Alcatel-Lucent Enterprise

OAW-AP User Guide (OAW-AP1101)
September 2016
060443-10 Rev. A

Alcatel·Lucent
Enterprise

Contents

Table of Figures

1 How to Use This Manual

This manual describes all features supported by the OAW-AP and provides instructions and examples for configuring ALE series Access Point (AP). It is designed for network administrators who are responsible for configuring and maintaining the Wi-Fi network. It assumes the reader is familiar with Layer2 and Layer3 networks and 802.11 protocols and related technologies. The manual covers an introduction to the OAW-AP and configuration samples. The examples describe the general steps of setting up a Wi-Fi network based on several typical deployment scenarios. It is useful for those new to the ALE Access Point configuration and those already familiar with the software wanting to know more about certain functions.

Access OAW-AP Through the GUI

This manual is developed for the OAW-AP GUI. Each OAW-AP supports up to three simultaneous GUI connections. The GUI is accessible through a standard web browser from a remote management console or workstation. The GUI includes configuration wizards that guide you to change administrator password and complete basic WLAN configuration. In addition to the wizards, the GUI includes a Dashboard monitoring feature that provides visibility into your wireless network's performance and usage. This allows you to easily locate and diagnose WLAN issues. For details on the GUI Dashboard, see Dashboard Overview.

Document Conventions

The following conventions are used throughout this manual to emphasize important concepts:

It indicates helpful suggestions, pertinent information, and important things to remember.

It indicates a risk of damage to your hardware or loss of data or some incorrect or improper operation that should be avoided.

2 Configuration Sample

This chapter describes the general steps to configure the OAW-AP with respect to several deployment topologies. Follow the configuration steps in the guide to configure your OAW-AP. This chapter contains the following topics:

Scenario 1: AP Group Without ALE OXO server

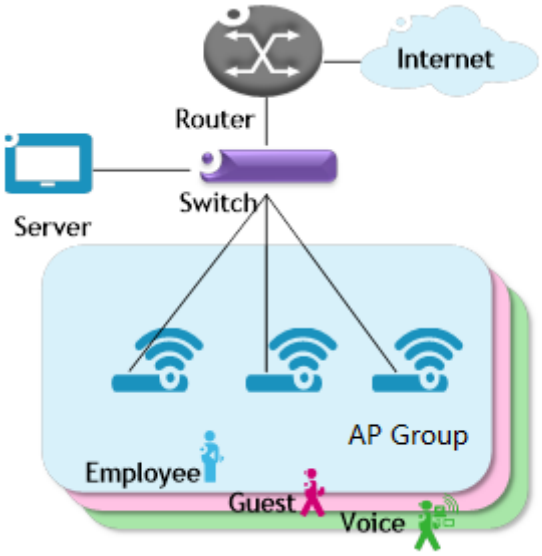

Figure 2-1 AP group without OXO

Following are the requirements for this scenario,

- ➔ There are three APs in this group. All APs connect to a standard PoE switch and the PoE switch connects to the core router. The core router provides DHCP server function to both APs and clients. The Primary Virtual Controller (PVC) in the group will be responsible for portal server, AP and client management and monitoring.
- ➔ All three APs broadcast three SSIDs: Employee, Guest and Voice.
- ➔ The Employee WLAN is used for company staff, by which both internal servers and the internet are accessible.

  For security, this WLAN will use 802.1x authentication methods. Anyone who tries connecting to this WLAN will be requested to input the user name and password registered in an internal RADIUS server.

- ➔ The Guest WLAN is designed for guests and can access the internet ONLY. It uses a captive portal authentication and a portal page will pop up when browsing any website. Guest can access the Internet only after inputting the access code or user name and password provided by the network administrator. The splash page can be customized to the customer's style.
- ➔ The Voice WLAN is designed for VoIP application ONLY. It will authorize voice traffic to be highest priority in QoS profile so as to provide a stable voice connection. The SSID will be hidden and inaccessible to both internal and external networks.
- ➔ ALL APs usage and client connections are visible in the UI dashboard.

According to the topology, the clients are separate in three service VLANs (For example: VLAN 100, VLAN 200 and VLAN 300) while APs are in the management VLAN (default VLAN of the switch ports, for example: VLAN 1). The APs and clients will be assigned an IP address from the DHCP server via the router. The router is the default gateway for APs and clients. Following are the detailed configuration steps:

- ➔ **Step1:** Configure a PoE switch as follows:
  1) The ports used to connect the APs have their default (untagged) VLAN as the AP management VLAN;
  2) Add tagged VLANs to the ports for all WLANs that will be created on the APs;
  3) Tag (trunk) all of the user and AP-Management VLANs on the uplink between the switch and the router.
- ➔ **Step2:** Connect all APs to the PoE switch and all APs will obtain an IP address from the DHCP server. Login to the AP group, change the administrator password and initially create WLAN 'Employee' using the wizard. Refer to Connect to pre-defined SSID and browse URL and Using the Initializing Wizard for details. Refer to Modify Your WLAN to set the mapping VLAN for WLAN 'Employee'.
- ➔ **Step3:** Create WLAN 'Guest' as per the steps in 'Create New WLAN' and configure the captive portal authentication according to 'How to configure captive portal authentication'.
- ➔ **Step4:** Create WLAN 'Voice' as per the steps in 'Create New WLAN'.
- ➔ **Step5:** Configure ACLs according to Access Control List to restrict the access domain of each WLAN.
- ➔ **Step6:** Check AP, Client and monitor the performance in the dashboard. Refer to Dashboard Overview for detail.

Scenario 2: AP Group With ALE OXO Server (ZTP)

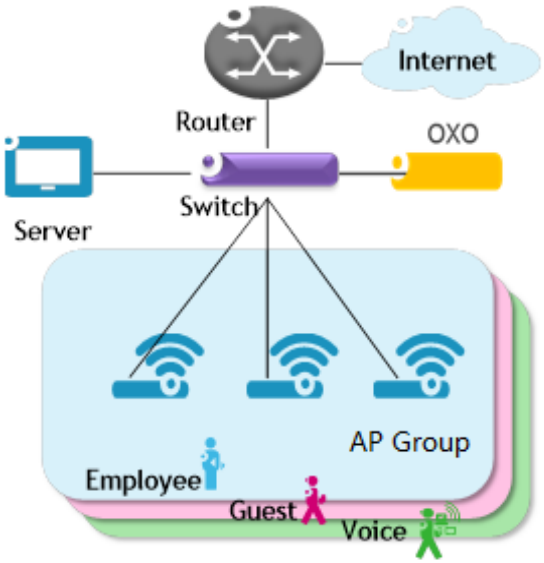

Figure 2-2 AP group with OXO

Following are the requirements for this scenario,

- ➔ There are three APs in this group. All APs connect to a standard PoE switch and the PoE switch connects to the core router and an ALE OXO server.
- ➔ All three APs broadcast three SSIDs: Employee, Guest, and Voice.
- ➔ The Employee WLAN is used for company staff, by which both internal servers and the internet are accessible.

  For security, this WLAN will use 802.1x authentication methods. Anyone who tries connecting to this WLAN will be requested to input the user name and password registered in an internal RADIUS server.
- ➔ The Guest WLAN is designed for guests and has access to the internet ONLY. It uses a captive portal page authentication and a portal page will pop up when browsing any website. Guest can access the Internet only after inputting the access code or user name and password provided by the network administrator. The splash page of captive portal authentication can be customized to customer's style.
- ➔ The Voice WLAN is designed for VoIP application ONLY. It will authorize voice traffic to be highest priority in QoS profile so as to provide a stable voice connection. It will be hidden and inaccessible to both internal and external networks.
- ➔ ALL APs usage and client connections are visible in AP UI dashboard.

According to the topology, APs will be assigned an IP address from the OXO server. Router is the DHCP server for the clients. Following is the detailed configuration steps:

- ➔ **Step1:** Connect all APs to the PoE switch and all APs will obtain an IP address, download firmware (if necessary) and configuration file from the OXO server.

- ➔ **Step2:** The APs will reboot automatically to setup a group and allow configuration from the OXO server take effect, all three WLANs are created.
- ➔ **Step3:** Check AP, Client and monitor the performance in the dashboard. Refer to Dashboard Overview for detail.

3 Connecting AP Group via Web Browser

Prerequisites for Setting up and Accessing AP Group

- Connect all APs to switch and power up.
- Ensure that a DHCP server is present and accessible in the network. The AP group uses an external DHCP server for IP address management of the access points and the wireless clients.
- Ensure that a DNS server is available in the network, which helps to parse the web URL used to access the AP. (*Refer to Note 3-1*)
- It is recommended that your configuring terminal should have a compatible operating system and browser.

Recommended OS	Recommended Browser
• Windows 7 • Window 8 • Window 10 • MAC OS X 10.10 • MAC OS X 10.11	• Google Chrome 38 and later • Mozilla Firefox 48 and later • Internet Explorer 11 and later

After above prerequisites are met, proceed to: Connect to pre-defined SSID and browse URL.

Note

Note 3-1: The process of connecting to a single AP through web is same as connecting to AP group.

Note 3-2: It is recommended to connect only one AP at a time to the network and complete the configuration, then plug in other APs one by one to synchronize the configurations.

Connect to Pre-defined SSID and Browse URL

The ALE WLAN solution is based on a group architecture. A maximum of 16 APs are supported in one AP Group. All APs have the same group ID that uniquely defines the AP group and all APs have to be in the same VLAN because the communication between group members is based on multicast. The group will select the Primary Virtual Controller (PVC) and Secondary Virtual Controller (SVC) based on the MAC address. The highest MAC address will be selected as the PVC and the one with the second highest MAC address will be set as the SVC. The PVC is responsible for the group management, such as configuration synchronization, usage data statistics, firmware upgrading, etc. and the SVC is the backup of the PVC. By default, the AP group will advertise the pre-defined SSID 'mywifi-xxxx' and you can connect to 'mywifi-xxxx' to browse the AP group GUI through http://mywifi.al-enterprise.com:8080 to the initializing wizard. After you complete Using the Initializing Wizard, the SSID 'mywifi-xxxx' will be deleted. (*'xxxx' is the last two bytes of PVC's MAC address*)

Note

Note 3-3: If there is no DNS server in the network, you can connect to the AP group directly using the IP address of any AP in the group, accessing "http://a.b.c.d:8080". (a.b.c.d is the AP's IP address)

Note 3-4: If there is no DHCP server in the network, the AP will default to the 192.168.1.254 address. See How

to Configure the AP if there is no DHCP server.

Using the Initializing Wizard

Initializing wizard page is loaded by connecting to the pre-defined SSID accessing the URL http://mywifi.al-enterprise.com:8080. Login with the Administrator account and the default password '**admin**', illustrated in Figure 3-1.

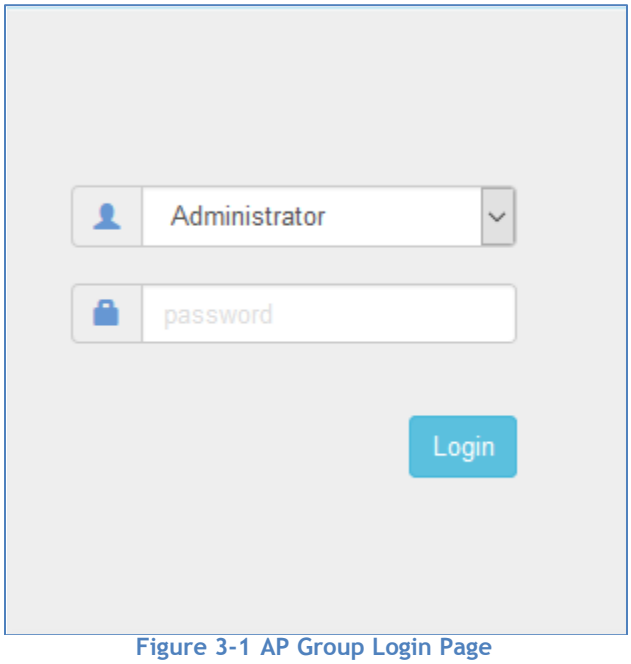

Figure 3-1 AP Group Login Page

The following are the Initialization Wizards:

Step1: Welcome Page

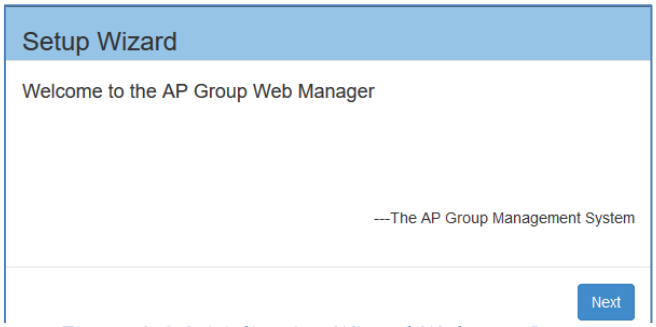

Figure 3-2 Initialization Wizard-Welcome Page

Step2: Change your Administrator password.

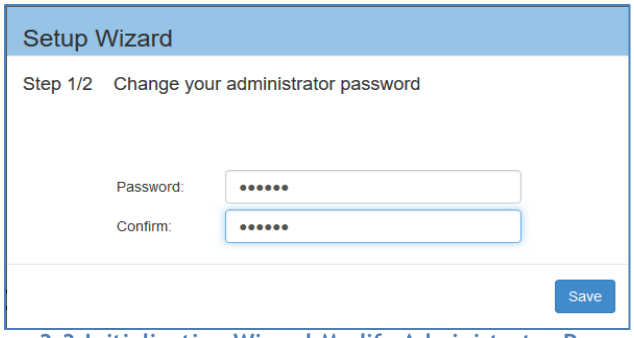

Figure 3-3 Initialization Wizard-Modify Administrator Password

---

Note

Note 3-5: It is highly recommended and a best security practice to change the default passwords for the predefined login accounts.

Step3: Select your country code and time zone. (Only for -RW models)

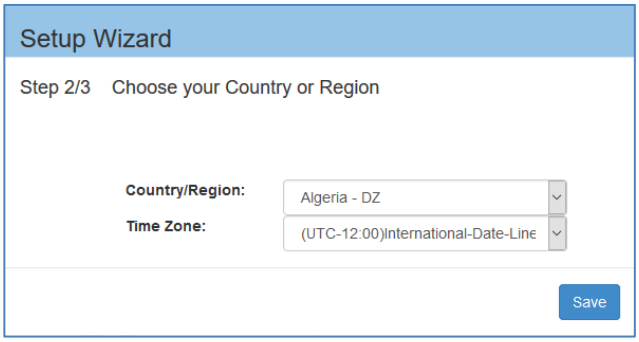

Figure 3-4 Initialization Wizard-Select country code and time zone

Step4: Create your own WLAN. You can click '[Create New WLAN](#)' for details.

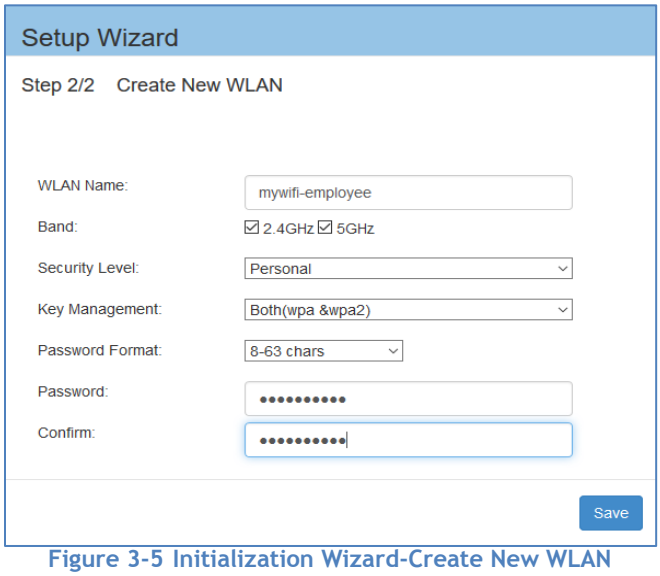

Figure 3-5 Initialization Wizard-Create New WLAN

Note 3-6: The VLAN assignment for the WLAN is not available in the initial wizard phase. You can modify the mapping VLAN value after the initial setup is completed, using the steps described in "Modify your WLAN" section which can be used to modify existing WLANs.

Step5: Complete Confirmation Page

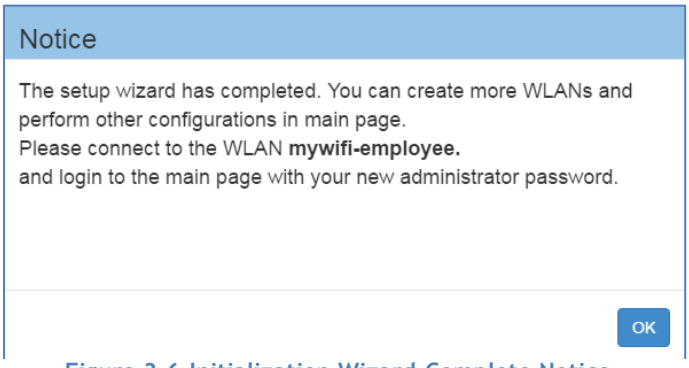

Figure 3-6 Initialization Wizard-Complete Notice

Note 3-7: While configuring the Initialization Wizards, please make sure your configuring terminal is connected to the pre-defined WLAN 'mywifi-xxxx' to keep the communication operational between AP group (or AP) and web browser. If not, you may encounter the following prompt and fail to complete the wizard configuration correctly:

Note 3-8: The pre-defined WLAN 'mywifi-xxxx' is deleted when the wizard is completed. For additional configuration through the wireless connection you need to connect to the new WLAN created in the wizard and then login to the web main page with your new administrator password.

Connecting to the AP Group via Web

When the initializing wizard has completed and new WLANs have been created, you can connect to each of the WLANs and browse the URL http://mywifi.al-enterprise.com:8080 to manage the AP group.

Another way of connecting to the AP group web management system is through the AP group management IP address. For information on setting of the Management IP address refer to AP Group Management.

The AP group web management system can be accessed through the wired network if the group management IP address is configured and is reachable.

4 Introduction to the AP Group Web Management System

Dashboard Overview

The OAW-AP provides a visualized dashboard for AP and client monitoring and configuration. As illustrated in Figure 4-1 Dashboard Overview, the dashboard is split into sub-windows for WLAN Window, AP Window, Client Window and Monitoring Window, System Page, Wireless Page and Access Page. You can briefly check the WLANs, APs or Clients in the dashboard or double click the framework of each window to see the details.

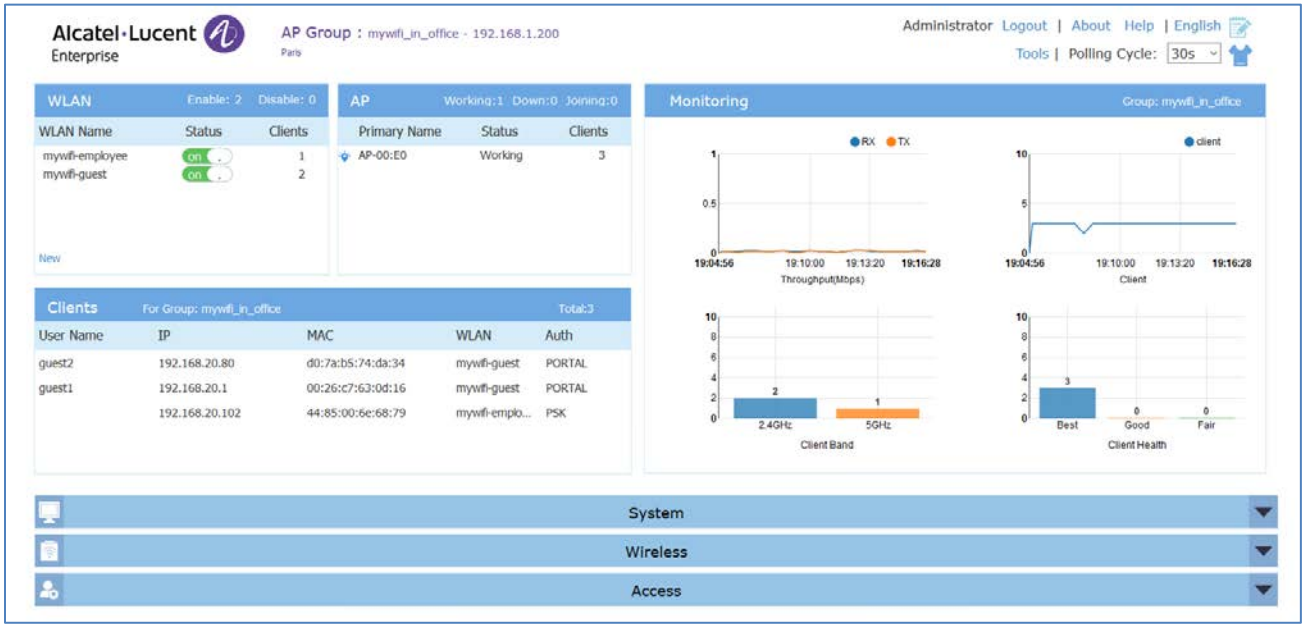

Figure 4-1 Dashboard Overview

WLAN Window

The WLAN configuration window is integrated with all WLAN related monitoring and operation tasks. There are two modes for the WLAN Window, Simplified Mode illustrated in Figure 4-2 and Advanced Mode illustrated in Figure 4-3. You can easily launch the Advanced Mode from Simplified Mode by clicking the WLAN Window Frame.

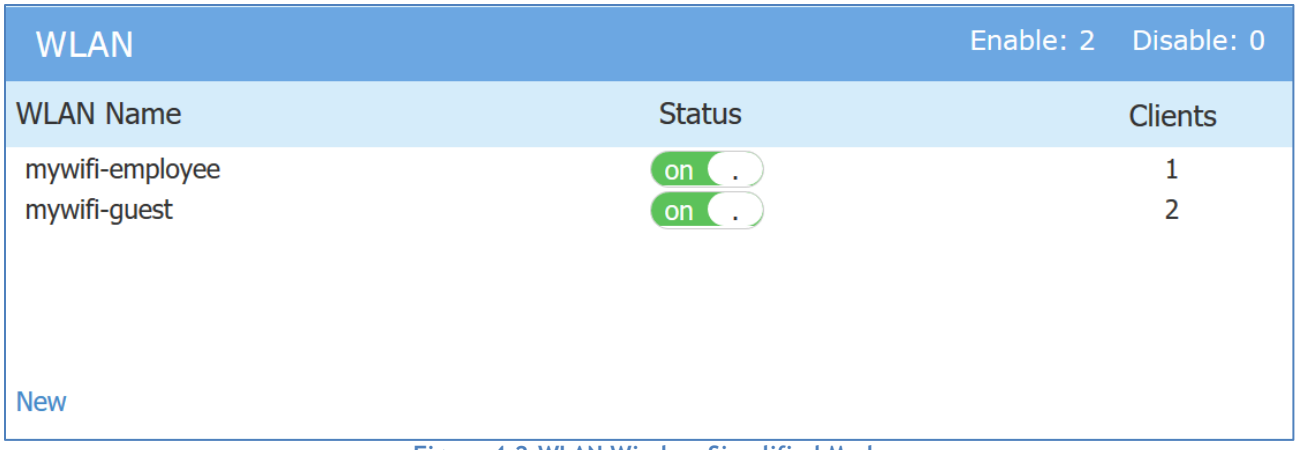

Figure 4-2 WLAN Window-Simplified Mode

Note

Note 4-1: The label below displays the number of enabled or disabled WLANs.

