send to WMA msgtype=zigbee-manager.get_gateway_info,message={ "version": "3.0", "messageID": "", "method": "zigbee-ma
nager.get_gateway_info", "macAddress": "DC:08:56:34:7B:00", "contents": { "success": "false", "error": { "errorCode": "1", "errorMessage": "The
 service is not be support" } } }
[2020-11-04 10:39:48]Main Receive from WMA msgtype=zigbee-manager.get_endpoint_info ,message={"version":"3.0","messageID":"","method":"zigbee-m
anager.get_endpoint_info","macAddress":"DC:08:56:34:7B:00","contents":{}}
[2020-11-04 10:39:48]Main Send to WMA msgtype=zigbee-manager.get_endpoint_info,message={ "version": "3.0", "messageID": "", "method": "zigbee-m
anager.get_endpoint_info", "macAddress": "DC:08:56:34:7B:00", "contents": { "success": "false", "error": { "errorCode": "1", "errorMessage": "T
he service is not be support" } } }
[2020-11-04 10:40:47]Main Send to WMA msgtype=zigbeeregist,message={ "version": "3.0", "messageID": "1677582688", "method": "zigbeeregist", "ma
cAddress": "DC:08:56:34:7B:00", "contents": { "success": "true", "error": { "errorCode": "", "errorMessage": "" }, "RegistInfo": { "ZigbeeSwitc
h": "On", "Workmode": "Coordinator", "PanId": 31488, "Channel": 20, "TxPower": 16, "ApMac": "DC:08:56:34:7B:00", "Prefix": "Door", "DeviceEui":
 "DE:08:56:FF:FE:34:7B:00" }, "mgmt": { "sn": "", "stype": "OVE", "region": "tenant.group", "tenant": "", "group": "mdns_duxn2" } } }
[2020-11-04 10:40:47]Main Receive from WMA msgtype=zigbeeregist ,message={"version":"3.0","messageID":"","method":"zigbeeregist","macAddress":"
DC:08:56:34:7B:00","contents":{"DeviceInfo":[],"success":"true"}}
```

- Zigbee log:

  After set zigbee, zigbee will appear in the log list, but not show up right away.

```
support@AP-7B:00:/tmp/log$ ls
Json.log                        dhcp.log                        fix_mode.log                    roam_track.log
activation_clientd.log          dhcp_relay.log                  iot-radio                       sysstat
agm.log                         dns_snooping.log                iot.log                         tid_umod.log
arp-proxy.log                   dpi.log                         lastlog                         um_monitor.log
behaviortrack.log               drm.log                         lbd.log                         wam.log
bt                              drm.log_20201104_074844.tar.gz  lighttpd                        wam.log_back.tar.gz
cert.log                        drm_2.4g.log                    lldp.log                        wam_info.log
cert_manage.log                 drm_5g.log                      msr.log                         wland.log
clienttrack.log                 drm_5g_bandwidth.log            netifd.log                      wmaagent.log
collect_log_manager.log         drm_5g_high.log                 netmgr.log                      wpa.log
configd.log                     drm_5g_high_bandwidth.log       power_manage.log                wtmp
core-mon-app-restore-syslog.txt eag.log                         rap.log                         zigbee
ddns                            eag.log.bak                     roam.log
```

  Show zigbee log to make sure whether scanning is beginning or is end:

  support@AP-7B:00:/tmp/log/zigbee$ tail -f zigbeed.log