Table 4-1: Key word specification in WLAN Window (Simplified Mode)

WLAN Name	Label or name of WLAN, which is composed by 0-9, a-z or other string.
Status	Indicates the WLAN state, on indicates that WLAN is in broadcast state, while off indicates WLAN is not in broadcast state.
Clients	The number of users connected to the WLAN.
New	Launch the WLAN creation window.

Figure 4-3 WLAN Window-Advanced Mode

Table 4-2 Key word specification in WLAN Configuration Window (Advanced Mode)

WLAN Name	Label or name of WLAN.
Status	Indicates the WLAN state, on indicates that WLAN is in broadcast state, while off indicates WLAN is not in broadcast state.
Security Level	Security Level of WLAN, from high to low is Enterprise>Personal>Open.
Captive Portal	Indicates whether the WLAN is using captive portal authentication. Yes means the WLAN is configured with captive portal authentication, while No means the WLAN is without captive portal authentication.
Operate	Operation for the WLAN. see Modify Your WLAN, see Delete Your WLAN, wmm see Modify WLAN QoS.
Create	Link for Creating new WLAN, see Create New WLAN.

AP Window

AP Window is integrated with all APs and group related monitoring and configuration functions. Similar to the WLAN Window, there are two modes for AP Window, Simplified Mode illustrated in Figure 4-4 and Advanced Mode illustrated in Figure 4-5. You can easily launch the Advanced Mode from Simplified Mode by clicking the AP Window Frame.

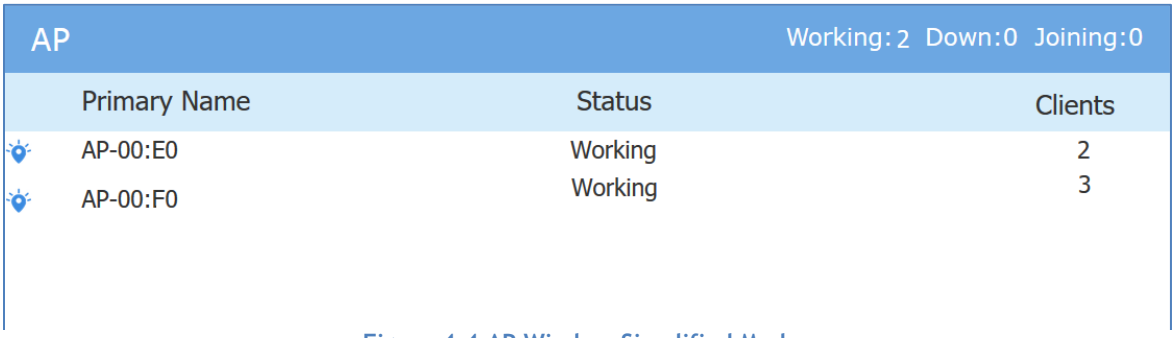

Figure 4-4 AP Window-Simplified Mode

Table 4-3 Key word specification in AP Window (Simplified Mode)

Primary Name	AP Mac address.
Status	Connection status of AP, there are three indication for AP status, they are Working, Down and Joining. See more in Note 4-2.
Clients	The total number of users currently connected to AP.

Note

Note 4-2: AP has three status indications when connecting to group, they are 'working' which indicates that AP has connected to the PVC successfully and is working normally, 'Down' indicates that AP is disconnected from the group, and 'Joining' indicates that AP is requesting to join the group but hasn't completed yet. The Label in AP Window indicates the number of APs in each status. AP Working:2 Down:0 Joining:0

Select an AP from the AP Configuration Window (Advanced Mode), you can learn the detailed information of the AP, see in Figure 4-5.

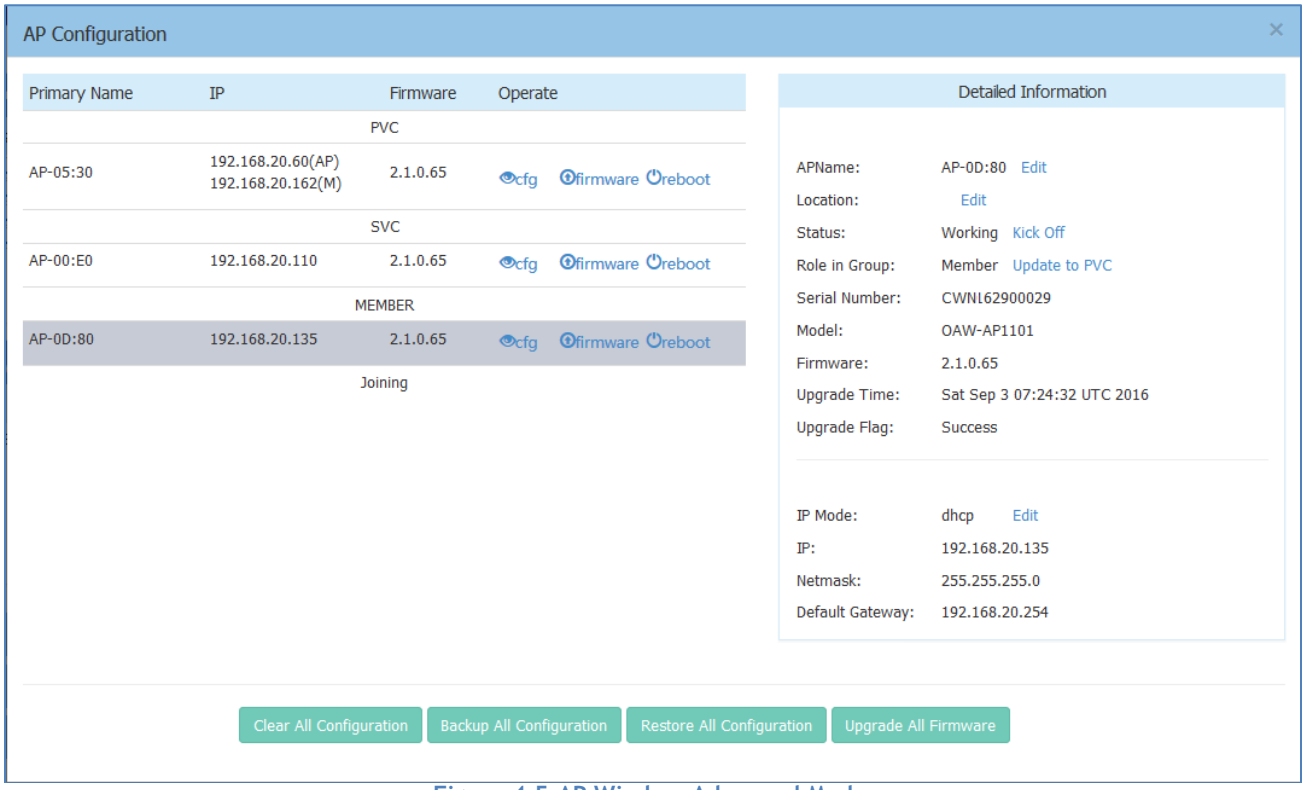

Figure 4-5 AP Window-Advanced Mode

Table 4-4: Key word specification in AP Configuration Window (Advanced Mode)

Primary Name	Name of the AP.
IP	IP address of the AP.
Firmware	Firmware version of the AP.
Operate	There are three optional operations for the AP: cfg, firmware and reboot.
PVC	Primary Virtual Controller in the AP group.
SVC	Secondary Virtual Controller in the AP group.
MEMBER	Other member APs in the group except PVC/SVC.
Joining	APs in joining state, needs to be authorized to join the group.
cfg	Checking the detailed configuration on the AP.
firmware	Upgrading firmware for the AP.
reboot	Execute to reboot the AP.
Clear All Configuration	Restore factory settings for all the APs in the group.
Backup All Configuration	Backup the configuration of the AP group.
Restore All Configuration	Restore the configuration for the AP group.

Upgrade All Firmware	Update the firmware for all the APs in the group.
Detailed Information	Detailed information for the selected AP.
AP Name	Name of the AP.
Location	Location of the AP.
Status	Connection status of AP, there are three indications for AP status, they are Working, Down and Joining. See more in Note 4-2.
Kick Off	Remove the AP from the group. When an AP is removed from the group, it changes into **Joining** state until the administrator permits it to join the group again. See more in Allow an AP to Join the Group.
Role in Group	AP role in the group, including PVC, SVC and Member.
Update to PVC	Upgrade the member or SVC to be the PVC of the AP group.
Serial Number	Serial Number of the AP selected.
Model	Product Model of the AP selected.
Upgrade Time	Last firmware upgrade time.
Upgrade Flag	Flag of last time firmware upgrade. Success means the firmware was upgraded successfully on the Upgrade Time, Failed means the firmware wasn't upgraded successfully on the Upgrade Time.
IP Mode	The way by which the AP attains its IP address, dynamically assigned from DCHP server or static IP configured manually. ◉DHCP ○Static
IP	IPv4 address of the AP selected.
Netmask	Netmask of the IPv4 address of the AP selected.
Default Gateway	Default Gateway of the AP selected.

Client Window

Client Window displays all the connected clients. Similar to the WLAN Window, there are two modes for Client Window, Simplified Mode illustrated in Figure 4-6 and Advanced Mode illustrated in Figure 4-7. You can launch the Advanced Mode from Simplified Mode by clicking the Client Window Frame.

Clients For Group: mywifi_in_office Total:3

User Name	IP	MAC	WLAN	Auth
guest2	192.168.20.80	d0:7a:b5:74:da:34	mywifi-guest	PORTAL
guest1	192.168.20.1	00:26:c7:63:0d:16	mywifi-guest	PORTAL
	192.168.20.102	44:85:00:6e:68:79	mywifi-empl...	PSK

Figure 4-6 Clients Window-Simplified Mode

Table 4-5: Key word specification in Client Window (Simplified Mode)

For Group: mywifi_in_office	Clients connected to the group.
For WLAN: mywifi-employee	Clients connected to the specified WLAN in the group.

For AP: 34:e7:0b:00:00:e0	Clients connected to the specified AP in the group.
User Name	User Name of the client.
IP	IPv4 address of the client.
MAC	MAC address of the client.
WLAN	WLAN to which the client connected.
Auth	Authentication type: Open, Portal (Captive portal), PSK (Personal), 802.1X (Enterprise).

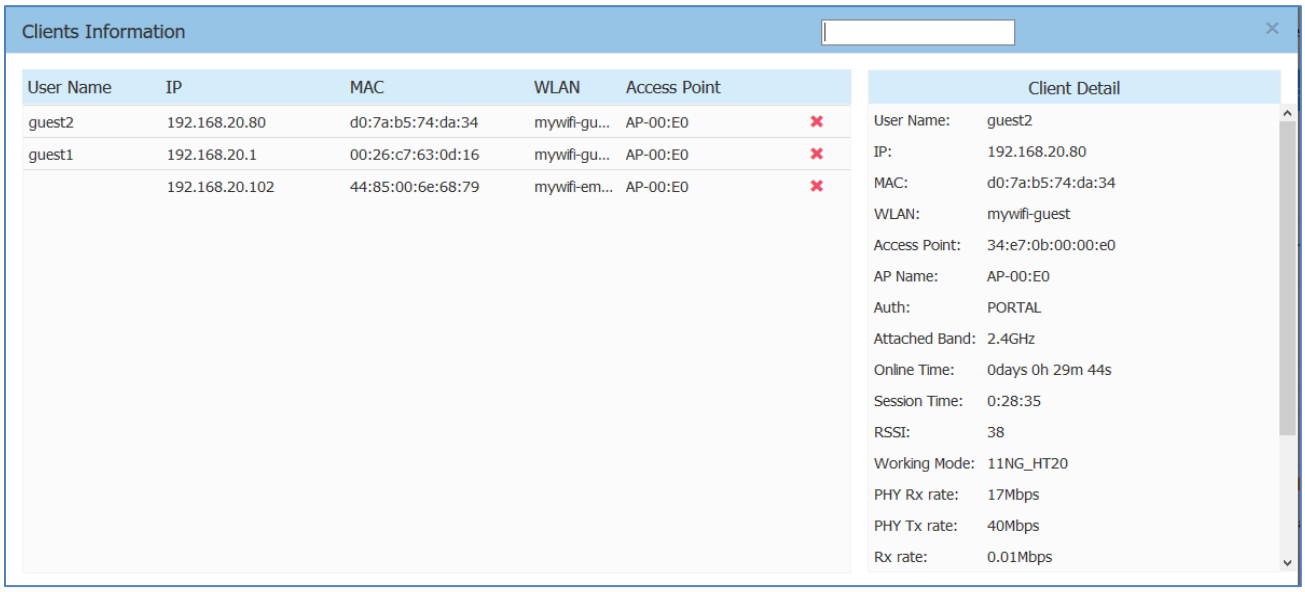

Figure 4-7 Clients Window-Advanced Mode

Table 4-6: Key word specification in Client Information Window (Advanced Mode)

User Name	User Name of the client.
IP	IPv4 address of the client.
MAC	MAC address of the client.
WLAN	WLAN to which the client connected.
Access Point	Access point to which the client connected.
✖	Remove the client from the wireless network.
AP Name	Name of access point that the client connected.
Auth	Authentication type: Open, Portal (Captive Portal), PSK (Personal), 802.1X (Enterprise).
Attached Band	The radio band through which the client attach to AP, 2.4GHz or 5GHz.
Online Time	Time when the client attached to the wireless network.
Session Time	Time when the client has passed the captive portal authentication, only for captive portal clients.
RSSI	Received Signal Strength Indication of the client, Value 0~99.
Working Mode	Wireless working mode of the client.
PHY Rx rate	Physical receive rate of the client.
PHY Tx rate	Physical sending rate of the client.
Rx rate	Packet receive rate of the client.
Tx rate	Packet sending rate of the client.
Download	Total download data size since the client connected to the wireless network.
Upload	Total upload data size since the client connected to the wireless network.
Device type	Device type of the client.
OS Type	Operating system type of the client.

Monitoring Window

The monitoring window displays the utilization of the wireless network, including statistics of traffic throughput and client working state.

The monitoring window can monitor from four different levels: group level, WLAN level, AP level and client level, illustrated in Figure 4-8, Figure 4-9, Figure 4-10 and Figure 4-11.

The group monitoring is the default display, you can select to monitor certain WLAN/AP/client from the WLAN Window/AP Window/Client Window on left side of the Dashboard.

The monitoring window is automatically refreshed every 30 seconds by default, and the data polling cycle can be set to 30s /60s /120s.

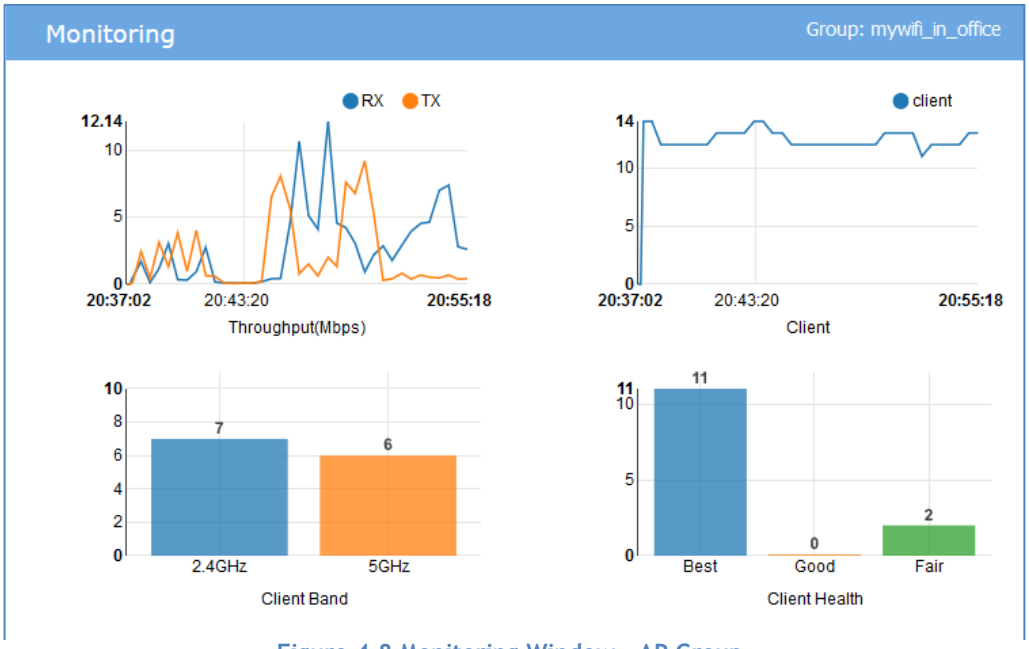

Figure 4-8 Monitoring Window - AP Group

Table 4-7: Key word specification in AP group Monitoring Window

RX	Total receiving rate of the AP group.
TX	Total sending rate of the AP group.
Client	The number of clients connected to the AP group.
Client Band	The working band distribution of clients connected to the AP group, including number of clients working on 2.4GHz band and number of clients working on 5GHz band.
Client Health	The wireless connection quality between client and OAW-AP, it is judged by the signals of client, and classified as below: • Best— Number of clients whose signal strength is more than 30. • Good— Number of clients whose signal strength is between 15 ~30. • Fair—Number of clients whose signal strength is less than 15.

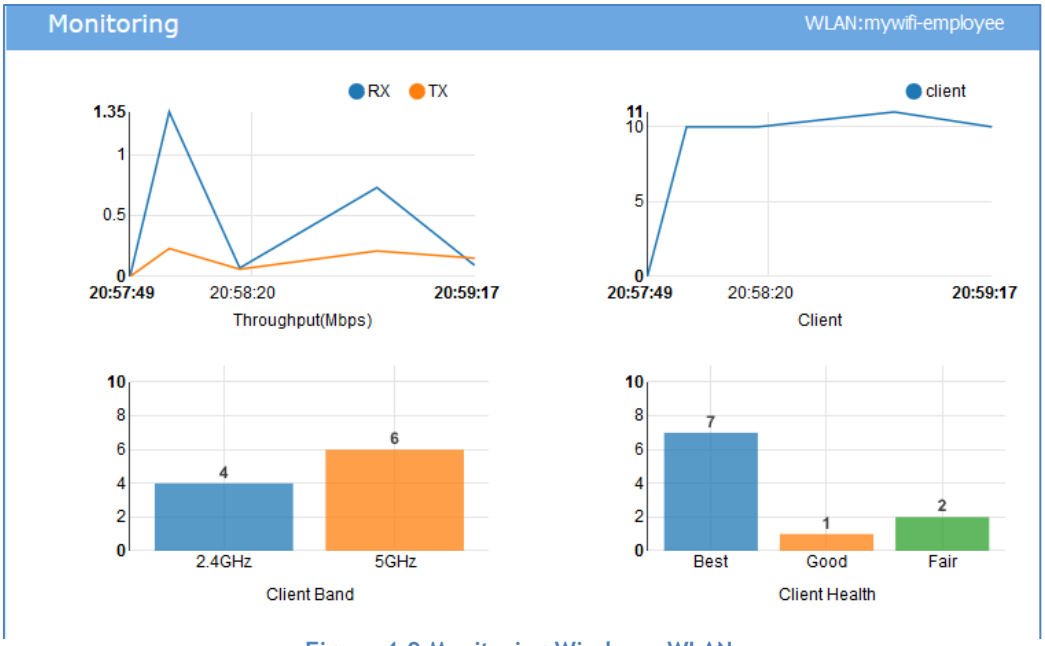

Figure 4-9 Monitoring Window - WLAN

Table 4-8: Key word specification in WLAN Monitoring Window

RX	Total receiving rate of the WLAN.
TX	Total sending rate of the WLAN.
Client	The number of clients connected to the WLAN.
Client Band	The working band distribution of clients connected to the WLAN, including number of clients working on 2.4GHz band and number of clients working on 5GHz band.
Client Health	The wireless connection quality between client and OAW-AP, it is judged by the signals of client, and classified as below: • Best— Number of clients which signal strength is more than 30. • Good— Number of clients which signal strength is between 15 ~30. • Fair—Number of clients which signal strength is less than 15.

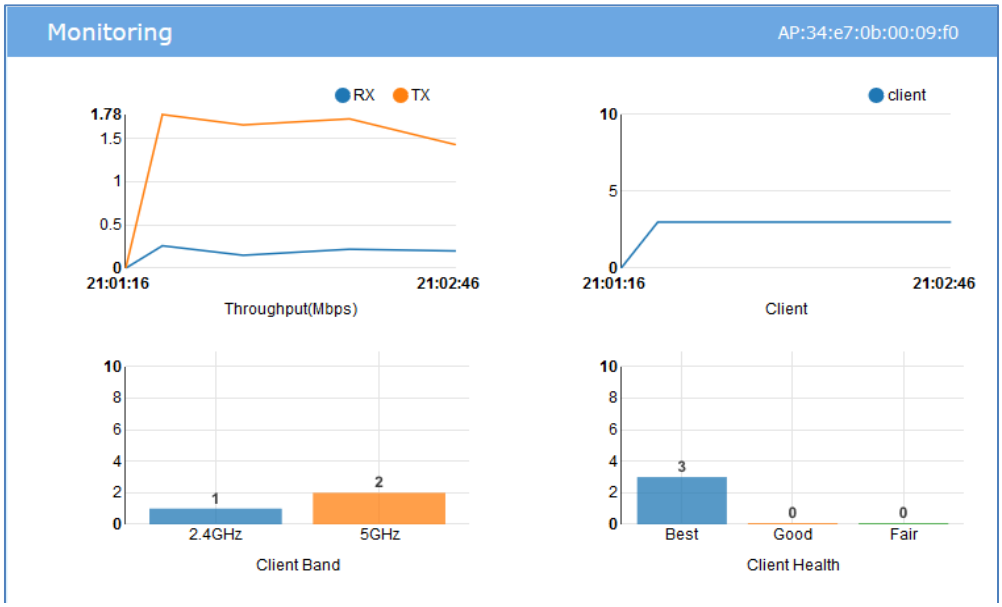

Figure 4-10 Monitoring Window - AP

Table 4-9: Key word specification in AP monitoring Window

RX	Total receiving rate of the AP.
TX	Total sending rate of the AP.
Client	The number of clients connected to the AP.
Client Band	The working band distribution of clients connected to the AP, including number of clients working on 2.4GHz band and number of clients working on 5GHz band.
Client Health	The wireless connection quality between client and OAW-AP, it is judged by the signals of client, and classified as below: • Best— Number of clients which signal strength is more than 30. • Good— Number of clients which signal strength is between 15 ~30. • Fair—Number of clients which signal strength is less than 15.