```
2020-11-04 10:40:31(000004,483) [z-app] - SetDiscoveryDurationFalse...
2020-11-04 10:40:31(000004,483) [af-main-host] - pJoin for 120 sec: 0x0
2020-11-04 10:40:47(000019,739) [z-ubus] - UbusGetRegistInfo
2020-11-04 10:40:47(000019,739) [z-app] - SetZcsStatusTrue...
2020-11-04 10:40:47(000019,739) [af-main-host] - GetRegistInfo zigbee_switch:1, zigbee_workmode:1,     panid:0x7b00, channel:20, tx_power:16
2020-11-04 10:40:47(000019,739) [af-main-host] - GetRegistInfo: eui: DE:08:56:FF:FE:34:7B:00
2020-11-04 10:40:47(000019,740) [z-utils] - GetApMacColon - size: 18
2020-11-04 10:40:47(000019,821) [z-utils] - GetApMacColon - mac: DC:08:56:34:7B:00
2020-11-04 10:40:47(000019,958) [z-ubus] - UbusUpdateDeviceList
2020-11-04 10:40:47(000019,958) [z-ubus] - UbusUpdateDeviceList - update_device_list: {"DeviceInfo":[],"success":"true"}
2020-11-04 10:40:47(000019,958) [z-utils] - func: ParseDeviceList
2020-11-04 10:40:47(000019,958) [z-ubus] - update_device_list error - deviceNum: 0
2020-11-04 10:40:47(000019,958) [z-ubus] - send_cmd_result
2020-11-04 10:40:49(000022,320) [af-main-host] - keep alive - panId: 0x7b00, channel: 20, power: 16, status: 0x0, timestamp: 1604457649
2020-11-04 10:41:09(000042,425) [af-main-host] - keep alive - panId: 0x7b00, channel: 20, power: 16, status: 0x0, timestamp: 1604457669
2020-11-04 10:41:29(000062,530) [af-main-host] - keep alive - panId: 0x7b00, channel: 20, power: 16, status: 0x0, timestamp: 1604457689
2020-11-04 10:41:48(000080,674) [z-ubus] - UbusGetGatewayInfo
2020-11-04 10:41:48(000080,674) [af-main-host] - GetGatewayInfo zigbee_switch:1, zigbee_workmode:1,     panid:0x7b00, channel:20, tx_power:16
2020-11-04 10:41:48(000080,674) [af-main-host] - GetGatewayInfo: eui: DE:08:56:FF:FE:34:7B:00
2020-11-04 10:41:48(000080,674) [z-utils] - GetApMacColon - size: 18
2020-11-04 10:41:48(000080,753) [z-utils] - GetApMacColon - mac: DC:08:56:34:7B:00
2020-11-04 10:41:48(000080,753) [z-ubus] - UbusGetGatewayInfo - panid_hex: 0x7b00
2020-11-04 10:41:48(000080,803) [z-ubus] - UbusGetEndpointInfo
2020-11-04 10:41:48(000080,803) [af-main-host] - GetEndpointInfo .
2020-11-04 10:41:48(000080,803) [z-app] - SetEndpointInfoTrue...
2020-11-04 10:41:48(000080,816) [af-main-host] - GetEndpointInfoEvent .
2020-11-04 10:41:48(000080,821) [af-main-host] - GetEndpointInfoEvent endpoint size: 32
2020-11-04 10:41:48(000081,044) [z-app] - SetEndpointInfoFalse...
2020-11-04 10:41:48(000081,045) [af-main-host] - GetEndpointInfo Success.
2020-11-04 10:41:50(000082,859) [af-main-host] - keep alive - panId: 0x7b00, channel: 20, power: 16, status: 0x0, timestamp: 1604457710
2020-11-04 10:42:10(000102,966) [af-main-host] - keep alive - panId: 0x7b00, channel: 20, power: 16, status: 0x0, timestamp: 1604457730
2020-11-04 10:42:30(000123,068) [af-main-host] - keep alive - panId: 0x7b00, channel: 20, power: 16, status: 0x0, timestamp: 1604457750
2020-11-04 10:42:34(000127,489) [af-main-host] - timer Handler.
2020-11-04 10:42:34(000127,494) [af-main-host] - close network: 0x0
2020-11-04 10:42:50(000143,172) [af-main-host] - keep alive - panId: 0x7b00, channel: 20, power: 16, status: 0x0, timestamp: 1604457770
```

  The default IoT mode of AP is BLE, if you set Zigbee configuration to AP at first time, the AP will upgrade firmware. Theprocess will spend about 120 S, during this time, if you set other configuration about IoT, the AP will not response for it. In fact, every time you change IoT mode, the AP will upgrade firmware.

  The AP which supports Zigbee Protocol currently including: OAW-AP1201, OAW-AP1201BG, OAW-AP1321, OAW-AP1322, OAW-AP1361, OAW-AP1361D, OAW-AP1362, OAW-AP1311.

  There are three conditions for Lock join AP:

  AP open Zigbee network (Zigbee Discovery)

  AP will need about 120S to change IoT Radio Mode, so if you set Zigbee switch ON to AP, it can’t work .

After the Zigbee Duration time, the AP will close Zigbee network, new Lock can’t join AP.
Lock searching for Zigbee network at the same time (Discovery Card

Vendor OUI is set, so we must open Vendor OUI Switch.

- Check if AP is working on Zigbee Mode

```
support@AP-6C:40:/tmp/log/zigbee$ cat /etc/config/iot_radio.conf
{
      "IotRadioParams":{
              "RadioMode":"Zigbee",
              "BleVersion":{
                      "major":2,
                      "minor":13,
                      "patch":6,
                      "build":327,
                      "bootloader":17104897,
                      "version":"1.0.3.1"
              },
              "ZigbeeVersion":{
                      "major":6,
                      "minor":5,
                      "patch":5,
                      "build":432
              }
          }
}
```

- Check to make sure AP and Lock are opening Zigbee Network at the same time
- Check to make sure Vendor OUI switch is ON
- For the interference from the same channels and the adjacent channels.

The channel we suggested [11/15/16/19/20/21/25/26], the channel only can be set in Use Private Config.

If your VisionlineServer displays following errors, that means the System Time is different with OV.

The System Time of OV and Server can’t differ by more than 20 Minutes.

After Lock become Orphan Join, some channel of the lock won't give Orphan Join Signal, we must avoid these channels, the channel suggested [11 ， 15， 16， 19， 20， 21， 25， 26]

8.37 Reflexive policies troubleshooting

1. The reverse strategy may affect the DPI function not working, please check:

   Is reflexive set to "NO"?

   Because DPI depends on first 15 packets of the same conntrack session, it might not work if the traffic matches --NOTRACK policy.

   Please configure "Yes" for reflexive.
2. If the reverse strategy function does not take effect, please check:
   (1) Please check whether there is a "Unified Policies" file with Reflexive="No". If there is, please change it to "Yes" and reapply it to the AP, because the mixed use of reflexive is not supported in 4.5R2.
   (2) If only "Unified Policies" is created.

- Please check if "Default List" is configured as NO. If it is configured as "No" and no policy list is bound, it will not be applied to the AP. Please configure "Default List" to Yes.

  (3) If a "Unified Policy List" is created.
- Please check whether the "Unified Policies" file is bound to the "Unified Policy List".
- Please check whether the "Unified Policy List" is bound to the "Access Role Profile" of the SSID.

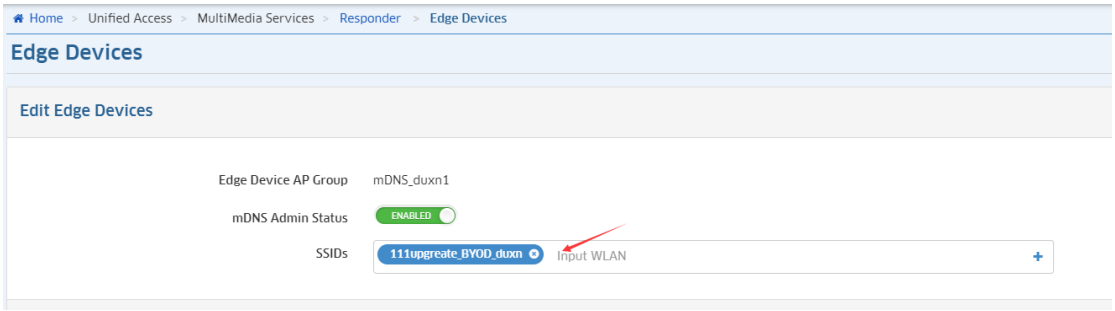
8.38 mDNS troubleshooting

If you cannot find the shared service device:

- Please check the AP model. Currently only AP1101 does not support it, and other models can be supported.
- Please check whether the mDNS switch is turned on;

```
support@AP-D9:A0:~$
support@AP-D9:A0:~$ cat /tmp/config/ms_relay.conf
{
"MDns": [
  {
    "mDnsAdminStatus":"ENABLED",
    "responder":{
      "ipAddress":"10.0.0.1",
      "mac":"2c:fa:a2:73:15:f7"
    },
    "ssdpAdminStatus":"DISABLED",
    "ssidList":[
      "2221x_BYOD_duxn",
      "222upgreate_BYOD_duxn"
    ]
  }
]
}
support@AP-D9:A0:~$
```

- Please check whether the server and client are both connected to the SSID;
- Please check whether the SSID accessed by the server and client has been added to the ssid list of mDNS;



- Please check whether a rule is added, and the user can match the rule;
- Please check whether the shared account is an Employee Account;
- Please check whether the shared device has passed BYOD certification;
- Please check whether the shared device is online or has remembered information

8.39 Web Content Filtering troubleshooting

Step1: check if the WCF is enabled on AP

```
cat /tmp/config/wcf.conf
```

Step2: check that client is associated to ARP with WCF profile

```
ssudo sta_list
cat /tmp/config/access_role.conf
```

Step3: check the wmaagent.log to ensure AP received the response from OV 2500

```
cat /var/log/wmaagent.log | grep wcf_response
```

If both wcf.log and wmaagent.log have no response but in wmaagent.log we can see the FQDN request, we must investigate on OV logs /opt/OmniVista_2500_NMS/logs/ucc/UCC.log

Note that 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.

In this case, we can use another client to connect the WLAN and try to open the same website, if user can not open the website, so there is no issue about WCF. We can use command to check whether the website be dropped by WCF policy

Step4: generate the cache file to list the filtered URL

```
ubus call wcf-manager generate_cache_file
cat /tmp/wcf_cache_list.txt (verdirct:[1] means:accept, verdirct:[0] means:drop)
```

8.40 Device name is not displayed for Open/PSK/portal authentication

If the client performed a roaming to another Stellar AP, the client should retain its network config and do not perform aDHCP request, as a consequence, the new associated Stellar AP does not have the DHCP information with client name, client name will be empty on the OV 2500 WLAN client list

8.41 160MHz channel width support in RF Profile Troubleshooting

If AP is working on 160MHz channel width the ath rate should be 2.4019Gb/s for AP 1321/1361

```
support@AP-0A:E0:~$ iwconfig ath11
ath11     IEEE 802.11axa  ESSID:"1x-ax-4k"
          Mode:Master  Frequency:5.22 GHz  Access Point: DC:08:56:76:0A:F0
          Bit Rate:2.4019 Gb/s   Tx-Power=1 dBm
          RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality=88/94  Signal level=-59 dBm  Noise level=-93 dBm (BDF averaged NF value in dBm)
          Rx invalid nwid:4294285  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

The ath rate should be 4.9039 Gb/s for 1351

If the current country code, combined channel, or power device does not support 160Mhz, when AP gets 160MHz configuration, it will choose the maximum bandwidth, such as 80MHz
Run command “iwpriv athXX get_mode” to make sure the AP is working on 160MHz channel width
Check the rfprofile.conf to make sure 160MHz configuration is saved.