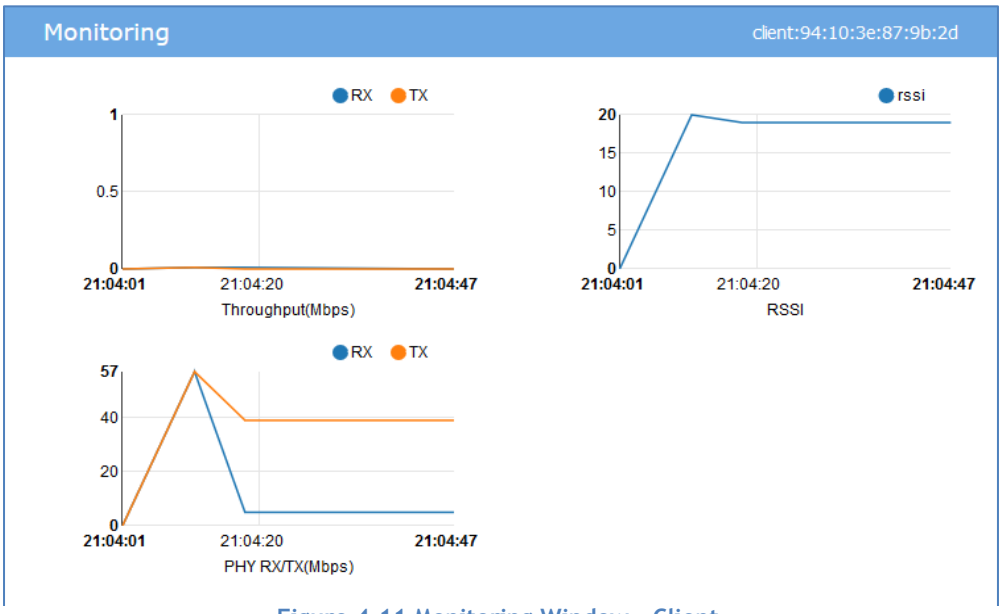

Figure 4-11 Monitoring Window - Client

Table 4-10: Key word specification in Client Monitoring Window

RX	Receiving rate of the client.
TX	Sending rate of the client.
RSSI	Received Signal Strength Indication of the client
PHY RX	Physical receiving rate of the client.
PHY TX	Physical sending rate of the client.

Note

Note 4-3: The data shown in the monitoring window is collected and displayed while the window is open. The data is not stored and no historical view of the data is available.

System Page

The System page focus on the basic settings of the AP group, including: AP group attributes, system management accounts, system time and syslog.

It is divided into three windows in System Page: General window, System Time window and Syslog window, illustrated in Figure 4-12 System page.

Figure 4-12 System page

General Window

General Window displays the basic information of the wireless system. There are two modes for General Window, Simplified Mode illustrated in Figure 4-13 General Window – Simplified Mode and Advanced Mode illustrated in Figure 4-14 General Configuration Window –Advanced Mode. You can launch the Advanced Mode from Simplified Mode by clicking the General Window Frame.

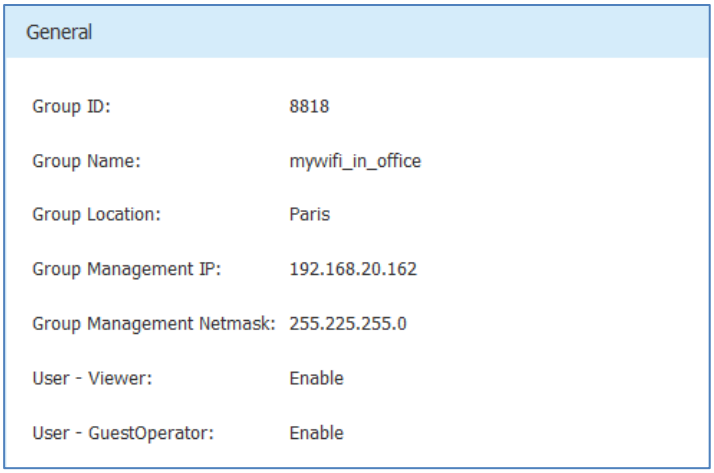

Figure 4-13 General Window - Simplified Mode

The General Configuration window includes two tabs: **Group Info Management** and **Account management**, illustrated in Figure 4-14 .

Group Info Management
Group Info Management contains the basic information of the AP group, you can edit it with your own group settings to identify a private Wi-Fi network.

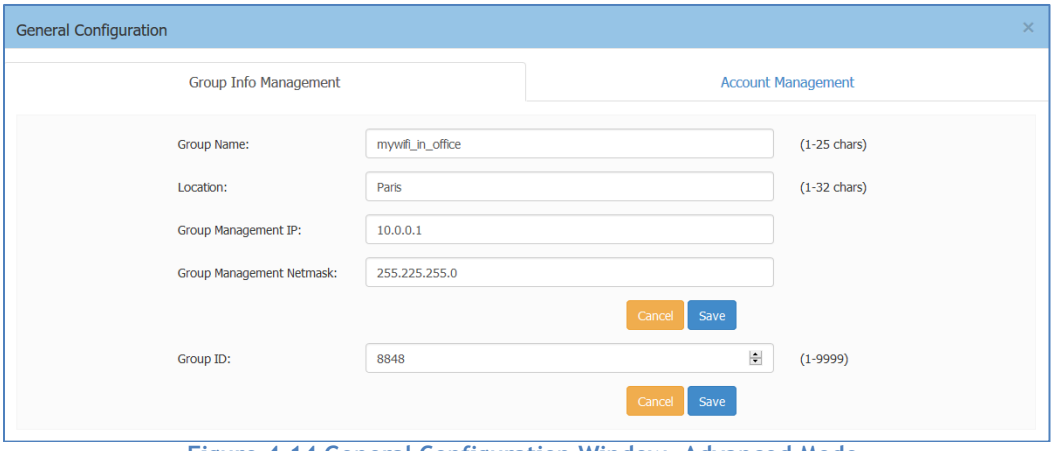

Figure 4-14 General Configuration Window -Advanced Mode

Table 4-11: Key word specification in Group Info Management Tab

Group Name	Name of the AP group.
Location	Location of the AP group.
Group Management IP	A virtual IP address for AP group management, default is 10.0.0.1, see more in Note 4-4.
Group Management Netmask	Netmask of Group Management IP.
Group ID	Identification of the AP group, default is 100.

Note

Note 4-4: AP of a group usually obtains its IP address dynamically from a DCHP server, and it is difficult to keep the same assigned IP address for the AP. So managing the AP group by the AP's dynamic IP address can be difficult. The Group Management IP (GMIP) is a static IP address configured for the AP group web management, and you can manage the AP group via accessing the URL: http://GMIP:8080 by wired or wireless. The GMIP is configured on the PVC of the AP group, and you have to make sure the GMIP on the PVC is routable from your configuring terminal (browser). A recommended method is to choose an idle IP address from the AP group domain to configure as a GMIP.

Account Management

There are three login accounts with different privileges: Administrator, Viewer, and GuestOperator.

Administrator account allows configuring and viewing the whole system, Viewer account allows checking configuration and monitoring of WLAN operations, while GuestOperator ONLY has the privilege to edit the guest portal users. Each account can be logged in at the same time.

By default, only the Administrator account is enabled; Viewer and GuestOperator are disabled.

In the Account Management tab, you can enable/disable the Viewer and GuestOperator account, change the password for Administrator, Viewer and GuestOperator, illustrated in Figure 4-15.

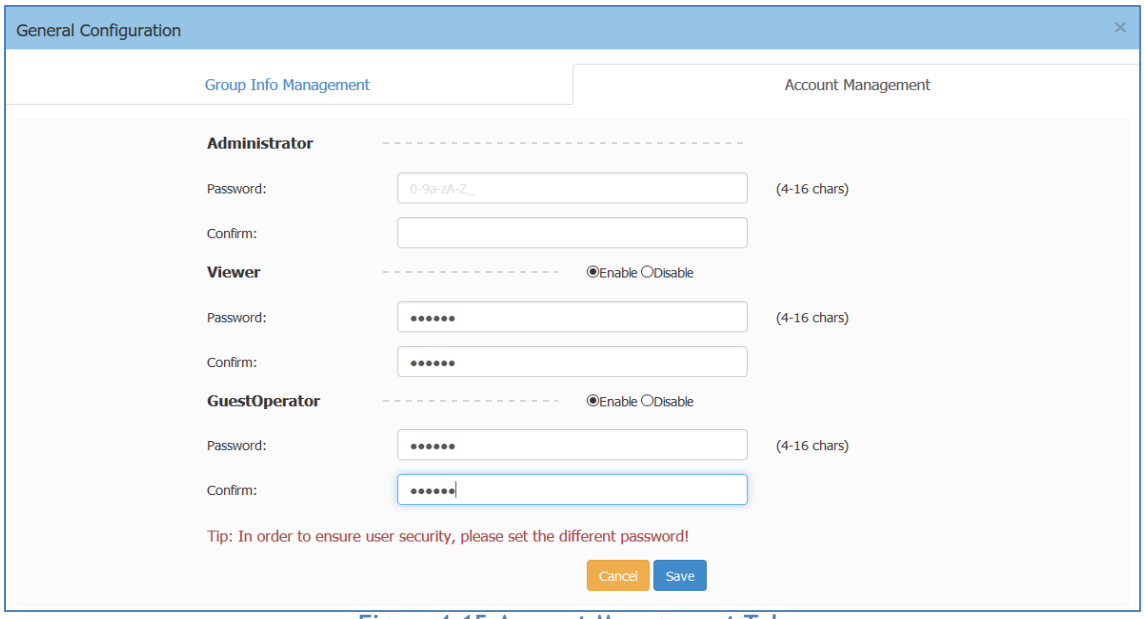

Figure 4-15 Account Management Tab

The password must be composed by 0-9 or a-z with the length of 4 to 16 characters.

System Time Window

It is important to ensure the system time is correct, this is because proper communication between network elements and syslog for troubleshooting are based on the correct time.

Network Time Protocol (NTP) is a networking protocol for time synchronization between the elements across the network. If you don't have a private NTP server in your network, it is suggested to add your favorite NTP server and prioritize it to the top of the NTP Server List, or use the default NTP servers in the system, illustrated in Figure 4-16 System Time.

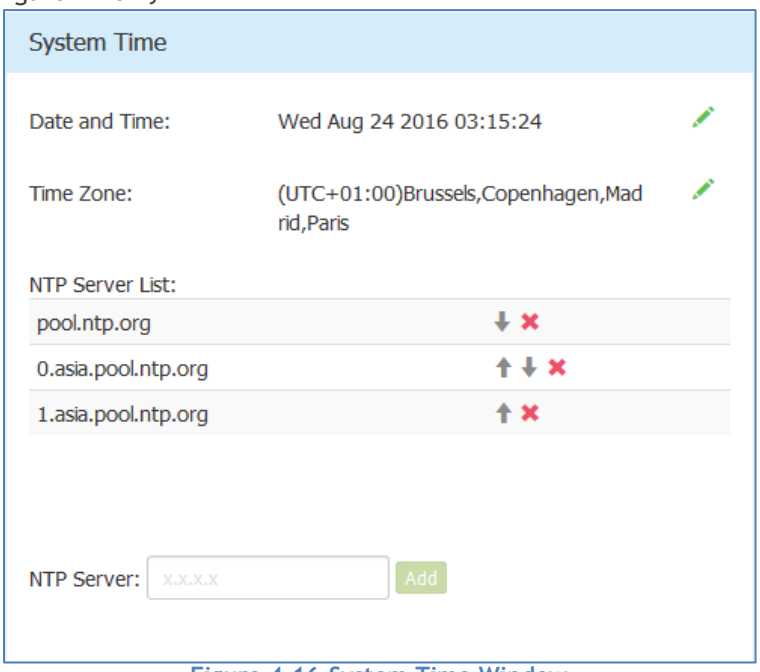

Figure 4-16 System Time Window

If configured, APs in the group synchronize the time with NTP sever in 15-minute intervals.

You can also specify the **Time Zone** of the AP group to coordinate with the local time.

Note

Note 4-5: In order to ensure time synchronization it is recommended to check the reachability before adding an NTP server. If the NTP server is not configured or is unreachable, an AP reboot may lead to variation in time.

Syslog Window

Syslog is a standard for message logging. Syslog is used for system management and security auditing as well as general informational, analysis, and debugging messages.

APs in group generate logs following the standard of Syslog, you can view logs and configure corresponding attributes in the Syslog Window.

Upper part of the Syslog Window displays **error** (and lower, see in Note 4-5) level Syslog generated by APs in the group.
Title is the content of the log message;
Level is the severity of the log message;
Source is the generator's IP address of the log message;

When you move the mouse cursor to certain row of log message, the generating time of the log displays, illustrated in Figure 4-17 Syslog Window.

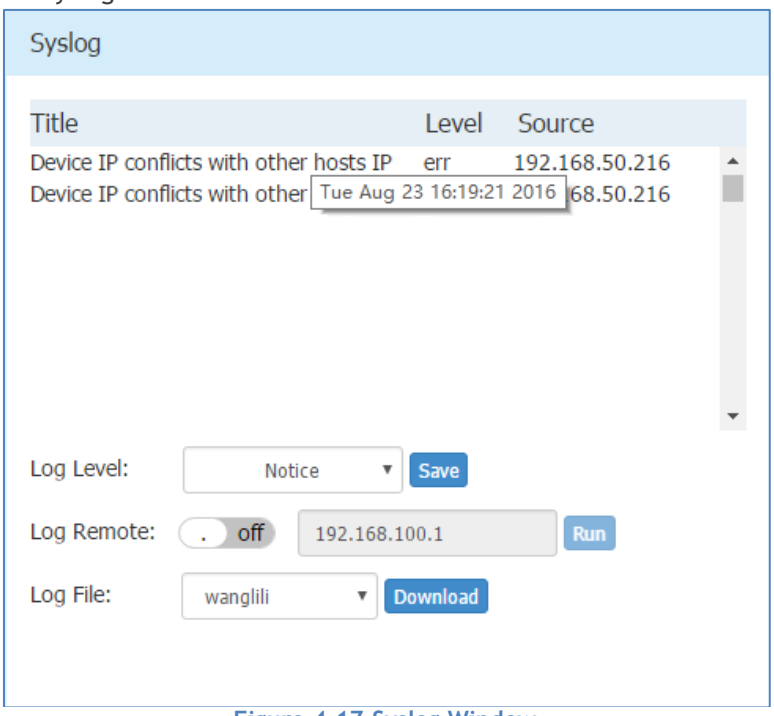

Figure 4-17 Syslog Window

Log Level: Setting of Syslog message severity. If certain level is specified, the AP group will generate Syslog messages including all lower levels. That is, if Syslog messages are separated by individual severity, a Warning level entry will also be included in Notice, Info and Debug processing. Notice is the default level of Syslog setting, and the system generates logs including levels of Notice, Warning, Error, Critical, Alert and Emergency.

Log Remote: Setting of remote log server. If configured and enabled, besides storage in local file, Syslog messages of all APs in group can be sent to and stored in the server once generated.

Log File: Download the log file on a selected AP in the group to your configuring machine. Syslog messages are stored in a local file when generated. For one AP, up to 1MB size of syslog messages can be saved in the local log file. The log file is FIFO, new syslog messages will replace the old ones if the size exceeds 1MB.

Note

Note 4-5: Syslog is divided into eight levels, and lowest level 0 is Emergency severity while highest level 7 is Debug severity. Definition of Syslog severity as follow:

Level Value	Severity	Keyword	Description
0	Emergency	emerg	System is unusable
1	Alert	alert	Should be corrected immediately
2	Critical	crit	Critical conditions
3	Error	err	Error conditions
4	Warning	warning	May indicate that an error will occur if action is not taken
5	Notice	notice	Events that are unusual, but not error conditions
6	Informational	info	Normal operational messages that require no action
7	Debug	debug	Information useful to developers for debugging the application

Wireless Page

The Wireless page focuses on advanced wireless functions, including three windows: RF (Radio Frequency), Wireless Intrusion Detection System/Wireless Intrusion Prevention System (wIDS/wIPS), and wireless performance optimization, illustrated in Figure 4-18 Wireless Page.

Figure 4-18 Wireless Page

RF Window

Radio Frequency (RF) window is for monitoring the wireless utilization and configuring wireless attributes like channel and transmitting power.

There are two modes for RF Window, Simplified Mode illustrated in Figure 4-19 RF-2.4GHz and Advanced Mode illustrated in Figure 4-21. You can launch the Advanced Mode from Simplified Mode by clicking the RF Window Frame.

Panel of RF displays the monitoring information of channel distribution, can be selected on 2.4G band or 5G band. Channels are separated by different colors, when you move the mouse cursor to the colored section of the pie chart, it displays the clients connected to the AP group through 2.4G band or 5G band, illustrated in Figure 4-19 RF-2.4GHz and Figure 4-20 RF-5GHz.

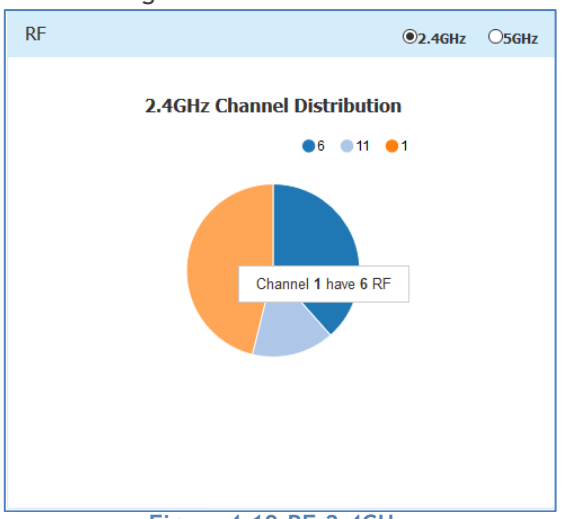

Figure 4-19 RF-2.4GHz

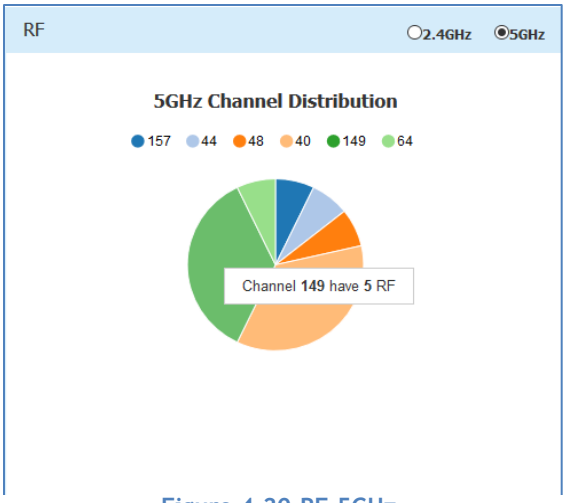

Figure 4-20 RF-5GHz

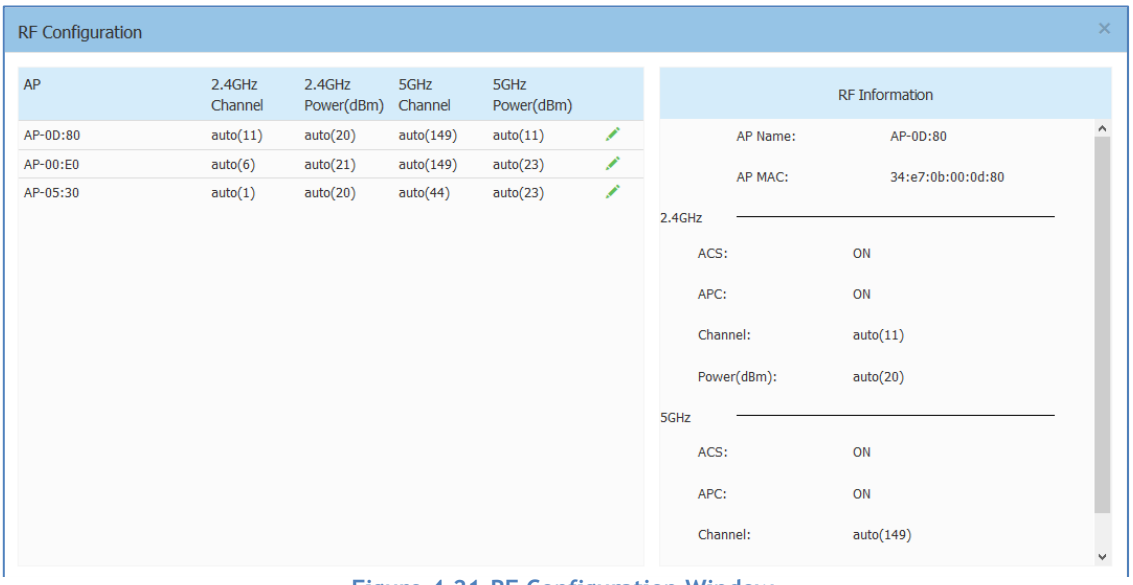

Figure 4-21 RF Configuration Window

The left side of the RF Configuration window displays the list of working channels and transmitting power of all APs in the group. When you pick an AP from the list, its detailed RF information is displayed on the right side of the window, illustrated Figure 4-21.

By default, the working channel and transmitting power are automatically managed by Radio Dynamic Adjustment™ (RDA) technology. If you want to set the channel and power values for an AP manually, you need to disable the ACS/APC function on the AP, illustrated in Figure 4-22.

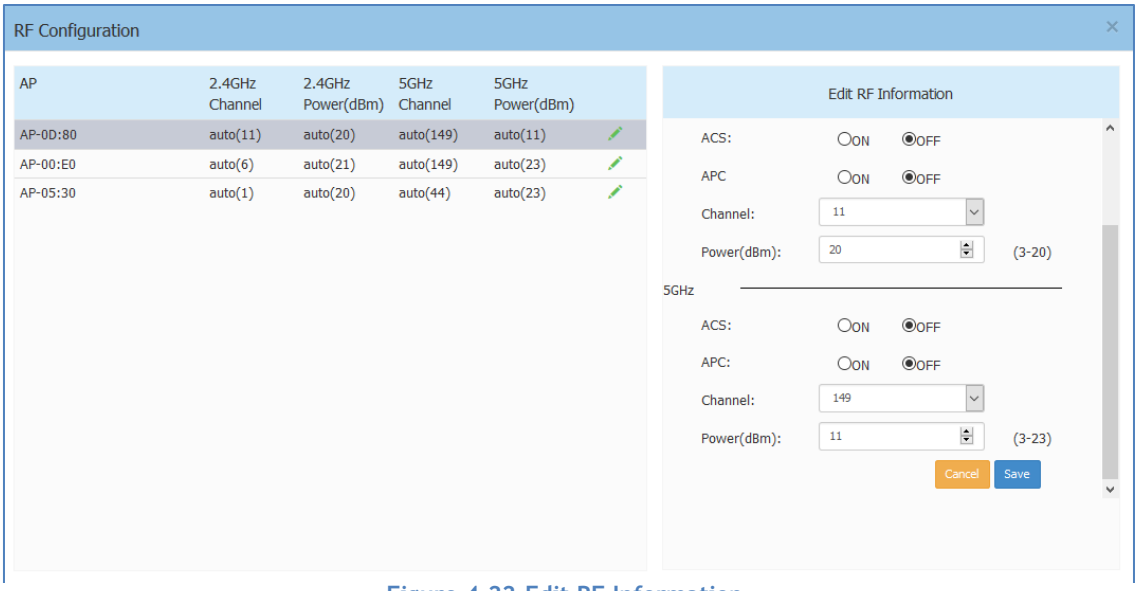

Figure 4-22 Edit RF Information

Note

Note4-6: Radio Dynamic Adjustment™ (RDA) is a technology that adjusts the radio working channel and transmitting power according to the wireless environment around it. It includes Auto Channel Selection (ACS) and Auto Power Control (APC) functions. By default, RDA is enabled.

RDA relies on the background scanning feature. To ensure the RDA is effective, make sure the background scanning is ON, see "Performance optimization Window".

---

wIDS/wIPS Window

wIDS/wIPS window focus on the wireless security of the OAW-AP network.

There are two modes for wIDS/wIPS Window, Simplified Mode illustrated in Figure 4-23 and Advanced Mode illustrated in Figure 4-24. You can launch the Advanced Mode from Simplified Mode by clicking the wIDS/wIPS Window Frame.

Wireless is a borderless network and always works in an open environment which can be interfered with and attacked. It is useful to discover the surrounding wireless conditions, and based on that, provide instructions and tools to help administrators improve the quality of the wireless network. Usually there are two types of foreign unknown APs having a negative effect on the wireless network, they are interfering APs and rogue APs.

An **interfering AP** is an AP seen in the wireless environment but not connected to the wired network. The interfering AP can provide RF interference potentially, however, it is not considered a direct security threat, because it is not connected to the wired network.

A **rogue AP** is an unauthorized AP plugged into the wired side of the network or a foreign interfering AP broadcasting the same SSID with the AP group. A rogue AP is considered a security threat to the AP group.

Panel of wIDS/wIPS displays top 5 OAW-APs with interference from surrounding APs, and the top 5 OAW-APs with the most rogue APs surrounding, illustrated in Figure 4-23.

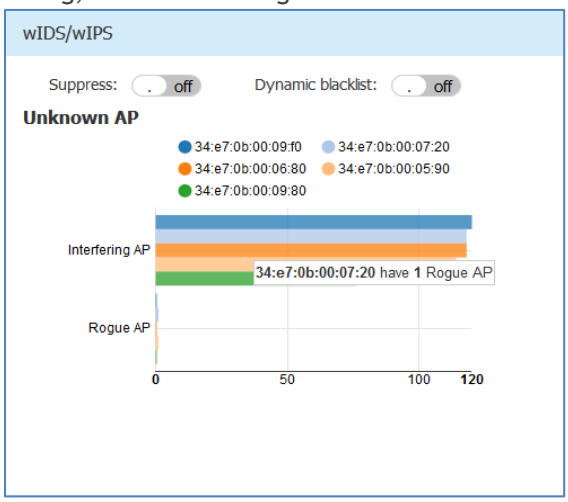

Figure 4-23 Top 5 AP interfered

AP whitelist: Both interfering APs and rogue APs are foreign unknown APs which can be found by background scanning and are listed in the unknown AP table, illustrated in Figure 4-24. However, some foreign APs found are trusted APs, those are not suitable for being classified as interfering APs or rogue APs. To avoid trusted foreign APs from being classified as interfering APs or rogue APs, you can add the trusted MAC address or MAC prefix to the AP whitelist, illustrated in Figure 4-25. If a foreign AP MAC address is added to the whitelist, it will not be displayed in the unknown AP list.

AP blacklist: Only rogue APs can be added to the blacklist. If a rogue AP is added to the blacklist, it cannot change its role to act as a client and access to the OAW-AP wireless network, illustrated in Figure 4-26.

Suppress: Enable/disable the function of rogue AP suppress. If enabled, the detecting OAW-AP will send DEAUTH frames to clients that have associated to the rogue AP, keeping the clients away from the unsafe wireless network. By default, the detecting OAW-AP does not send DEAUTH frames, see in Figure 4-23.

Dynamic blacklist: If enabled, all the rogue APs found will be added to the AP blacklist automatically, which prevents the rogue AP from changing its role to act as a client and access to OAW-AP wireless network. By default, the rogue AP is not added to the blacklist automatically, see in Figure 4-23.

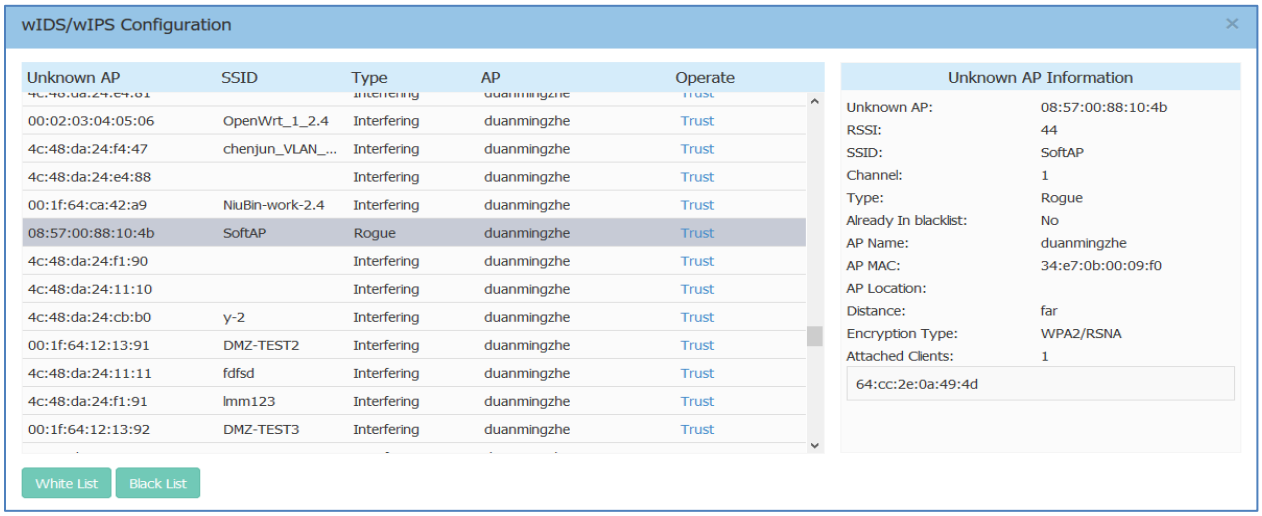

Figure 4-24 wIDS/wIPS Configuration Window

Table 4-12: Key word specification in wIDS/wIPS Configuration Window

Unknown AP Parameter	Specification
Unknown AP	MAC address of the unknown AP detected in the nearby.
SSID	SSID broadcasting by the unknown AP.
Type	Classified result of the unknown AP, can be interfering AP or rogue AP.
RSSI	Received Signal Strength Indication of the unknown AP.
Channel	Working channel of the unknown AP.
Already In Blacklist	Flag of rogue AP, depends on "the Dynamic blacklist" switch. If on, the rogue AP will be automatically added to the blacklist and the flag is true (Yes); If off or the unknown AP in list is not a rogue AP, the flag is false (No).
AP/AP Name	Name of detecting AP in the group.
AP MAC	MAC of detecting AP in the group.
AP Location	Location of detecting AP in the group.
Distance	Distance between unknown AP and the detecting AP in the group, it is measured by RSSI of the unknown AP: Nearest- RSSI>75; Near- 50<RSSI<75; Far-25<RSSI<50; Farthest-RSSI<25;
Encryption Type	The encryption type of the SSID being broadcast by the unknown AP.
Attached Clients	The number of clients attached to the unknown AP, and MAC of each client.
Operate	Operation to trust the foreign AP and delete it from the unknown AP list. If the foreign AP is trusted, its MAC address will be added to the whitelist.
White List	Whitelist of foreign APs. Those not considered as security threat to the OAW-AP network, you can add the trusted MAC address into whitelist manually, see more in Figure 4-25.
Black List	Blacklist of foreign APs. Those classified as rogue APs and pretending to act as a client to access the OAW-AP network. If Dynamic blacklist: on and there are detected rogue APs, all the rogue APs will be added to the blacklist automatically. You can remove a foreign AP from the blacklist by the **Trust** operation, see more in Figure 4-26.

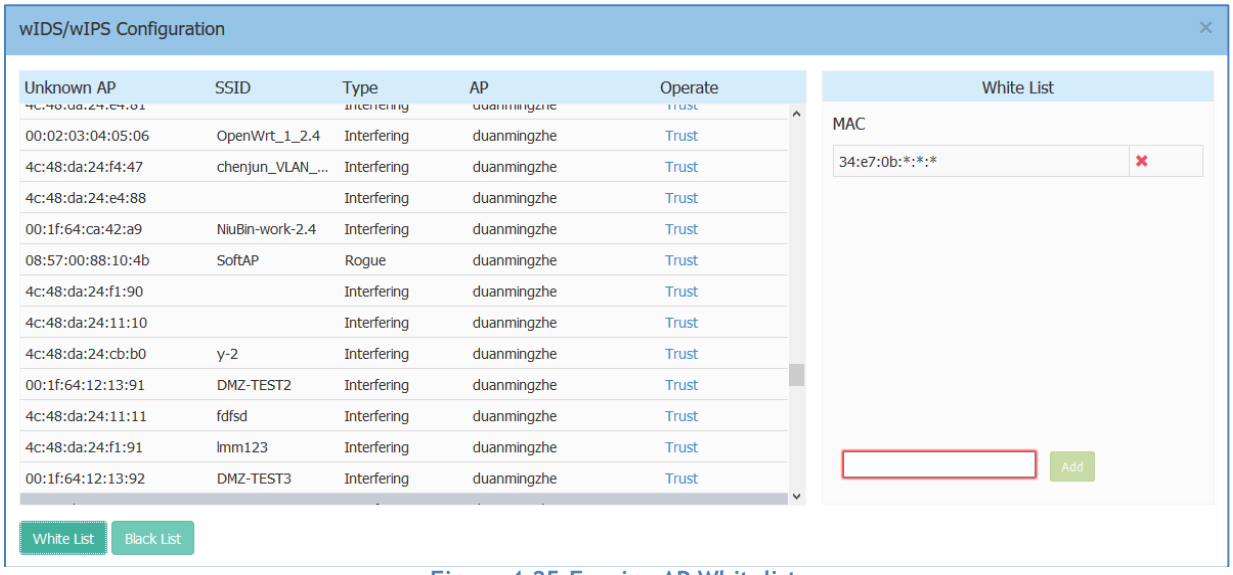

Figure 4-25 Foreign AP Whitelist

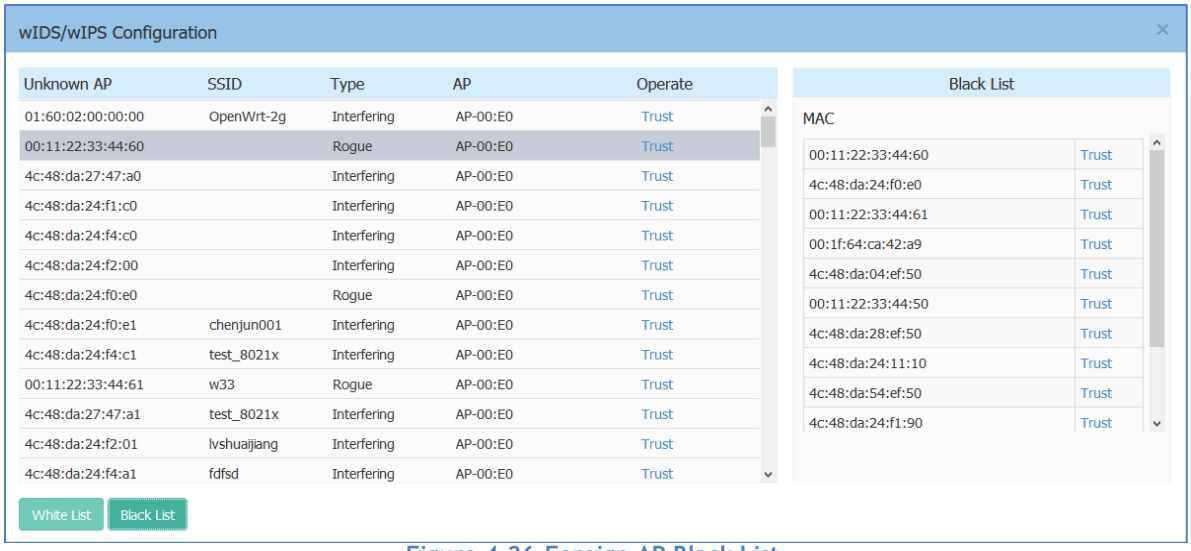

Figure 4-26 Foreign AP Black List

You can remove a foreign AP from the Unknown AP list or blacklist by the **Trust** operation. If you trust an unknown AP (interfering AP/rogue AP), it is removed from the Unknown AP list and blacklist, and its MAC address will be added to whitelist.

Performance Optimization Window

Wireless performance optimization is useful to enhance the quality of wireless service for users. The performance optimization includes Background Scanning, Band Steering, Voice and Video Awareness, and Multicast, illustrated in Figure 4-27 and Figure 4-28.

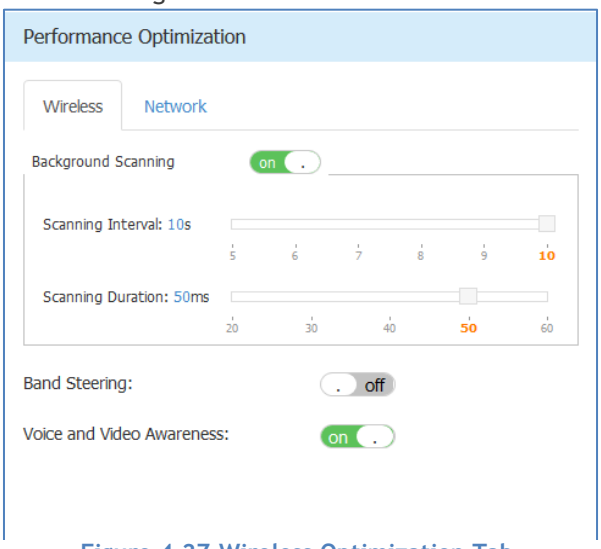

Figure 4-27 Wireless Optimization Tab

Background Scanning: Wireless networks operate in environments with electrical and radio frequency devices that can interfere with network communications. Microwave ovens, cordless phones, and even adjacent Wi-Fi networks are all potential sources of continuous or intermittent interference. The background scanning is able to examine the radio frequency (RF) environment in which the Wi-Fi network is operating, identify interference and classify its sources.

Background scanning is the basis for some advanced features such as: wIDS/wIPS, RDA (ACS/APC) etc. When it's turned OFF, the foreign AP detection and rogue suppression will stop and the RDA will drop its precision.

By default, background scanning is enabled.

Voice and Video Awareness: Background scanning needs to be aware of existing traffic on the OAW-AP, if there is an ongoing voice/video service, scanning should not be done to ensure uninterrupted traffic; and allows to resume scanning when there is no active voice/video session.

By default, Voice and Video Awareness feature is enabled.

Band Steering: Band steering supports **Prefer 5GHz** and **User Load Balance**.
Prefer 5GHz feature assigns the clients to the 5 GHz band prior to the 2.4G band. Thus can reduce co-channel interference and increase available bandwidth for clients, because there are more channels on 5 GHz band.

User Load Balance: Based on the user amount of adjacent APs, clients are steered from a busy AP to an idle AP.

By default, band steering is disabled.

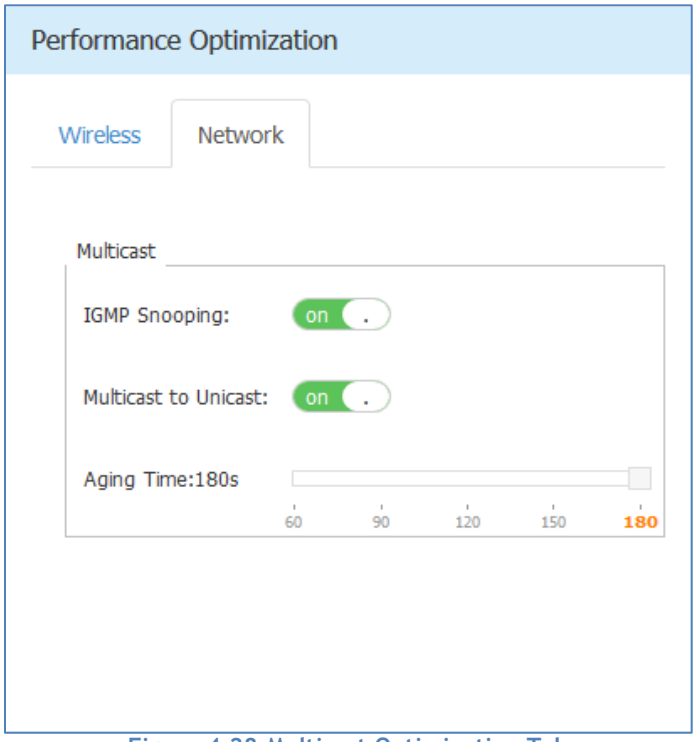

Figure 4-28 Multicast Optimization Tab

Multicast optimization includes IGMP Snooping and Multicast to Unicast.

IGMP Snooping: IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows APs to listen in on the IGMP conversation between hosts and server. By listening to these conversations the AP maintains a table of multicast receivers.

The multicast receiver can be aged out if it doesn't receive any multicast packets for a while, the aging time can be set, default value is 180 seconds, illustrated in Figure 4-28.

By default, IGMP snooping is enabled.

Multicast to Unicast: This feature allows APs to convert multicast streams into unicast streams over the wireless network based on the IGMP snooping table. Enabling Multicast to Unicast can enhance the quality and reliability of video streams, while preserving the bandwidth available to the non-video services.

By default, Multicast to Unicast feature is enabled.

Access Page

The Access page focuses on user access management including: user authentication, user backlist and whitelist and user access control list.

The Access page is divided into three windows: Authentication window, Blacklist & Whitelist window, ACL window, illustrated in Figure 4-29.

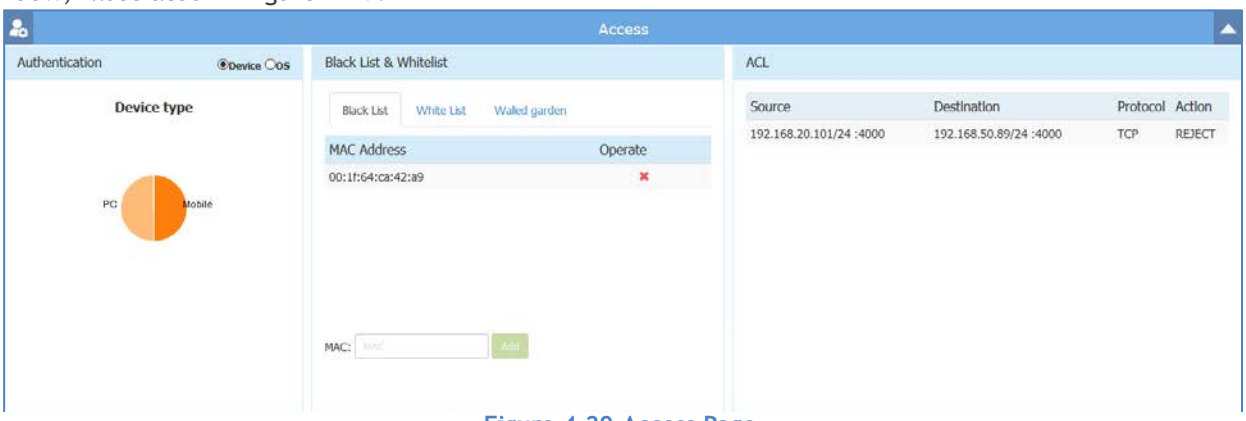

Figure 4-29 Access Page

Authentication Window

Authentication Window displays the user authentication and accessing information.

There are two modes for Authentication Window, Simplified Mode illustrated in Figure 4-30 and Advanced Mode illustrated in Figure 4-31. You can launch the Advanced Mode from Simplified Mode by clicking the Authentication Window Frame.

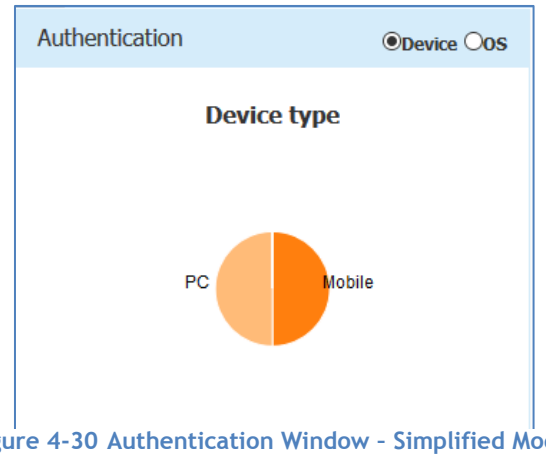

Figure 4-30 Authentication Window – Simplified Mode

The simplified Authentication Window displays the statistics information of the users' device and operating system, illustrated in Figure 4-30.

The advanced Authentication Window is mainly used to configure the captive portal authentication, illustrated in Figure 4-31.