Check the log to make sure 160MHz configuration is issued: `cat /tmp/log/wland.log`

8.42 CSA support in RF Profile Troubleshooting

When the Automatic Channel Selection is enabled, we can turn on the CSA. In the AP `/tmp/config/rfprofile.conf` check the csastatus is enabled and the csa count is set (default 4)

```
cat /tmp/log/wland.log | grep csa
2023-04-05 09:24:21(1363779,011) [wland] - [ ubus call drm config_drm … csaStatus":"enable",
"csa":4}}}' ] --- [ubus.c:rfSendConfigBySystem():9402]
```

Check the DRM log if CSA takes effect: `cat /tmp/log/drm.log | grep csa`

```
2023-04-01 23:26:36(1068563,816) [LOG] - [my config:wifi1_meshmode=0,
wifi2_meshmode=0,wifi0_antenna_gain=255,wifi1_antenna_gain=255,wifi2_antenna_gain=255,wifi0_cli
entawareness=0,wifi1_clientawareness=1,wifi2_clientawareness=1,wifi0_csa_enable=1,wifi1_csa_ena
ble=1,wifi2_csa_enable=1,wifi0_csacount=4,wifi1_csacount=4,wifi2_csacount=4]--
[ubus_interface.c:2224]
2023-04-02 03:16:03(1082330,899) [LOG] - [drm set channel exttool --chanswitch --interface
wifi2 --chan 112 --chwidth 0 --numcsa 4]--[icm.c:2150]
```

8.43 Allow List in Client Isolation Troubleshooting

Check the Client isolation is enabled in `cat /tmp/config/wlanservice`.conf and in logs `cat /tmp/log/wland.log | grep isolate`
Check the Client isolation allowed list is received from OV with command `cat /tmp/log/wmaagent.log` and added in config with command `cat /tmp/config/access_role.conf`
Check the SSID and ARP used are correct where Client isolation is enabled
In the iptables rules, the Client isolation allowed list is created in the OUTPUT policy (policy ACCEPT):

```
support@AP-C0:A0:~$ ssudo iptables -nvL
Chain INPUT (policy ACCEPT 977 packets, 193K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 1138 packets, 640K bytes)
 pkts bytes target     prot opt in     out     source               destination
36692   16M MSR        all  --  *      *       0.0.0.0/0            0.0.0.0/0
36692   16M CP_DNSS    all  --  *      *       0.0.0.0/0            0.0.0.0/0
28212   13M CP_FILTER  all  --  *      *       0.0.0.0/0            0.0.0.0/0
28847   13M isolation_cli  all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT 728 packets, 105K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain 111-hu-guest (1 references)
 pkts bytes target     prot opt in     out     source               destination
  448  151K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            MAC destination MAC 00:1F:64:12:03:48
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            MAC destination MAC 00:13:32:FF:FF:FF/FF:FF:FF:00:00:00
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            MAC destination MAC 88:3C:93:FF:FF:FF/FF:FF:FF:00:00:00
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            MAC destination MAC DC:08:56:FF:FF:FF/FF:FF:FF:00:00:00
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            MAC destination MAC 34:E7:0B:FF:FF:FF/FF:FF:FF:00:00:00
  110 28405 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            MAC destination MAC 01:FF:FF:FF:FF:FF/FF:00:00:00:00:00
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            MAC destination MAC FF:FF:FF:FF:FF:FF
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            MAC destination MAC 02:E6:A9:A3:2E:F8
    0     0 __111-hu-guest  all  --  *      *       0.0.0.0/0            0.0.0.0/0            MAC source MAC 02:E6:A9:A3:2E:F8
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain CP_DNSS (1 references)
 pkts bytes target     prot opt in     out     source               destination
27589   13M WL_ARP_2   all  --  *      *       0.0.0.0/0            0.0.0.0/0
27836   13M WL_ARP_0   all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain CP_FILTER (1 references)
 pkts bytes target     prot opt in     out     source               destination
28210   13M CP_F_DEFAULT  all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain CP_F_DEFAULT (1 references)
 pkts bytes target     prot opt in     out     source               destination
 2629 3061K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            source IP range 88.1.1.3-88.1.1.3
 2736  264K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            destination IP range 88.1.1.3-88.1.1.3
  278 39065 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:53
  278 18215 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:53
   89 29492 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:67
   48 15744 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:67
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:68
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:68

Chain MSR (1 references)
 pkts bytes target     prot opt in     out     source               destination

Chain WL_ARP_0 (1 references)
 pkts bytes target     prot opt in     out     source               destination

Chain WL_ARP_2 (1 references)
 pkts bytes target     prot opt in     out     source               destination

Chain __111-hu-guest (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            MAC destination MAC 02:E6:A9:A3:2E:F8
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            MAC destination MAC 54:48:10:A2:86:24

Chain isolation_cli (1 references)
 pkts bytes target     prot opt in     out     source               destination
  558  180K 111-hu-guest  all  --  *      *       0.0.0.0/0            0.0.0.0/0            MAC source MAC 02:E6:A9:A3:2E:F8
support@AP-C0:A0:~$
```

SSID interface chain for client connection

ARP chain with client isolation allowed list

Online client

8.44 Update certificate for Captive Portal on AP Troubleshooting

Check if the certificate is successfully loaded and enabled with commands `ls /etc/user_cert/` and `cat /tmp/config/cert_list.conf`

```
support@AP-60:40:~$ ls /etc/user_cert/
server2.pem  server3.pem
support@AP-60:40:~$ cat /tmp/config/cert_list.conf
{
        "cert_cfg":[
                {
                        "cert_type":"Internal_Portal",
                        "cert_name":"2222",
                        "cert_filename":"server2.pem",
                        "cert_format":"PEM",
                        "cert_passwd":"68182ce2a066941a9ff482601def0c32",
                        "cert_url":"hu.portal-test222.com",
                        "cert_enable":"disable"
                },
                {
                        "cert_type":"Internal_Portal",
                        "cert_name":"1111",
                        "cert_filename":"server3.pem",
                        "cert_format":"PEM",
                        "cert_passwd":"",
                        "cert_url":"hu.portal-test333.com",
                        "cert_enable":"enable"
                }
```