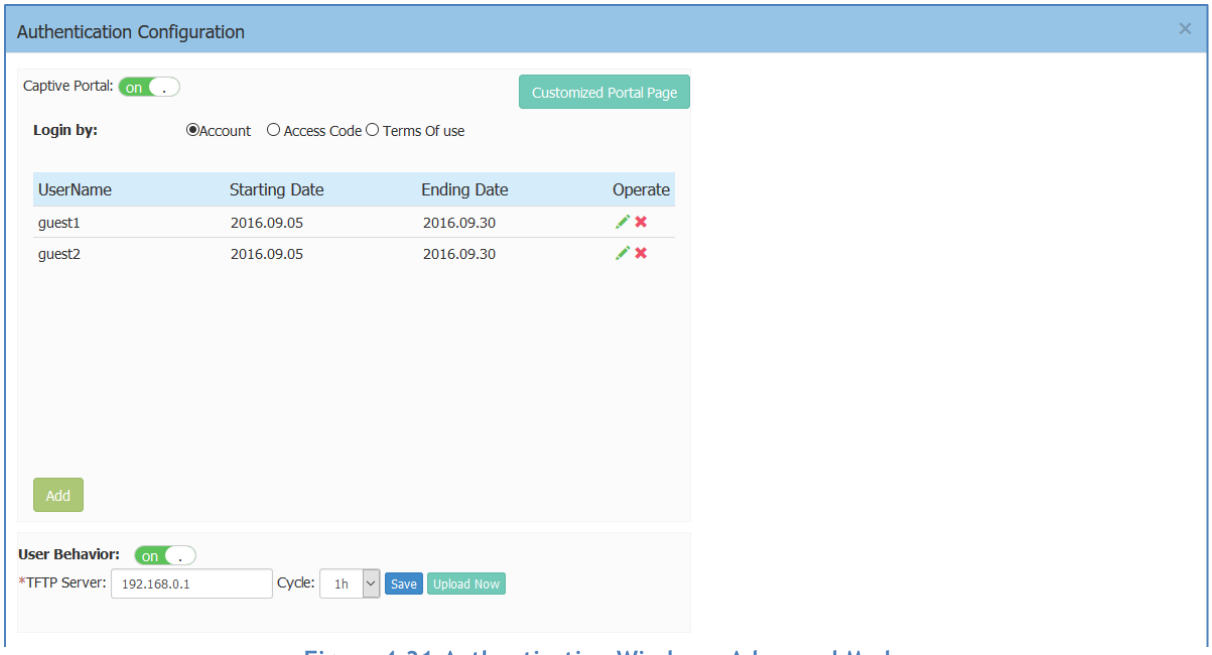

Figure 4-31 Authentication Window - Advanced Mode

Table 4-13: Key word specification in Authentication Window (Advanced Mode)

Captive Portal: on	Captive portal service enable/disable switch. It MUST be enable/on to make the captive authentication effective.
Login by: Account Access Code Terms Of use	Login method used by the captive portal users, corresponding to different login page and credentials: • Account - Login by user account, you need to add accounts for portal users, see Create Users or Access Code. The users enter their usernames and passwords to pass the authentication and access the wireless network, see more in Customized Portal Page - Login by Account. • Access Code - Login by access code, you need to add access code for portal user, see Create Users or Access Code. The users enter the access code to pass the authentication, see more in Customized Portal Page - Login by access code. • Terms of use - Login by terms of use. The users accept the terms of use and pass the authentication, see more in Customized Portal Page - Login by Terms of use.
UserName	Account of captive portal user.
Starting Date	Account effective starting date.
Ending Date	Account effective ending date.
Operate	Edit or delete captive portal users.
Add	Add users for captive portal authentication when using login by account.
Customized Portal Page	Customized portal web page according to application requirement.
Preview	Preview the customized portal web page.
Default	Return the customized portal web page to the system default.

User Behavior: on	Enable logging user behavior to a TFTP server, including: client online and client offline. More details can see in Note4-7.
TFTP Server: 192.168.0.1	Specify the TFTP server to restore the user behavior logs.
Cycle: 1h	Specify the cycle for uploading user behavior logs to TFTP server, can be set to 1 hour, 2 hours and 4 hours.
Save	Save the TFTP setting for uploading user behavior logs.
Upload Now	Upload the user behavior logs to the TFTP server manually.

Note

Note 4-7: The log information of user behavior includes: username, user MAC, user IP, connecting WLAN, Online/Offline behavior and time stamp.

Customized Portal Page Panel

You can customize your splash page used in the captive portal authentication by changing the Logo, background and terms of use, illustrated in Figure 4-32.

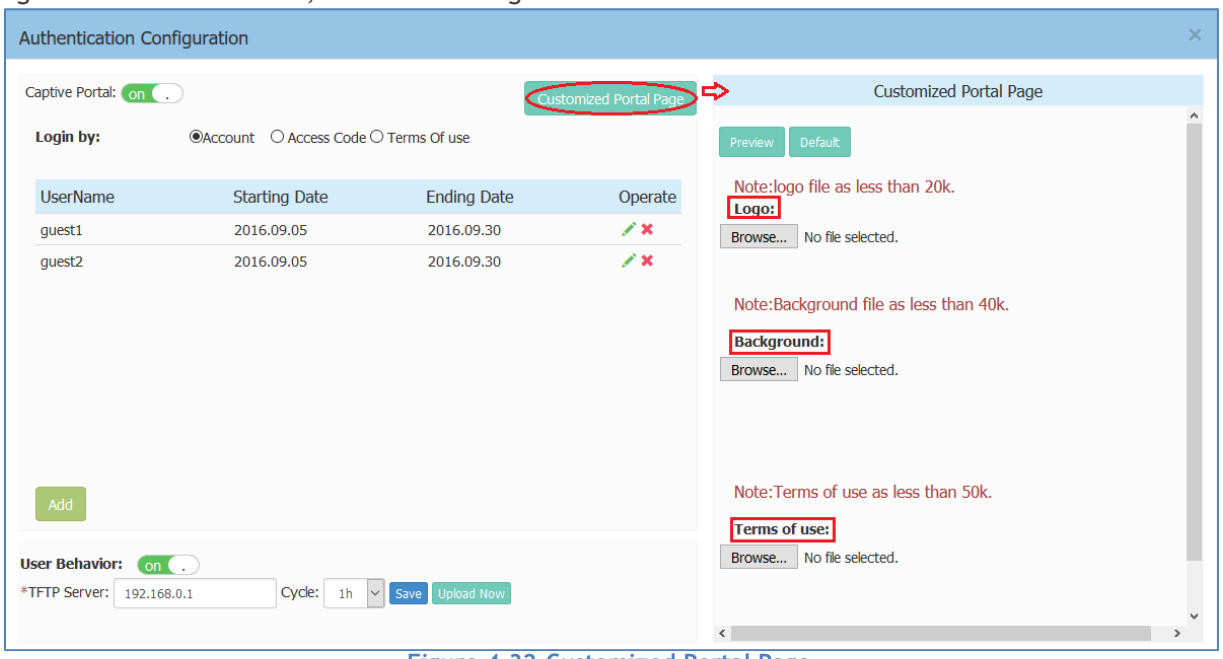

Figure 4-32 Customized Portal Page

There are three splash page templates provided by the system, you can choose your captive portal login method and customize your own splash page accordingly, see more in Customized Portal Page - Login by Account, Customized Portal Page - Login by access code and Customized Portal Page - Login by Terms of use.

Customized Portal Page – Login by Account

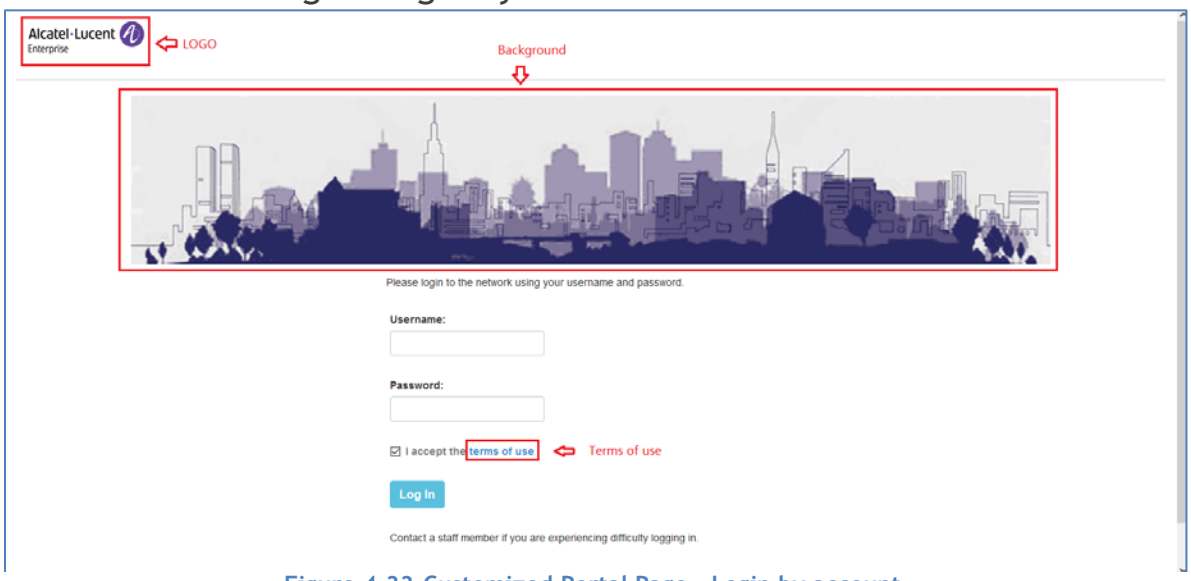

Figure 4-33 Customized Portal Page – Login by account

Customized Portal Page – Login by Access Code

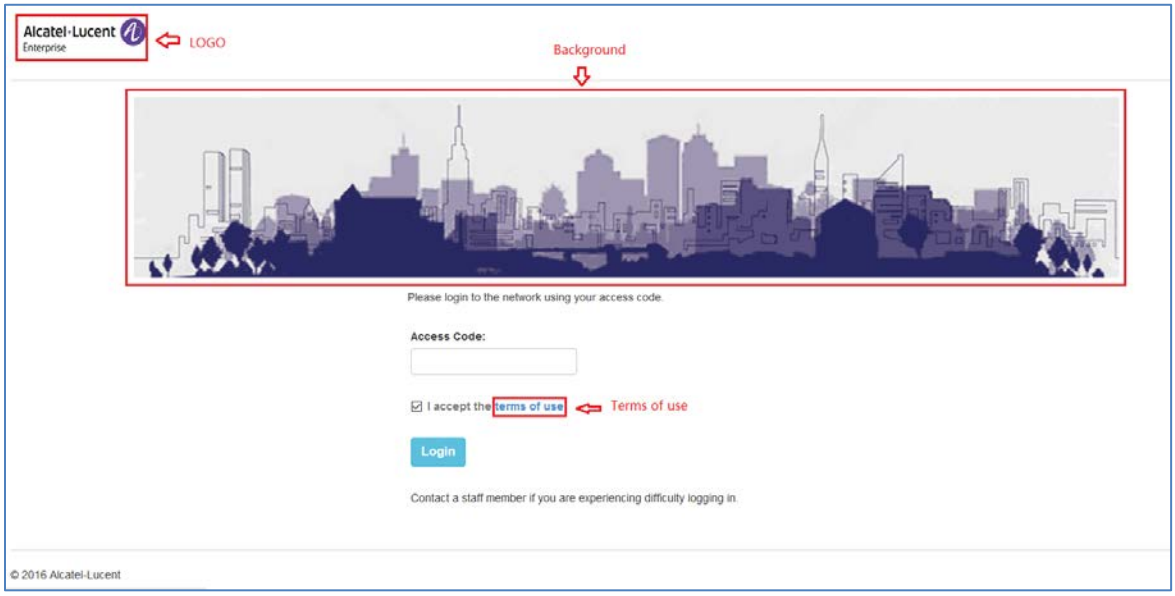

Figure 4-34 Customized Portal Page – Login by access code

Customized Portal Page – Login by Terms of Use

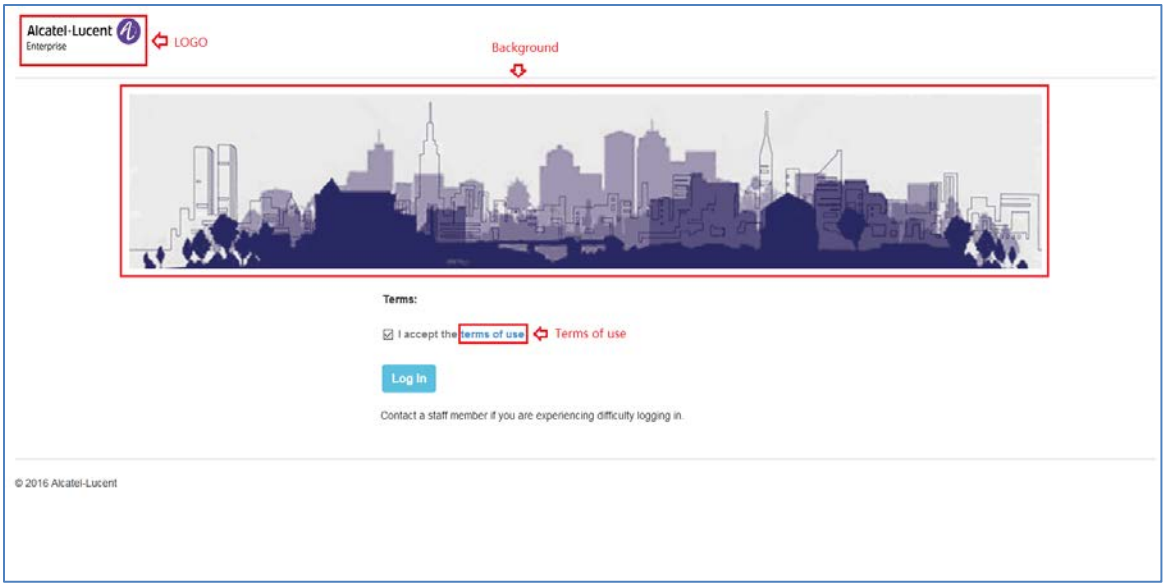

Figure 4-35 Customized Portal Page – Login by Terms of use

Figure 4-36 Customized Portal Page – Terms of use

Client Blacklist & Whitelist Window

Blacklist & Whitelist Window focuses on the basic access control mechanism for users connecting to the ALE WLAN network based on the client level. It includes three tabs: Black List Tab, Whitelist Tab and Wall Garden Tab.

Those clients on the blacklist are denied to associate to the OAW-AP wireless network. Once a client is in the blacklist, it cannot connect to any WLAN of any security level (Enterprise/Personal/Open). You can add/delete the blacklist based on client's MAC address, illustrated in Figure 4-37.

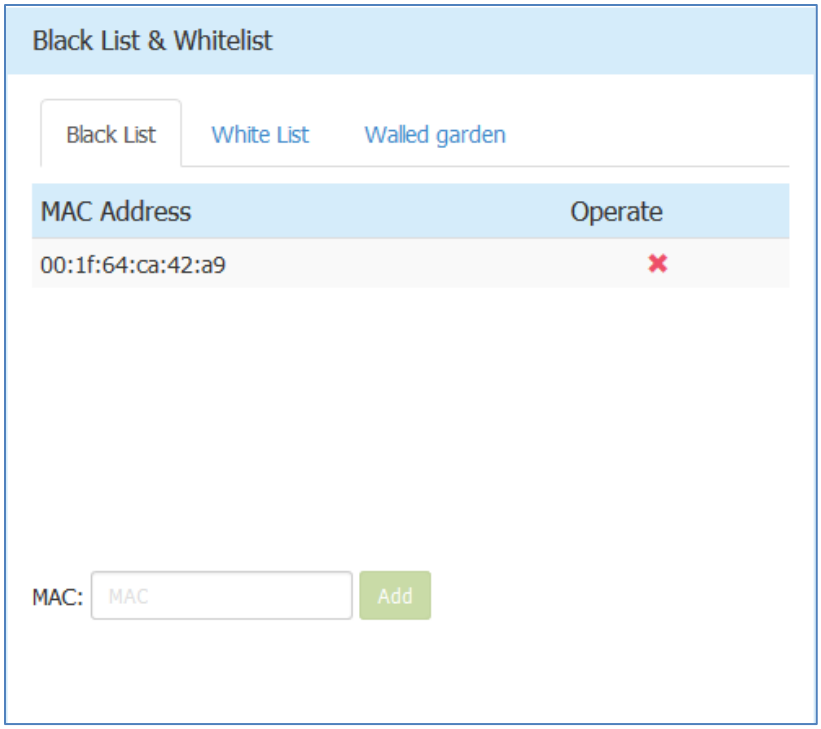

Figure 4-37 Black List Tab

The whitelist is applied to captive portal authentication ONLY. Those clients on the whitelist are permitted to access the network resource without passing the captive portal authentication. You can manually add/remove client(s) to/from the whitelist for captive portal authentication by MAC address, illustrated in Figure 4-38. The whitelist does not support Enterprise/Personal WLANs. This means that the clients in the whitelist are not allowed to access Enterprise/Personal WLANs without using correct credentials.

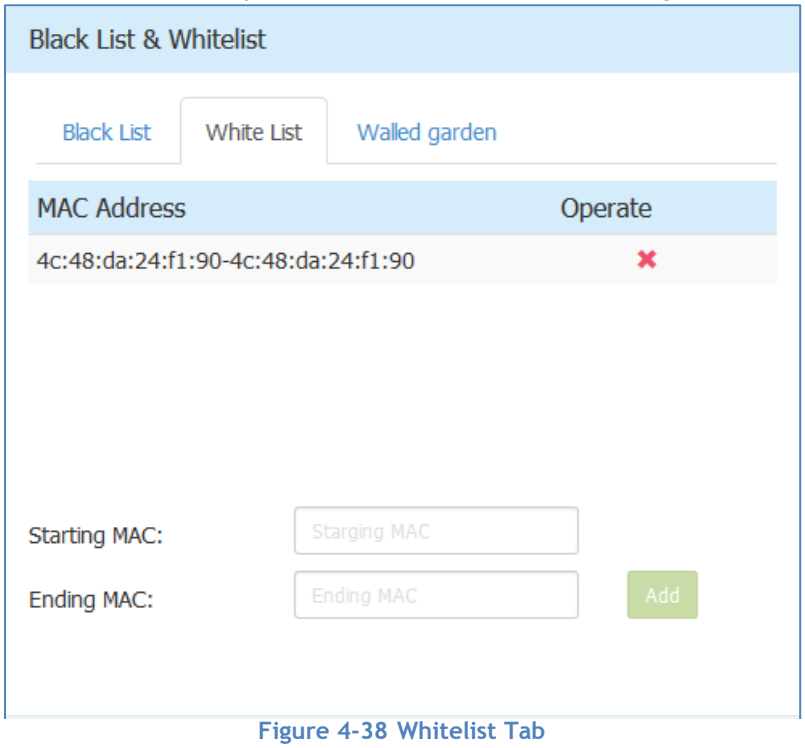

Figure 4-38 Whitelist Tab

The walled garden is a control mechanism over network resources, it restricts access to non-approved applications or content. The walled garden is applied for captive portal authentication ONLY. The client is able to access the network resource (For example: website of the hotel) before passing the captive portal authentication. You can add/remove allowed IP(s) to/from the walled garden, illustrated in Figure 4-39.

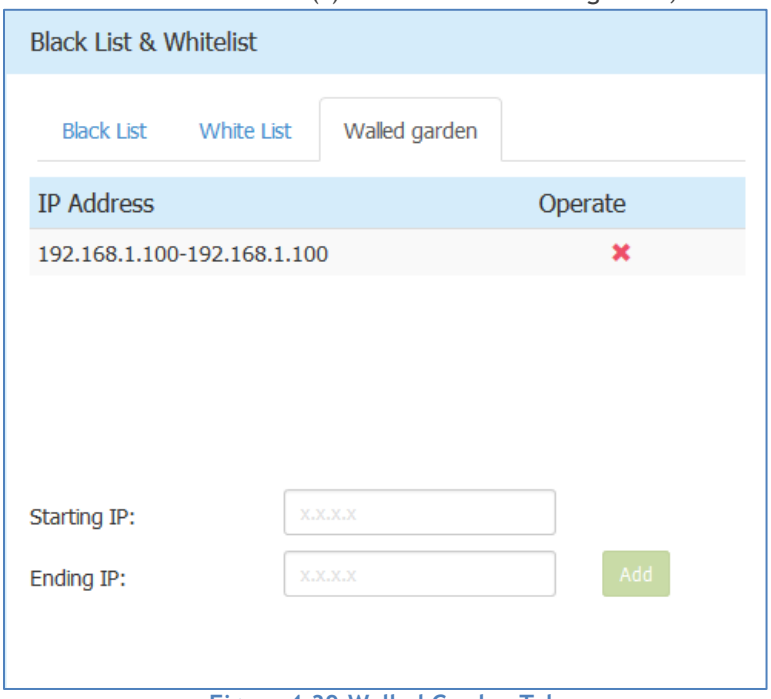

Figure 4-39 Walled Garden Tab

Note

Note 4-7: To allow the user to access some network resources (For example: office website or open file server) before passing the captive portal authentication, you have to know the IP address of the network resource and add it into the walled garden.

Access Control List Window

There are two modes for ACL Window, Simplified Mode illustrated in Figure 4-40 and Advanced Mode illustrated in Figure 4-41. You can launch the Advanced Mode from Simplified Mode by clicking the ACL Window Frame.

The simplified ACL Window displays the ACLs configured, illustrated in Figure 4-40.

You can create L3 ACLs using wildcard entries for both IP address and TCP/UDP/ICMP ports. See the advanced ACL Window illustrated in Figure 4-41.

The ACL rules created in the list are applied sequentially, based on the precedence of top-to-bottom.

By default, traffic is allowed to pass if no ACL rules are matched (Default ACL action is ‘Accept’).

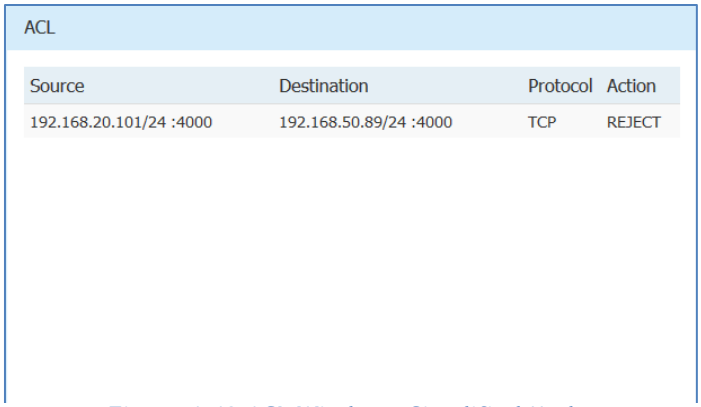

Figure 4-40 ACL Window - Simplified Mode

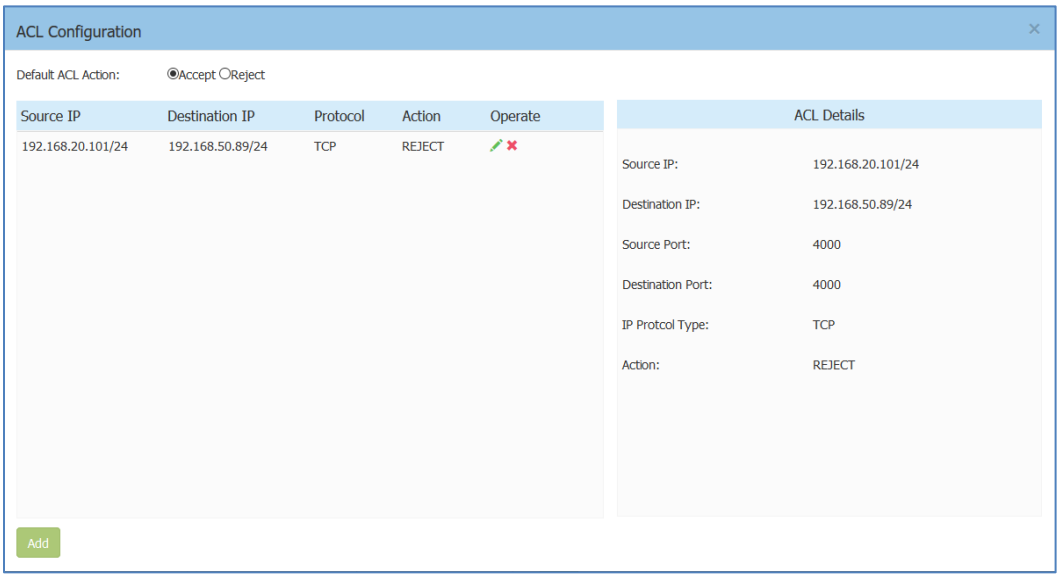

Figure 4-41 ACL Window - Advanced Mode

Table 4-14 ACL Parameter Specification

Parameter	Specifications
Source IP	The source IP address.
Destination IP	The destination IP address.
Source Port	Source UDP or TCP port.
Destination Port	Destination UDP or TCP port.
IP Protocol	There are three options for IP Protocol, TCP, UDP or ICMP.
Action	Accept or Reject

Note

Note 4-8: OAW-AP supports L2 ACLs, you can blacklist/white-list certain MACs or a range of MAC addresses, see Blacklist & Whitelist Window. Also, you can setup rules based on 802.1p/DSCP while creating a new SSID, see Modify WLAN QoS.

5 WLAN Configuration

Configuring WLAN should be the first step when setting up your Wi-Fi network. This section contains the following topics:

- ➔ Create NEW WLAN
- ➔ Delete Your WLAN
- ➔ Modify Your WLAN
- ➔ Modify WLAN Qos

Create New WLAN

To create a new WLAN, click on the hyperlink 'New' to launch the WLAN creation window. There are three security levels of WLANs that can be created: Enterprise, Personal and Open (Captive Portal).

Enterprise: Also referred to as 802.1X mode, this is designed for enterprise networks and requires a RADIUS authentication server. This requires a more complicated setup, but provides additional security (e.g. protection against dictionary attacks on short passwords). Various kinds of the Extensible Authentication Protocol (EAP) are used for authentication. Enterprise mode is available with both WPA and WPA2.

Personal: Also referred to as PSK (pre-shared key) mode, this is designed for home and small office networks and doesn't require an authentication server. Each wireless network device encrypts the network traffic using a 256 bit key. This key may be entered either as a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters. Personal mode is available with both WPA and WPA2.

Open (Captive Portal): No Authentication or encryption method for the wireless network. User data will be transmitted as plain text transmit mode over the air. Captive portals are mainly used in wireless open networks where the users are shown a welcome message informing them of the conditions of access. Often captive portals are used for marketing and commercial communication purposes and they allow the providers of this service to display or send advertisements to users who connect to the Wi-Fi access points.

Create an Enterprise WLAN

Enterprise WLAN creation window has two display modes, simplified mode and advanced mode, respectively illustrated in Figure 5-1and Figure 5-2. You can switch to advanced mode from simplified mode by clicking the hyperlink Advance .

There are six essential parameters needed to be configured in simplified mode, they are WLAN Name, Security Level, Key Management and AuthServer, AuthPort and AuthSecret. Other parameters will be considered as per the default value. To configure other advanced parameters, you must switch to advanced mode. Refer to Table 5-1 for details about each parameter.

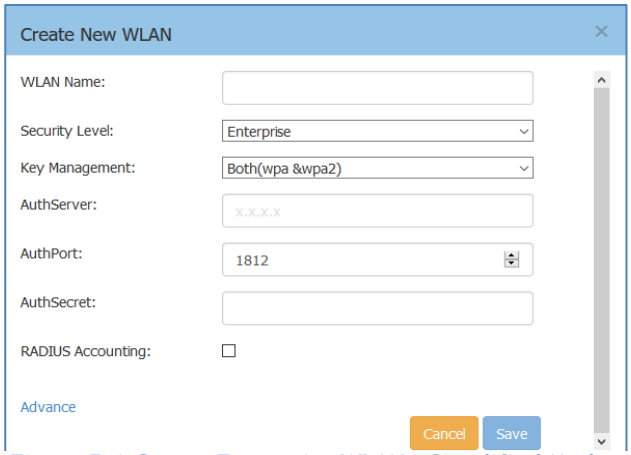

Figure 5-1 Create Enterprise WLAN - Simplified Mode

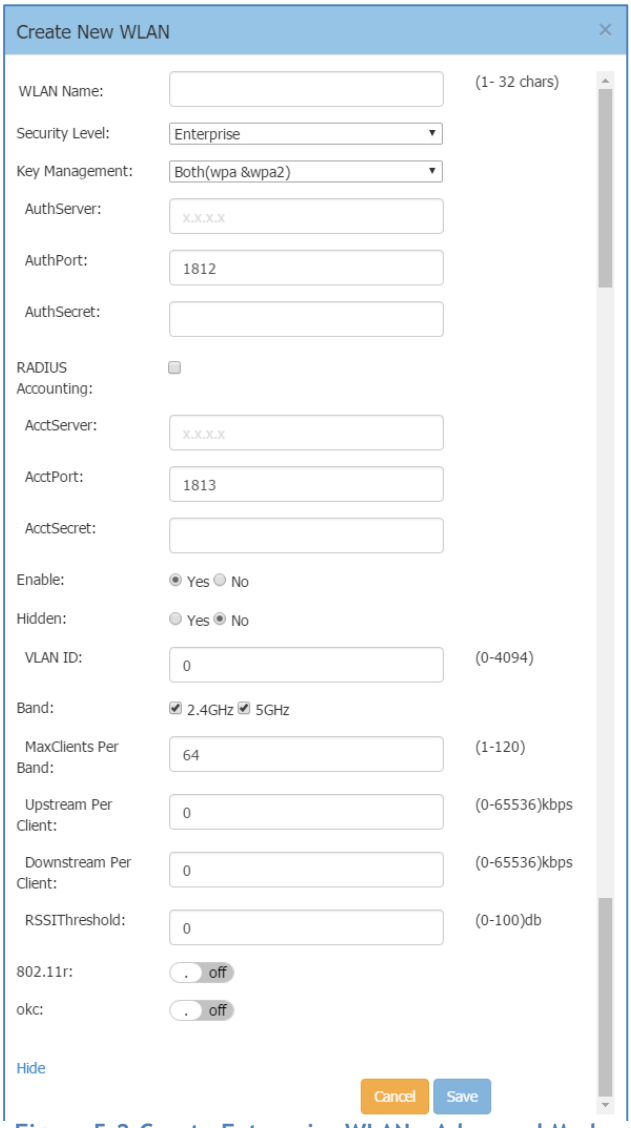

Figure 5-2 Create Enterprise WLAN - Advanced Mode

Table 5-1: Key word specification in Enterprise WLAN Configuration Window

WLAN Parameter	Specification
WLAN Name	Label or name of WLAN.
Security Level	Security mode of WLAN, from high to low is Enterprise>Personal>Open. Here select the Enterprise mode.
Key Management	WPA2/WPA encryption method. It is applicable to Enterprise/Personal WLANs only.
AuthServer	IPv4 address of the authentication server (RADIUS).
AuthPort	Communication port of the authentication server. The default value is 1812.
AuthSecret	Shared secret key used by the authentication server, in ASCII format.
RADIUS Accounting	Select the checkbox if accounting service is needed. By default it is not selected.
AcctServer	IPv4 address of the accounting server.
AcctPort	Communication port of the accounting server. The default value is 1813.
AcctSecret	Shared secret key used by the accounting server, in ASCII format.
Enable	Specify the WLAN state, Yes indicates that WLAN is in broadcast state, while No indicates WLAN is not in broadcast state.
Hidden	Specify visibility of the WLAN, Yes indicates that WLAN is visible to users, while No indicates WLAN is invisible.
VLAN ID	Identifier of the VLAN to which the WLAN mapping, it is a user VLAN.
Band	Select a value to specify the band at which the network transmits radio signals. You can set the band to 2.4 GHz, 5 GHz, or All. The All option is selected by default.
Max Clients per band	Specify the maximum number of clients that can be configured for each BSSID on a WLAN. You can specify a value within the range of 0 to 120. The default value is 64.
Upstream Per Client	Specify the maximum upstream bandwidth limitation for each user.
Downstream Per Client	Specify the maximum downstream bandwidth limitation for each user.
RSSIThreshold	Specify a threshold value to limit the number of incoming probe requests.
802.11r	Select to enable IEEE 802.11r (Fast BSS Transition). The Fast BSS Transition mechanism minimizes the delay when a client transitions from one BSS to another within the same group.
okc	If OKC is enabled, a cached pairwise master key (PMK) is used when the client roams to a new AP. This allows faster roaming of clients without the need for a complete 802.1x authentication.
Cancel	The WLAN Creation Window is closed if you click 'Cancel' button.
Save	Click 'Save' to save the configuration and create the WLAN.

Create a Personal WLAN

Personal WLAN creation window has two display modes, simplified mode and advanced mode, respectively illustrated in Figure 5-3 and Figure 5-4. You can switch to advanced mode from simplified mode by clicking the hyperlink Advance .

There are five essential parameters to be configured for a Personal WLAN in simplified mode, they are WLAN Name, Security Level, Key Management, Password Format and Password. Other parameters will be considered as per the default value. To configure other advanced parameters, you must switch to advanced mode. Refer to Table 5-2 for details about each parameter.

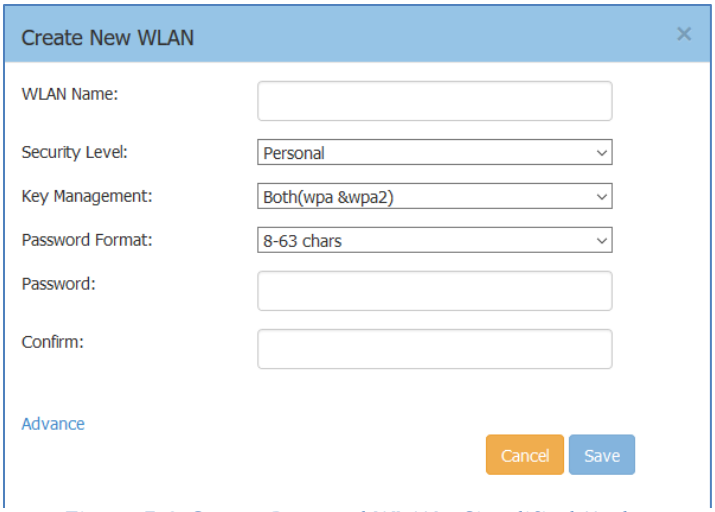

Figure 5-3 Create Personal WLAN - Simplified Mode

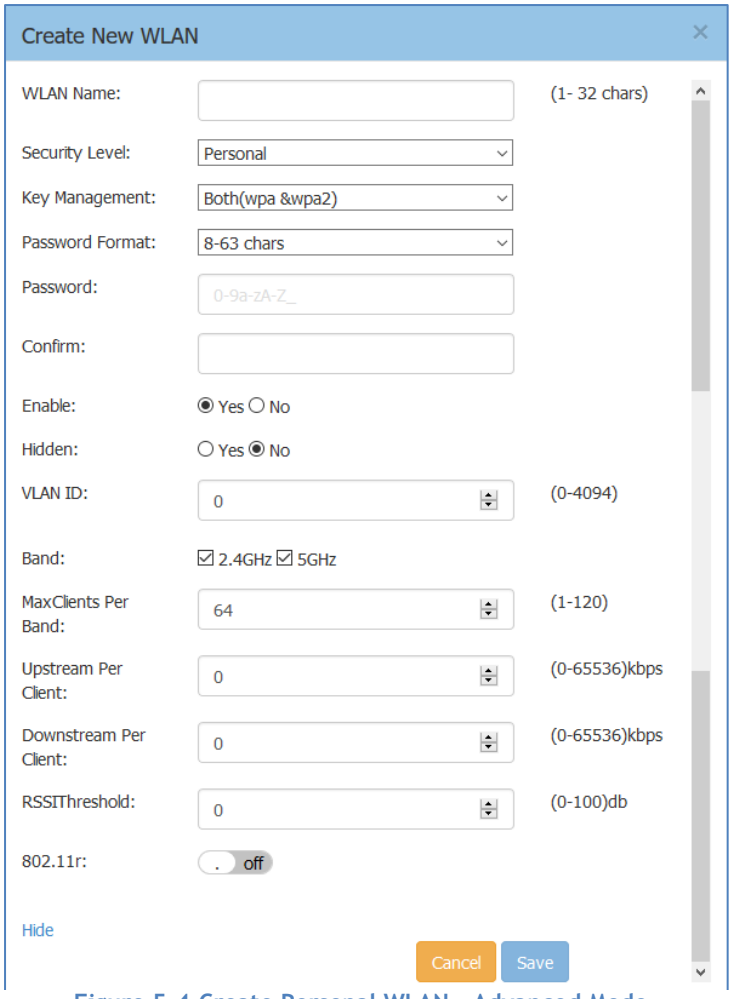

Figure 5-4 Create Personal WLAN - Advanced Mode

Table 5-2: Key word specification in Personal WLAN Configuration Window

WLAN Parameter	Specification
WLAN Name	Label or name of WLAN.
Security Level	Security Level of WLAN, from high to low is Enterprise>Personal>Open. Here select the Personal type.
Key Management	WPA2/WPA encryption method. It is applicable to Enterprise/Personal WLANs only.
Password Format	Password format of Personal WLAN. There are two password formats to be selected: Either as a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters.
Password	Enter the password for the Personal WLAN.
Confirm	Reenter the password for the Personal WLAN.
Enable	Specify the WLAN state, Yes indicates that WLAN is in broadcast state, while No indicates WLAN is not in broadcast state.
Hidden	Specify visibility of the WLAN, Yes indicates that WLAN is visible to users, while No indicates WLAN is invisible.
VLAN ID	Identifier of the VLAN to which the WLAN mapping, it is a user VLAN.
Band	Select a value to specify the band at which the network transmits radio signals. You can set the band to 2.4 GHz, 5 GHz, or All. The All option is selected by default.
Max Clients per band	Specify the maximum number of clients that can be configured for each BSSID on a WLAN. You can specify a value within the range of 0 to 120. The default value is 64.
Upstream Per Client	Specify the maximum upstream bandwidth limitation for each user.
Downstream Per Client	Specify the maximum downstream bandwidth limitation for each user.
RSSIThreshold	Specify a threshold value to limit the number of incoming probe requests.
802.11r	Select to enable IEEE 802.11r (Fast BSS Transition). The Fast BSS Transition mechanism minimizes the delay when a client transitions from one BSS to another within the same group.
Cancel	The WLAN Creation Window is closed if you click 'Cancel' button.
Save	Click 'Save' to save the configuration and create the WLAN.

Create a Captive Portal WLAN

Captive Portal WLAN creation window has two display modes, simplified mode and advanced mode, respectively illustrated in Figure 5-5 Create Captive Portal WLAN - Simplified Mode and Figure 5-6 Create Captive Portal WLAN - Advanced Mode. You can switch to advanced mode from simplified mode by clicking the hyperlink Advance .

There are three essential parameters to be configured for a Captive Portal WLAN in simplified mode, they are WLAN Name, Security Level (Open) and Captive Portal (Yes). Other parameters will be considered as per the default value. To configure other advanced parameters, you must switch to advanced mode. Refer to Table 5-3 for details about each parameter.

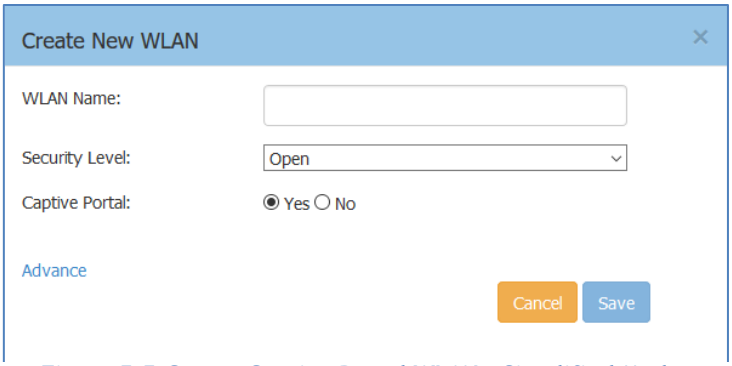

Figure 5-5 Create Captive Portal WLAN - Simplified Mode

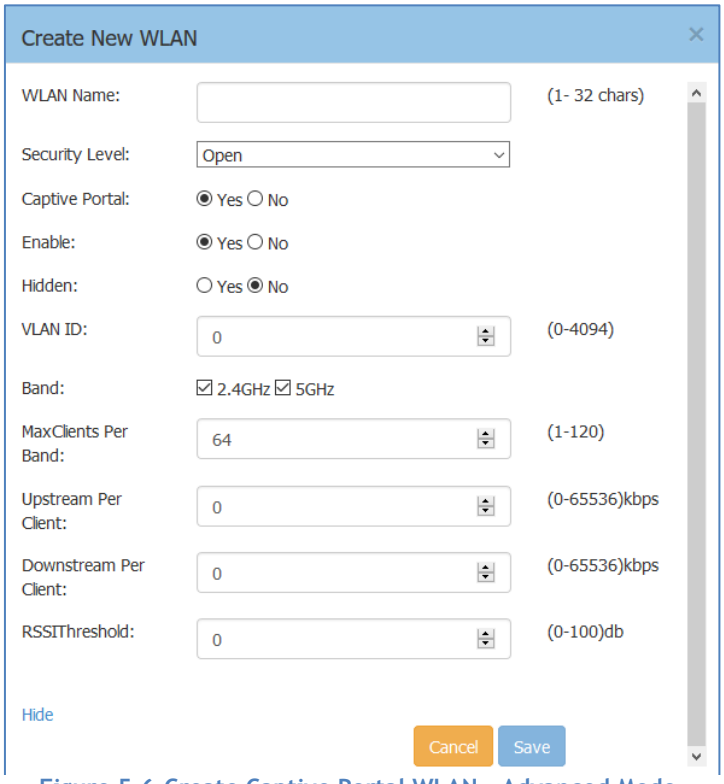

Figure 5-6 Create Captive Portal WLAN - Advanced Mode

Table 5-3: Key word specification in Captive Portal WLAN Configuration Window

WLAN Parameter	Specification
WLAN Name	Label or name of WLAN.
Security Level	Security Level of WLAN, from high to low is Enterprise>Personal>Open. Here select the Open type.
Captive Portal	Specify the captive portal authentication supporting state. Yes indicates the WLAN supports captive portal authentication, while No indicates the WLAN does not support captive portal authentication.
Enable	Specify the WLAN state, Yes indicates that WLAN is in broadcast state, while No indicates WLAN is not in broadcast state.
Hidden	Specify visibility of the WLAN, Yes indicates that WLAN is visible to users, while No indicates WLAN is invisible.

VLAN ID	Identifier of the VLAN to which the WLAN mapping, it is a user VLAN.
Band	Select a value to specify the band at which the network transmits radio signals. You can set the band to 2.4 GHz, 5 GHz, or All. The All option is selected by default.
Max Clients per band	Specify the maximum number of clients that can be configured for each BSSID on a WLAN. You can specify a value within the range of 0 to 120. The default value is 64.
Upstream Per Client	Specify the maximum upstream bandwidth limitation for each user.
Downstream Per Client	Specify the maximum downstream bandwidth limitation for each user.
RSSIThreshold	Specify a threshold value to limit the number of incoming probe requests.
Cancel	The WLAN Creation Window is closed if you click 'Cancel' button.
Save	Click 'Save' to save the configuration and create the WLAN.

After the WLAN has been created, proceed to: How to Configure Captive Portal Authentication to compete the configuration.

Delete Your WLAN

In WLAN Window Advanced Mode Figure 4-3 WLAN Window-Advanced Mode, you can delete the WLAN by clicking the '✖' Button, as shown in Figure 5-7.

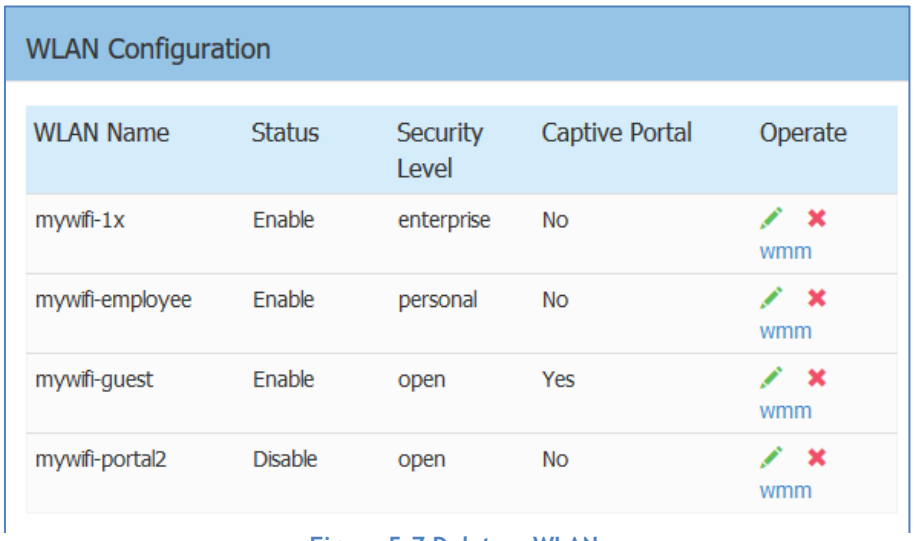

Figure 5-7 Delete a WLAN

Modify Your WLAN

In WLAN Window Advanced Mode Figure 4-3 WLAN Window-Advanced Mode, you can modify the WLAN by clicking the ' ' Button, shown in Figure 5-8. All configurable WLAN parameters will be displayed on the right of WLAN Window Advanced Mode, Enterprise WLAN see Table 5-1, Personal WLAN see Table 5-2 and Captive Portal WLAN see Table 5-3. Click Cancel to cancel the modification or click Save to save the configuration.