Check whether the portal URL is correct after the certificate is updated with command `cat /tmp/log/eag.log`

```
support@AP-60:40:~$ cat /tmp/log/eag.log |grep set_domain
[2022-11-01 16:12:54]:  eag_ins.c:9487:eag_set_dns_resolve cmd=ubus call dnsrd set_domain '{"cmd":"add","url":"hu.portal-test333.com","ip":"1.1.1.1","ip6":"fe80::8a3c:93ff:fe00:6040","type":"ExPortal"}'
support@AP-60:40:~$
```

8.45 AP running in restricted mode (no enough power) Troubleshooting

When AP does not receive enough power from switch, AP will run in restricted mode and some side effects could be observed like no SSID broadcasted, no LLDP frames generated. Below the description of functions when AP is running in restricted mode:

port&power supply		work mode	Description
eth0	eth1		
802.3bt type3	N/A	High power mode	Full Function
802.3bt type4	N/A	High power mode	Full Function
N/A	802.3bt type3	High power mode	Full Function
N/A	802.3bt type4	High power mode	Full Function
802.3at	802.3at	Limit power mode	USB disabled
802.3at	802.3af/NULL	Low power mode	1. USB disabled 2. DBDC 2*2 work mode 3. eth1 port disabled
802.3af/NULL	802.3at	Low power mode	1. USB disabled 2. DBDC 2*2 work mode 3. eth0 port disabled
802.3af/NULL	802.3af/NULL	Low power mode	1. USB disabled 2. DBDC 2*2 work mode

Check if AP is running in restrict mode with command `cat /tmp/power_manage.conf`

```
{
                "board_info":"ap351",
                "power_mode":"POE",
                "poe_level":"802.3at dual",
                "power_manage":true,
                "msg_info":"Limit power mode: Disable USB"
}
```

8.46 Bypass and Trust Tag Troubleshooting

This feature is supported on models 1201H/1201HL/1301H/1311

Trust tag and Bypass cannot bind the same VLAN ID to one Downlink port. For instance we cannot apply Trust tag 10 to downlink port 1 and then apply the Bypass VLAN 10 to same downlink port 1.

On AP1311 and 1301H, the Bypass and Trust tags only support unicast packets

This feature is not supported on Mesh network

Check the config is applied with command `cat /tmp/config/access_auth_profile.conf` and check the correct downlink ports is bound to bridge-vlan with command `brctl show`

8.47 SNMPv3 Troubleshooting

With any MIB Browser you can explore the Stellar AP MIBs, the authentication protocol is SHA, privacy protocol is AES-128.

Check the config with command `cat /tmp/config/snmptrap.conf`

```
{ "trap_config": { "status": "on", "trap_community": null, "trap_server": "192.168.10.200",
"version": "v3", "username": "test", "password": "3236e9e1c70a76b5199e60e53e9eaffe" } }
cat /tmp/config/snmpmib.conf
{ "snmp_config": { "status": "on", "community": null, "version": "v3", "username": "test",
"password": "3236e9e1c70a76b5199e60e53e9eaffe" } }
```

8.48 GRE Tunnel resiliency Troubleshooting

Check the GRE Tunnel resiliency (Primary/Backup) is applied with command cat /tmp/config/access_role.conf. farEndIP and farEndIP2 with preemption enabled shall be present.

8.49 Wifi Analytics and Quality User Experience troubleshooting

You can refer to Troubleshooting page: https://docs.ovcirrus.com/ov/Troubleshooting.546504705.html

Step1: Check the configuration file of your Access Points. Your server key should be set to the correct region:

- APAC region: broker.apac.analytics.ovng.myovcloud.com:9093
- US region: broker.us.analytics.ovng.myovcloud.com:9093
- EU region: broker.eu.analytics.ovng.myovcloud.com:9093

Step2: Check that process is loaded:

```
support@AP-2D:40:~$ ps | grep mdps 3641 support     1332 S      grep mdps
30177 root      16960 S     /sbin/mdps -c /tmp/config/qoe.conf
```

Step3: Check that data are well sent to OmniVista Cirrus 10.x platform:

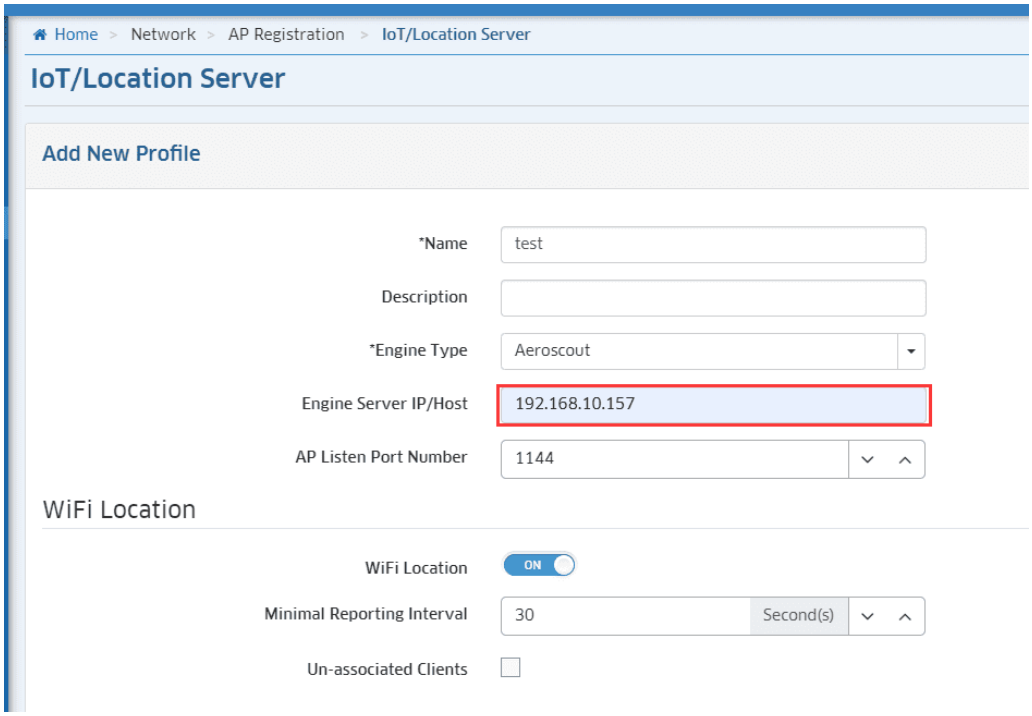
```
support@AP-2D:40:~$ cat /var/log/mdps.log
2021-09-27 02:21:54(251102,949) [MDPS] - Uploader Enqueued apinfo.report message (2415 bytes)
for topic ext_ov_qoe_events
2021-09-27 02:21:54(251102,950) [MDPS] - Uploader Enqueued shortapinfo.report message (635
bytes) for topic ext_ov_qoe_events
2021-09-27 02:21:55(251103,566) [MDPS] - Uploader Enqueued apradioinfo.report message (955
bytes) for topic ext_ov_qoe_events
2021-09-27 02:21:55(251103,711) [MDPS] - Uploader Enqueued apwlaninfo.report message (1508
bytes) for topic ext_ov_qoe_events
```

If after following these steps you are still not able to get data, please open an eSR and collect the support logs from the OmniVista interface. Please connect to your OmniVista 2500 / OmniVista Cirrus instance and go to the Administration -> Audit -> Collect Support Info page

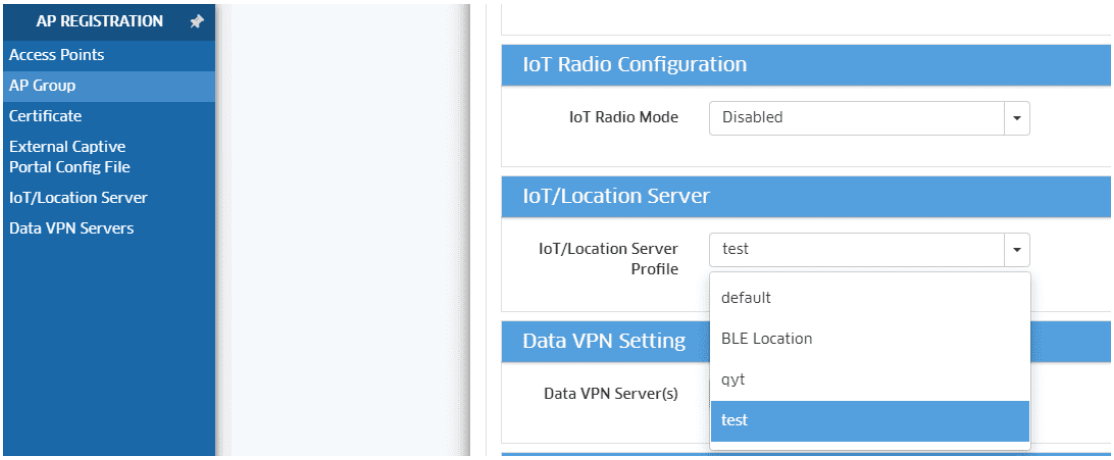
```
support@AP-2D:40:~$ cat /var/config/qoe.conf
{
"QOEReportConfig":{
"server":"broker.eu.analytics.ovng.myovcloud.com:9093","topic":"ext_ov_qoe_events",
"enginetype":"kafka", "username":"system",
"password":"21a2a30ee53a20737151b89db06b9b1a","sslenable":1,
"timer":{
"report":"enable",
"event":"all",
"group":"all", "priority":"warning","interval":30, "userinterval":60, "apinterval":60,
"subevents":[
```