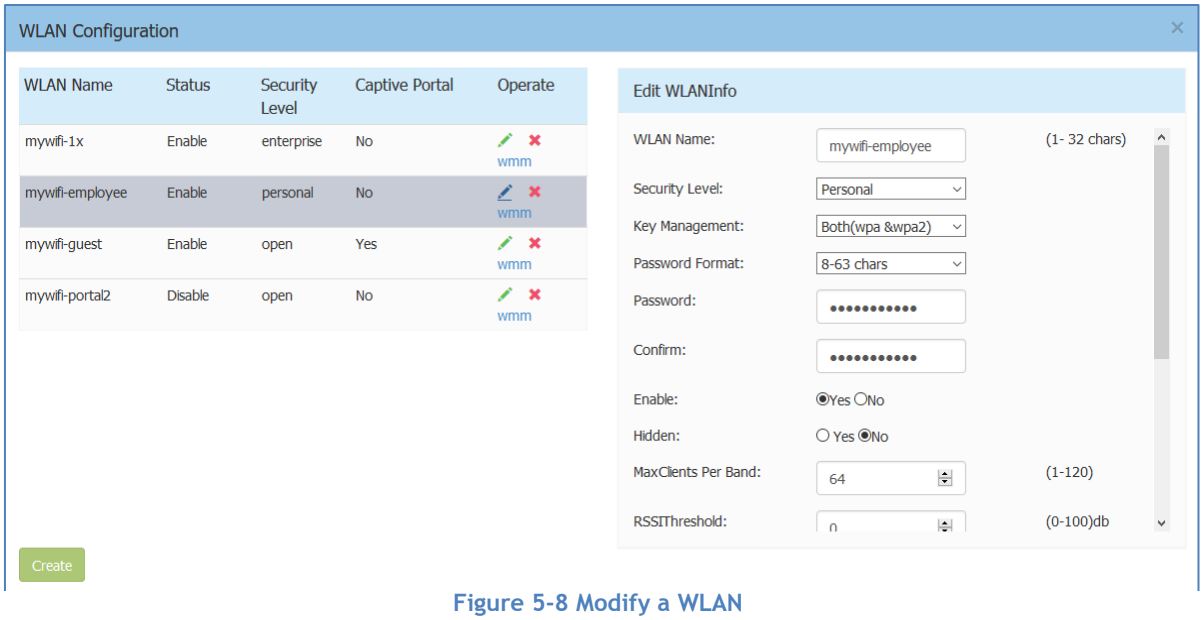

Figure 5-8 Modify a WLAN

Modify WLAN QoS

Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic Quality of service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to four Access Categories (AC): voice (AC_VO), video (AC_VI), best effort (AC_BE), and background (AC_BK). It is suitable for well-defined applications that require QoS, such as Voice over IP (VoIP) on Wi-Fi phones.

You can edit the mapping relationship between DSCP/802.1p values and WMM priorities for a WLAN on OAW-AP, illustrated in Figure 5-9.

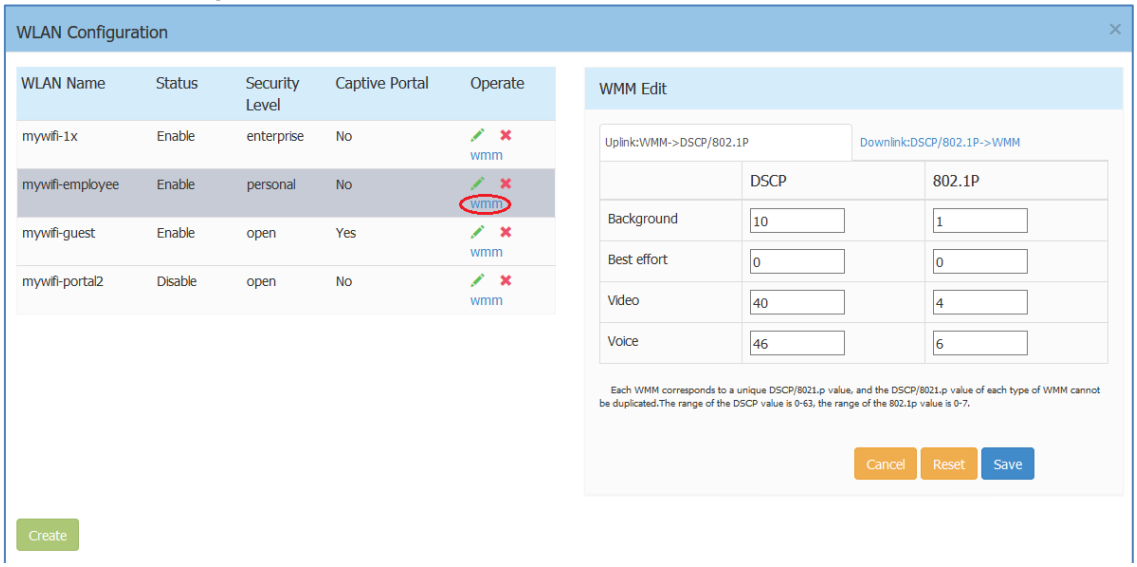

Figure 5-9 Modify WLAN QoS

6 AP Management

This chapter describes how to configure and manage your AP. The ALE Wi-Fi solution is a controller-less based architecture. The APs can establish an autonomous group, in which there are three types of AP roles, Primary Virtual Controller (PVC), Secondary Virtual Controller (SVC) and member AP. This chapter describes how to manage the group and how to check, backup, restore AP configuration and to upgrade firmware in GUI.

AP Management procedures described in this chapter include:

- ➔ AP Group Management
- ➔ Import and Export AP Configuration
- ➔ Upgrade AP Firmware
- ➔ Modify AP Name and IP Address
- ➔ Check AP Configuration Detail
- ➔ Modify AP Transmission Power and Channel
- ➔ AP LED Specification
- ➔ Locate AP or Turn LED Off
- ➔ Kick off an AP from the group
- ➔ Allow an AP to join the group
- ➔ How to add a new AP to the group
- ➔ How to replace an current AP in the group
- ➔ How to Setup Wireless Networks with more than 16 APs
- ➔ How to Configure the AP if there is no DHCP server

AP Group Management

By default, APs will have the group ID 100 and all APs that have the same group ID will align to the same group. The group will select the AP which has the highest MAC address as the PVC and the AP which has the second highest MAC address as the SVC. Each group has a management IP address that is a virtual IP and will be assigned to the PVC. When the PVC fails to respond due to an unexpected error or issue, the SVC will automatically upgrade to act as the PVC. There will be no interruption or service disturbance to member APs or any of the wireless users.

Table 6-1 describes the several group attributes parameters.
To configure or modify the group attributes, launch the window 'System-General Configuration', as shown in Figure 6-1. AP group information will be displayed at the top of the Dashboard, as shown in Figure 6-2.

Table 6-1: AP Group Attribution Parameters Specification

Parameter	Specification
Group ID	Define a unique AP Group
Group Name	Name of the group
Location	Specify where you will deploy this group of APs. Provide specific name to identify the group location.
Group Management IP	It is a virtual IP address and will be dynamically assigned to the PVC. It is used for the group management and can be configured manually.
Group Management Netmask	Netmask of Group Management IP.

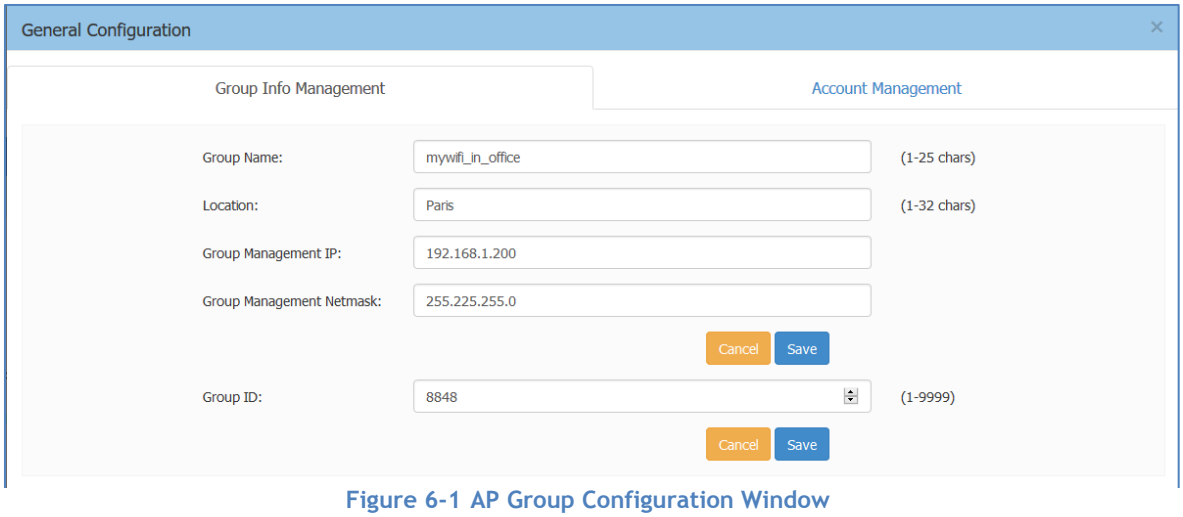

Figure 6-1 AP Group Configuration Window

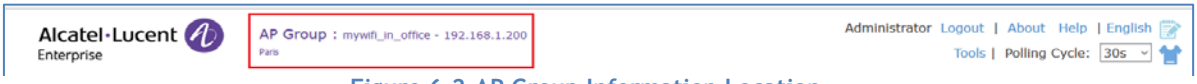

Figure 6-2 AP Group Information Location

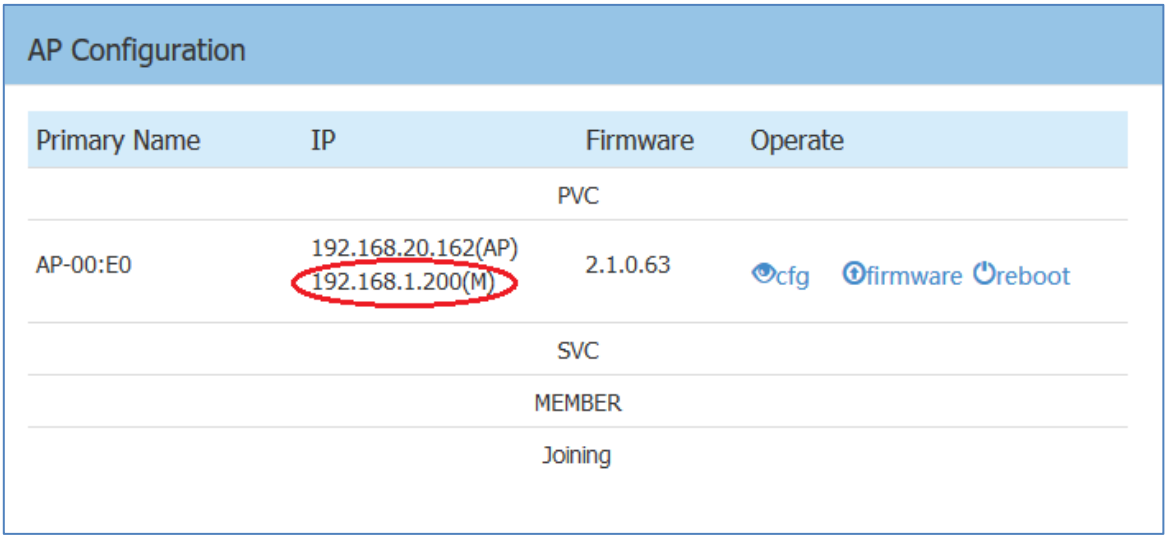

Figure 6-3 AP Group Management IP

There are two IP addresses on the PVC of the group, illustrated in Figure 6-3 (Navigate:**Dashboard** – **AP Window** – **AP Configuration Window**).
1. AP IP address [e.g.: 192.168.20.162(AP)] – The IP of the PVC which used to communicate with other OAW-APs in the group and with network entities outside the group. It can be set manually or assigned from a DHCP server in the network.

2. AP Group Management IP address [e.g.: 192.168.1.200(M)] – The virtual IP for the group management. It can be set by the administrator manually and as a static group management entrance through wired or wireless access.

Import and Export AP Configuration

In the AP Configuration Window (Navigate:**Dashboard** – **AP Window** – **AP Configuration Window**), you can backup, recover or clear the group configuration, illustrated in Figure 6-4 and Figure 6-5.

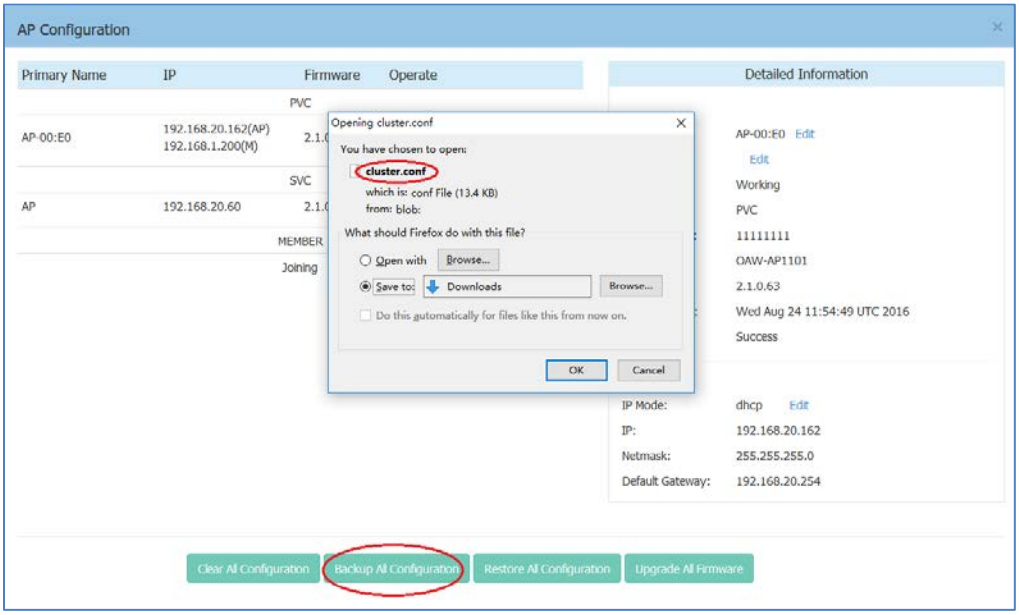

Figure 6-4 Export AP Group Configuration

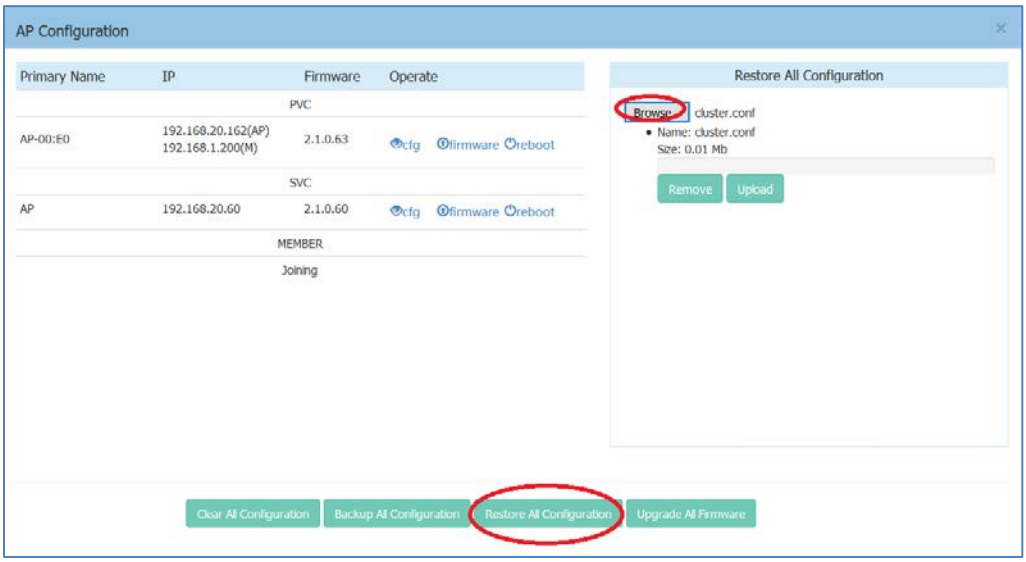

Figure 6-5 Import AP Group Configuration

Table 6-2: AP Group Configuration

Parameter	Specification
Clear All Configuration	Clear all AP configurations, return to factory state.
Backup All Configuration	Download and backup configuration file of AP group, it is recommended to do this when you have completed all configuration.
Restore All Configuration	Upload configuration file to all APs.

Upgrade All Firmware	Upgrade all AP's firmware.

Note

Note6-1: All configuration settings (clear, backup or restore) will be applied to the entire group. There is no need to select specific APs to apply configuration settings. The entire group of APs have one configuration file.

Upgrade AP Firmware

Before upgrading the AP you should prepare the firmware file to be upgraded. You can download the firmware file and save it in the local drive of the machine you are using to connect to the OAW-AP or save the firmware file in a remote TFTP server.

In the AP Configuration Window (Navigate: **Dashboard-AP Window-AP Configuration Window**), there are separate entrances for upgrading a single AP or all the APs in a group:

1. **Upgrade single AP:** Select the AP to be upgraded from the AP list, click firmware to upload firmware, illustrated in Figure 6-6 and Figure 6-7. Generally, it takes approximately five minutes to upgrade the AP firmware.
2. **Upgrade all APs:** Click on Upgrade All Firmware to upload the AP firmware to all APs and upgrade, illustrated in Figure 6-8. APs are upgraded in parallel when Upgrade All Firmware is selected.

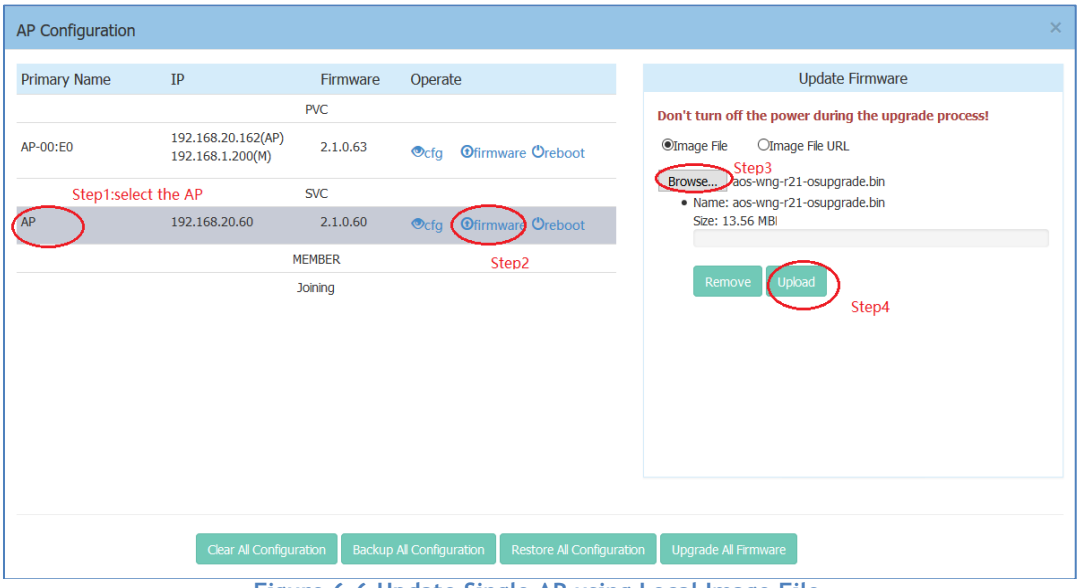

Figure 6-6 Update Single AP using Local Image File

You can also upload the AP firmware from a specified URL as shown in Figure 6-7.

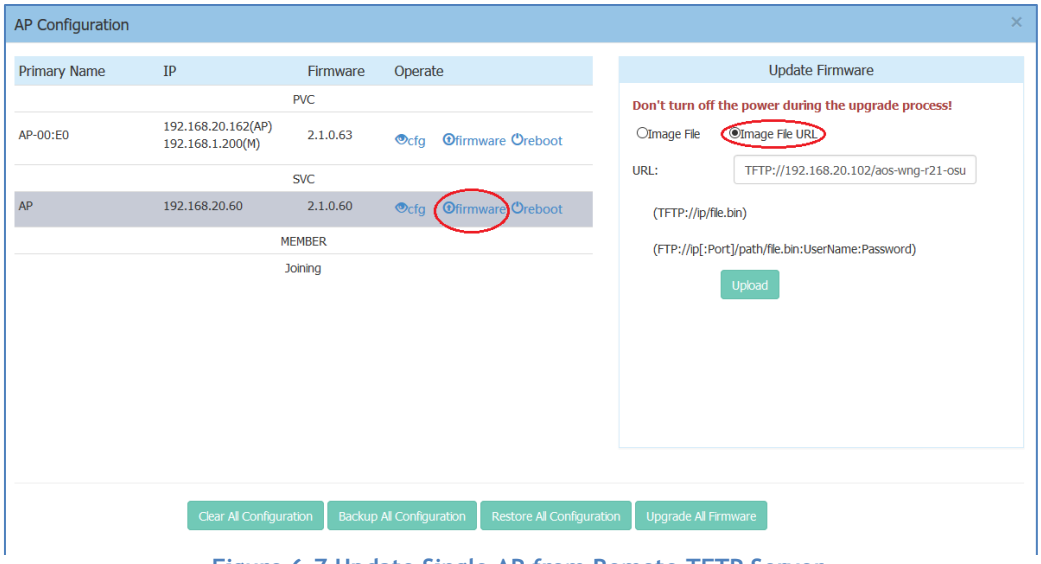

Figure 6-7 Update Single AP from Remote TFTP Server

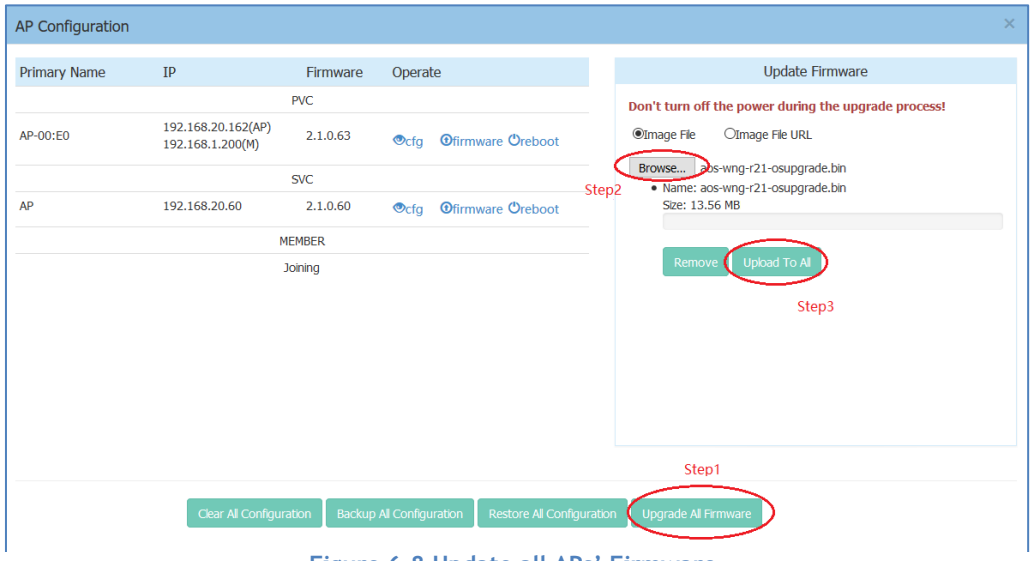

Figure 6-8 Update all APs' Firmware

Warning 6-1:

Don't turn off the power during the upgrade process!