9 How to configure RTLS with AEROSCOUT

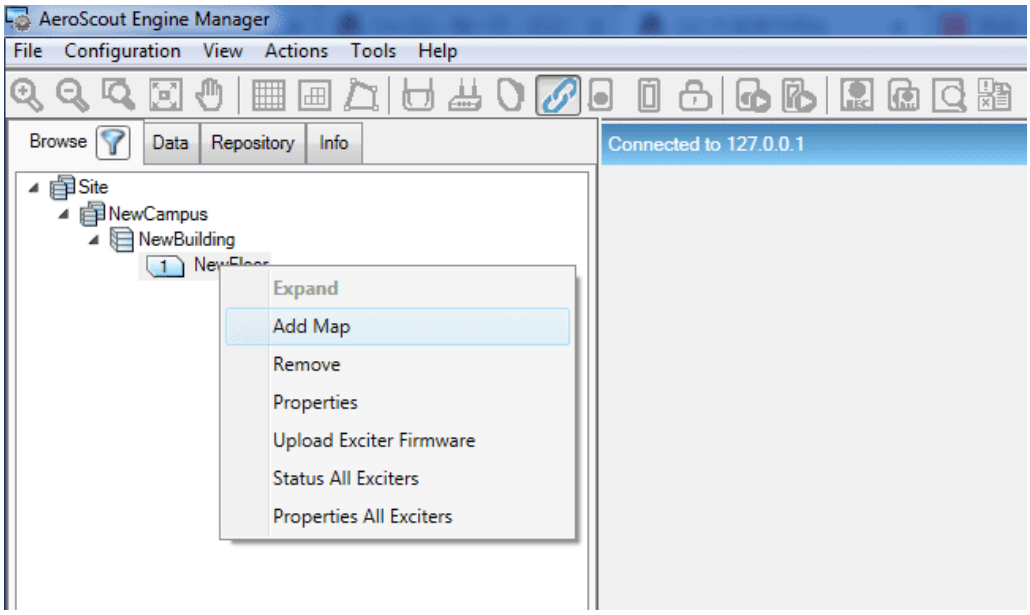
Step1: create the IoT/Location Server on OV 2500 or OV Cirrus, go to Network -> AP Registration -> IoT/Location Server and set the AES Server IP/Host



Step2: Edit the AP Group and apply the IoT/Location Server profile to AP Group



Step3: connect to AES Server, add Map and AP:

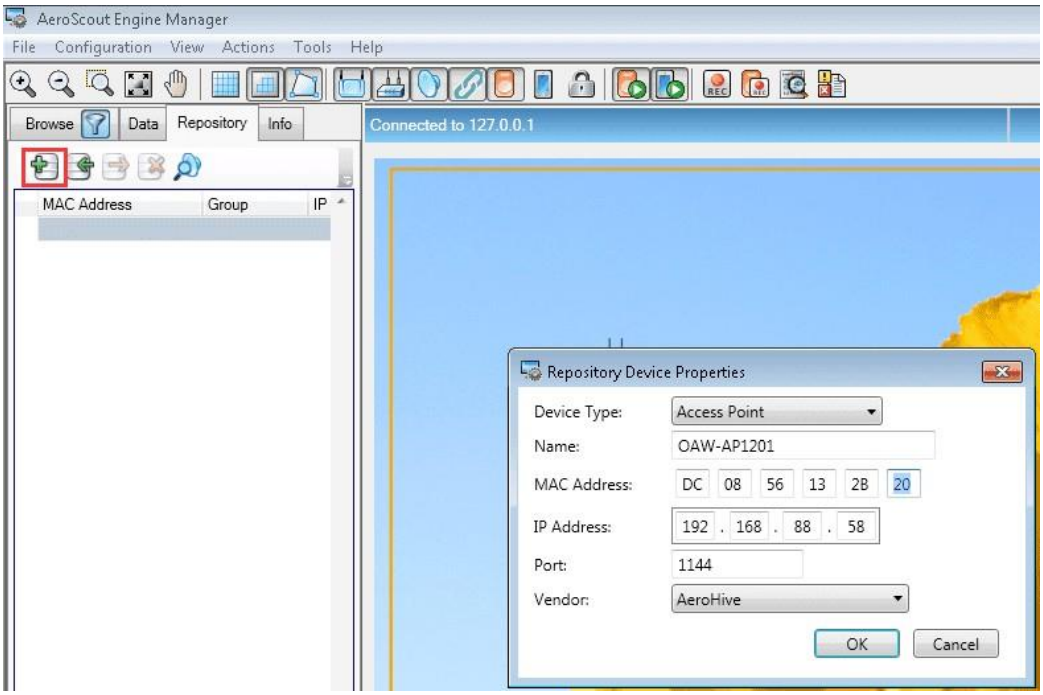


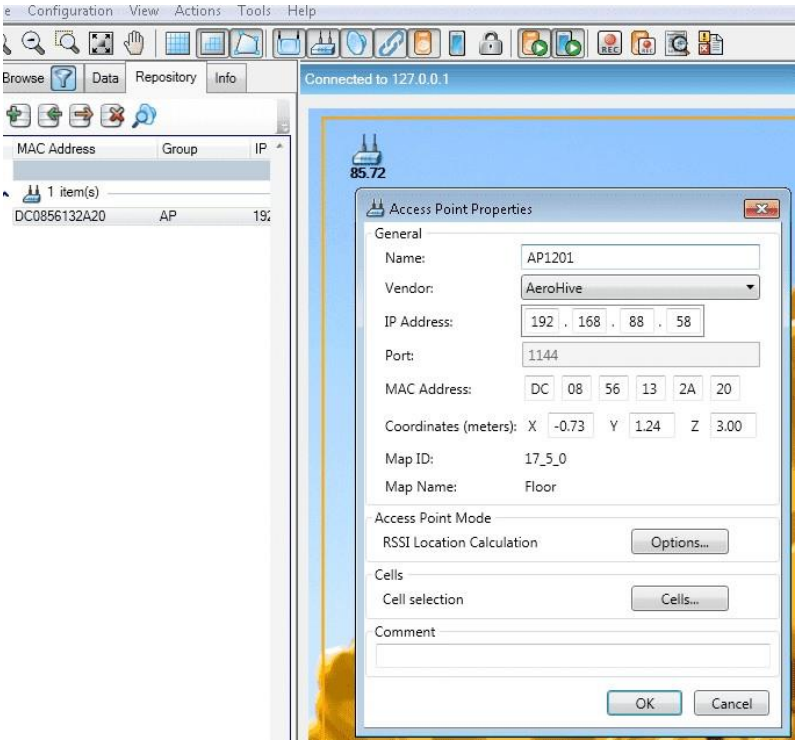
Step4: right-click on the Map and choose Mark(0,0)

Step5: right-click on the Map and choose Calibration -> Calibration Distance and click on the Map -> OK

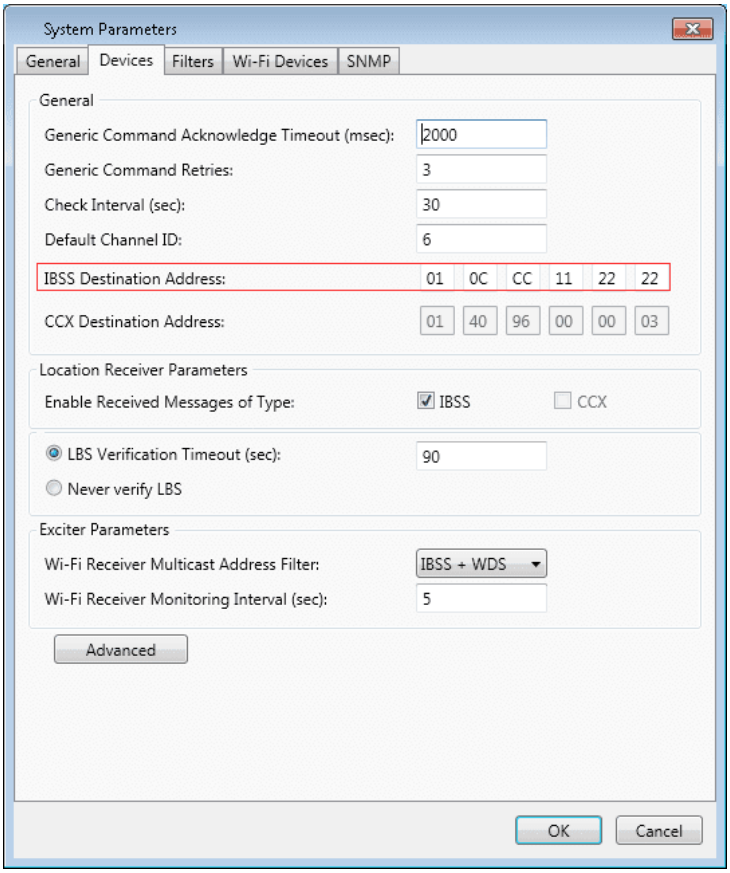
Step6: right-click on the Map and choose Apply Calibration

Step7: add Stellar AP and drag it onto the Map

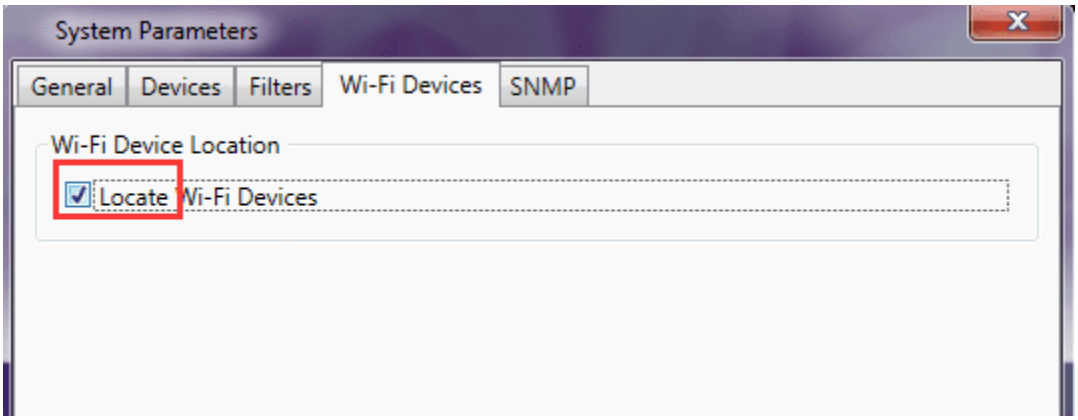




Step8: On the AES Server -> Configuration -> Server Parameters -> System Parameters, set the IBSS Destination Address



And select Locate Wifi Devices



AP will start sending data only after receive HTTP Get Channel from the AES Server as described on below call flow