CAUTION

Note 6-2: In order to make sure you're running the latest software, we strongly recommend to clear the browsing data in your browser after the software upgrade, including:

- Cookies
- Cache

Modify AP Name and IP Address

In the AP Configuration Window (Navigate: **Dashboard–AP Window–AP Configuration Window**), you can modify the name and other parameters as needed for the AP in Detailed Information panel.

➔ **Modify AP Name**

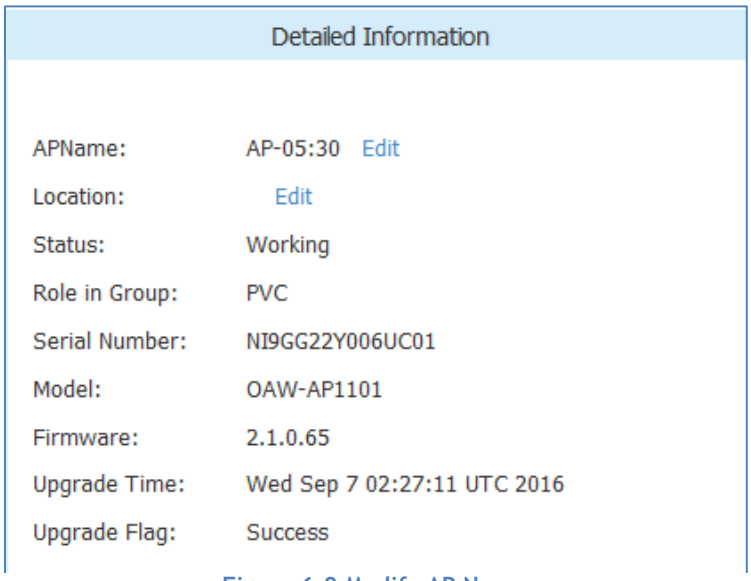

Figure 6-9 Modify AP Name

Click on "**Edit**" to modify the AP name. Enter a name to identify the AP. By default, an OAW-AP is named with the last two bytes of its MAC address (e.g. 05:30 is the last-two-byte MAC address of the OAW-AP in Figure 6-9).

➔ **Modify AP IP Address**

Enter an IP address to modify AP IP address. OAW-AP supports both static and dynamic IP addresses, illustrated in Figure 6-10.

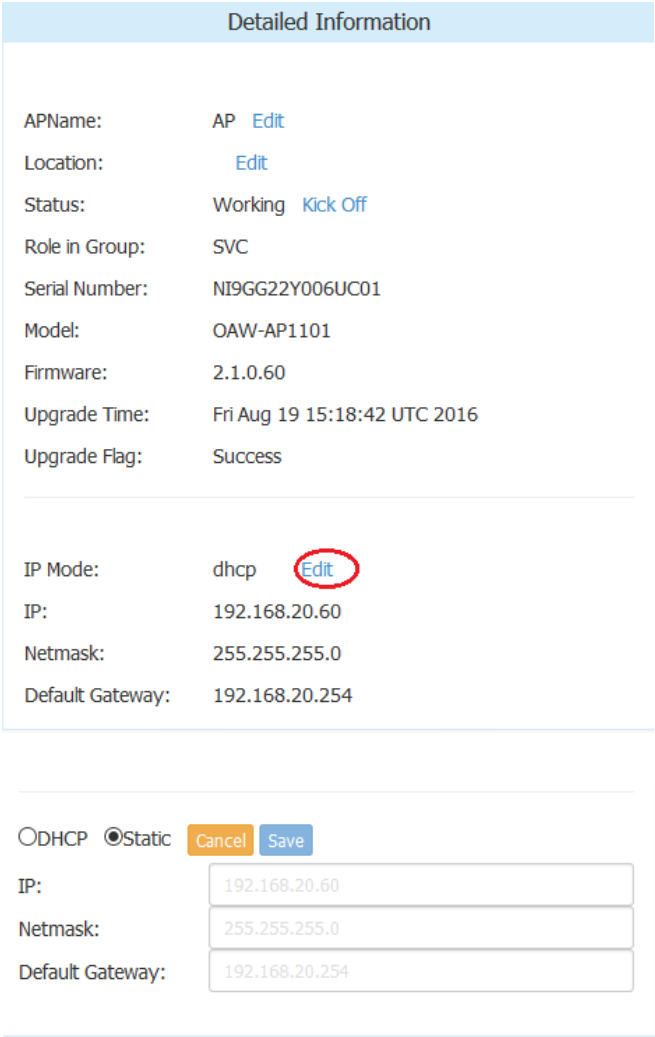

Figure 6-10 Modify AP IP Address

Check AP Configuration Detail

Click cfg to verify AP configuration in the AP Configuration Window (Navigate: **Dashboard-AP Window-AP Configuration Window**).

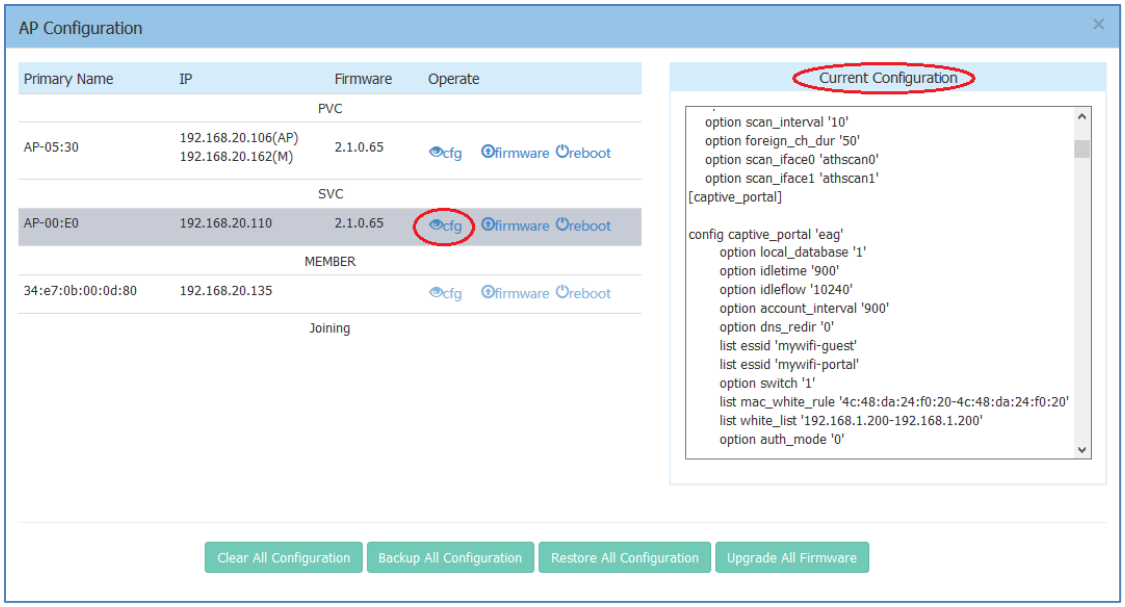

Figure 6-11 Check AP Configuration Detail

Modify AP Transmission Power and Channel

You can modify the transmission power and working channel for the OAW-AP in the RF Configuration Window. (Navigate: **Dashboard-Wireless Page-RF Window-RF Configuration Window**)

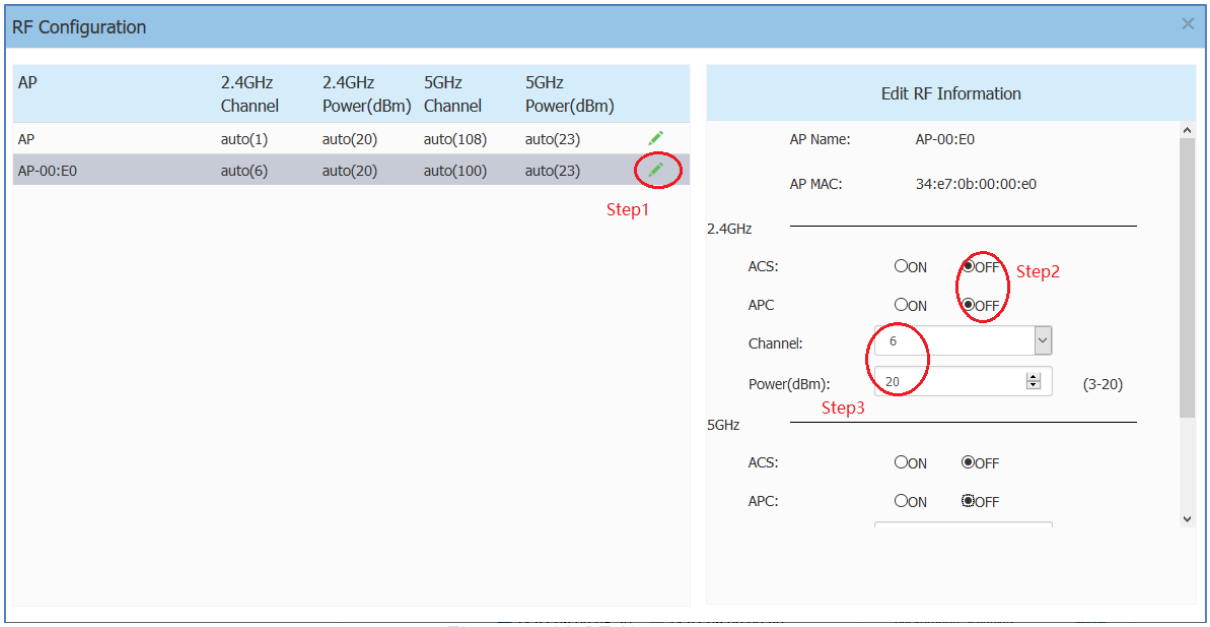

Figure 6-12 RF Management

Automatic Channel Selection (ACS) and Automatic Power Control (APC) are turned ON by default. The AP transmission power and channel are adjusted dynamically by default. If you disable ACS and APC the channel used by the AP and the transmit power must be set manually. In manual mode the AP transmit power can be adjusted in 1 dB increments. These values must be set for both radio bands.

AP LED Specification

Table 6-3: Describes the LED status during different stages of OAW-AP.

Red	Blue	Green	Time Line	Status
ON			Power on	Power on
ON			Bootloader-OS loading	System start up
Flash			System running	Network abnormal (Interface down)
		Flash	System running	Network normal, without SSID created
		ON	System running	Network normal, single band working, ether 2.4Ghz or 5Ghz working
	ON		System running	Network normal, dual bands working, 2.4Ghz and 5Ghz are both working
Flash	Flash		System running	Red and Blue LED rotate flash in a specific frequency; OS upgrading
Flash	Flash	Flash	System running	3 LED rotate flash in a specific frequency; Used for location an AP

Locate AP or Turn LED Off

Step1: Click in **AP Window** of Dashboard to launch 'LED-Off/Locate' buttons.
Step2: Click 'LED-Off' to turn off the LED light.

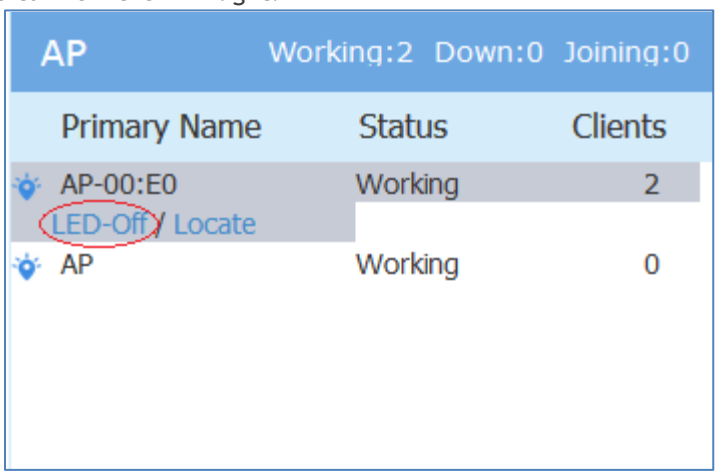

Figure 6-13 Turn LED off

Step3: Click "Locate" to locate AP.

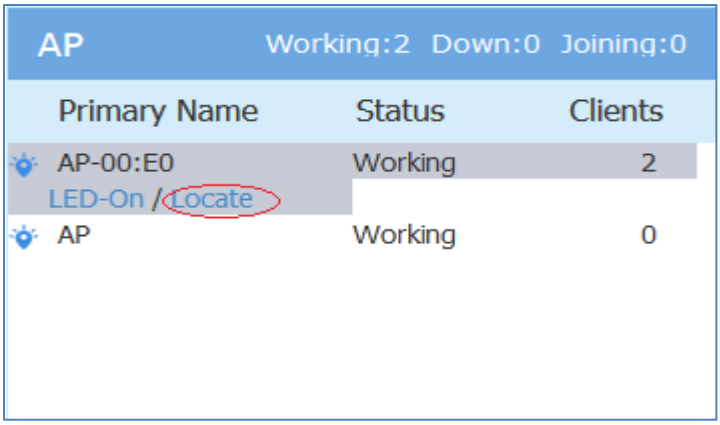

Figure 6-14 Locate AP

The Restore window appears. The LED blinks with red, blue and green color.

Step 4: Click "Restore" to return to the normal state.

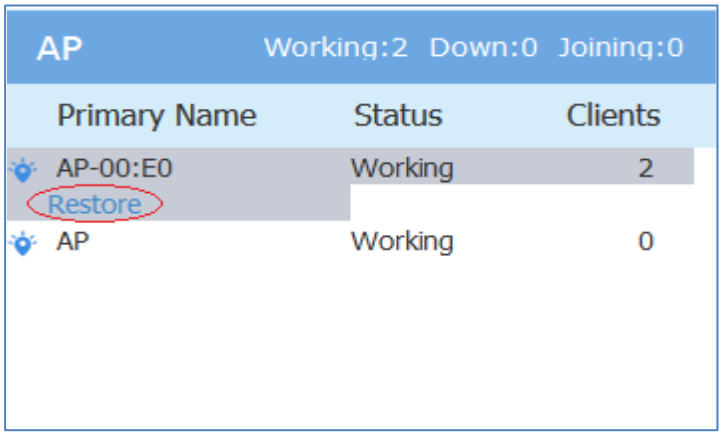

Figure 6-15 Restore AP state

Remove an AP from the Group

An AP is removed from the AP group list (PVC/SVC/Member) by selecting “kick off”. Then the AP enters a group blacklist, if it is not disconnected from the network it will move to the ‘**Joining**’ state, and without authorization is not permitted to be a member of group again.
See in Figure 6-16 and Figure 6-17.

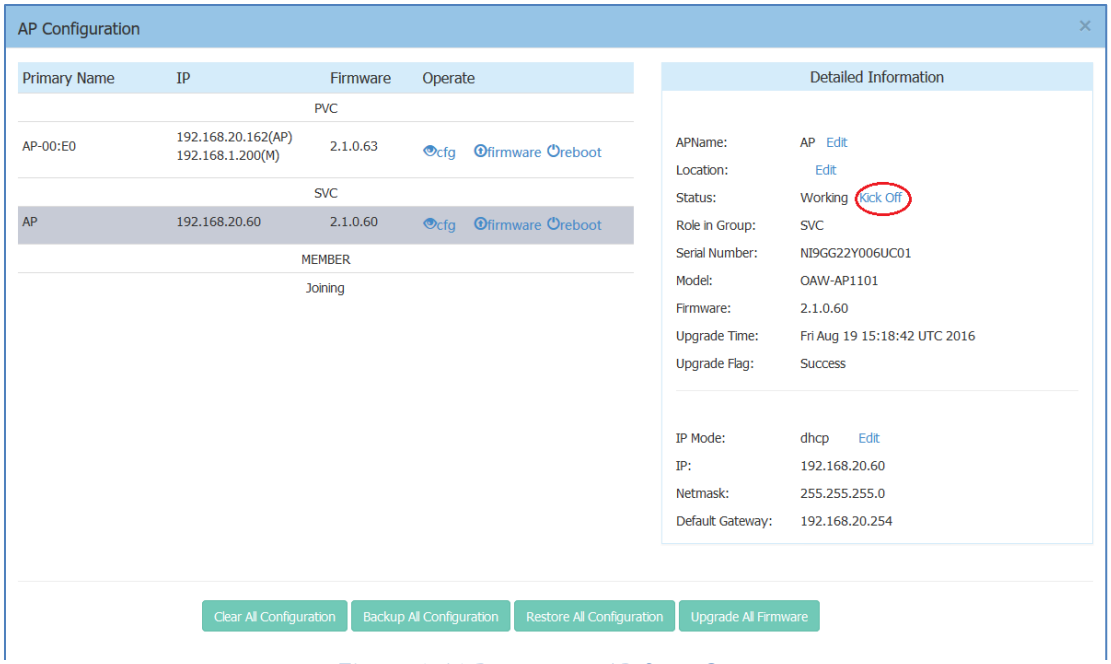

Figure 6-16 Remove an AP from Group

Allow an AP to Join the Group

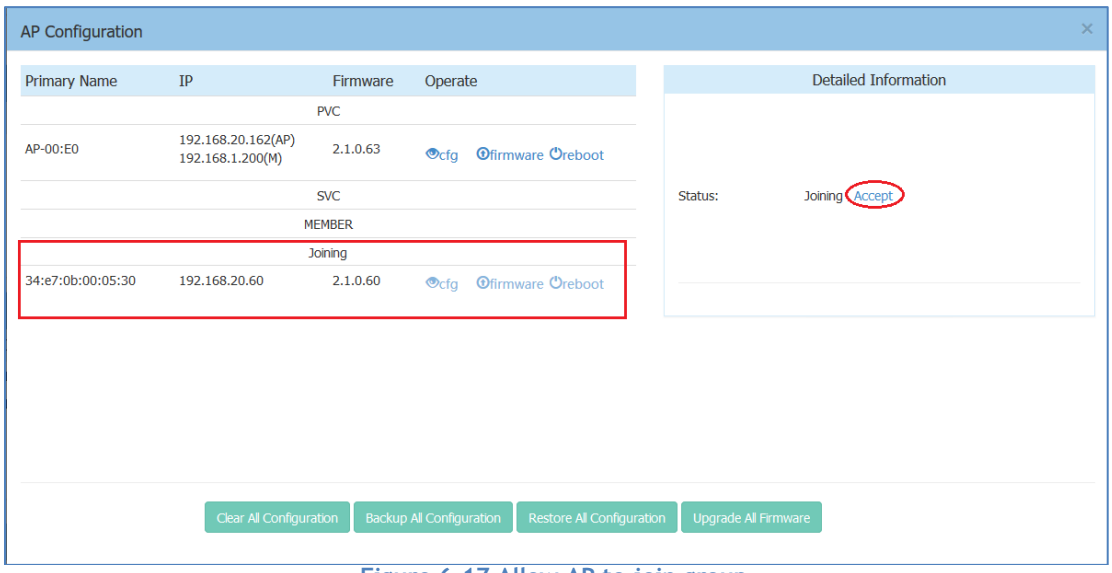

Figure 6-17 Allow AP to join group

In the displayed AP Configuration screen, an AP in 'Joining' state is in the group blacklist, the 'Accept' operation lets it join the group and removes it from the group blacklist.

How to Add a New AP to Group

To add a new AP to the group, ensure that the PVC is not in the 'Down' state. If the PVC is down, upgrade the SVC to be the PVC before plugging in the new AP.

How to Replace a Current AP in Group

1. **To replace the current PVC**: Upgrade the SVC to the PVC before disconnecting the old PVC. Then replace the old PVC with a new OAW-AP.
2. **To replace the SVC or a MEMBER of the group**: Disconnect and replace the SVC or member directly with a new OAW-AP, users on other OAW-APs will not be affected.

How to Setup Wireless Networks With More Than 16 APs

If you have more than 16 OAW-APs, you can setup more than one AP group to provide Wi-Fi service.

There are two methods to setup more than one AP group in the network:
Method one: Divide the OAW-APs into different subnets by changing the default VLAN of the switch ports to which the OAW-APs connect; for example: subnet-A uses default VLAN 100 while subnet-B uses default VLAN 200.
Method two: Setup up different group IDs for each AP group respectively. Perform the following steps:

1. Select the APs which you want to work in Group-A, plug in to the switch to build the first AP group;
2. Browse to the Group-A management interface and change its group ID. (For example: change the group ID from 100 to 8818), see in General Window.
3. Repeat the above process to setup Group B/C/etc.

Note

Note 6-3: Each group is managed independently and roaming between groups is not supported.

How to Configure the AP if There is No DHCP server

Case one: If the APs reboot and the DHCP server is not accessible, all the APs return to the system default IP -192.168.1.254. This means there are duplicate IPs in the broadcast domain. All the APs work separately as the PVC and broadcast the same WLANs. In this case, it is highly recommended to fix the DHCP sever in the network and let the wireless service recover.

Case two: If you want to configure a single OAW-AP without a DHCP server, perform the following steps:

1. Connect the OAW-AP (default IP address is 192.168.1.254) to your configing terminal (laptop for example) directly with an Ethernet cable.
2. Specify a static IP address and a DNS sever for the network card of your laptop, for example: IP Address - 192.168.1.100; Subnet Mask – 255.255.255.0; Default Gateway - 192.168.1.254; DNS sever -192.168.1.254.
3. Browse http://mywifi.al-enterprise.com:8080 or http://192.168.1.254:8080 to configure the OAW-AP.

7 Authentication Management

As WLANs evolve from best-effort to mission-critical infrastructure, organizations are finding that the operational aspects of network security take on much greater importance. The ALE Wi-Fi solution supports enhanced security methods to assure your wireless connection is more secure to eliminate any type of potential sniffers and other security threats. The major features of the ALE WLAN are:

- **To secure users and network traffic in a WLAN** - ALE provides a full suite of authentication, encryption, and policy enforcement capabilities in an architecture that allows easy integration of additional security services.
- **Wireless Intrusion Prevention System (WIPS)** - To enforce no-wireless policies or detect attacks against a WLAN, ALE AP provides advanced threat detection and suppressing functions. An AP can scan the wireless environment and detect the potential rogue and restrict it from replying to user connection requests.

AP Security described in this chapter includes:

- Authentication and Encryption Methods
- How to Configure Captive Portal Authentication

Authentication and Encryption Methods

When creating a WLAN, select the security type as illustrated in Figure 7-3.

- **Open**: No Authentication or encryption method for this WLAN. User data will be transmitted as Plain text Transmit Mode.
- **Personal**: There will be several WPA, WPA2, AES and TKIP combinations available once you select Personal. This does not require an external RADIUS server as illustrated in Figure 7-3.
- **Enterprise**: Authentication method will be based on WPA Enterprise Architecture. Encryption method TKIP or AES is selected. An external RADIUS server is required as illustrated in Figure 7-4.

Note

Note 7-1: WPA uses 802.1X authentication which is one of the Extensible Authentication Protocol (EAP) types available today. 802.1X is a port-based network access control method for wired, as well as wireless, networks. It was adopted as a standard by the IEEE in August of 2001. EAP handles the presentation of users' credentials, in the form of digital certificates (already widely used in Internet security), unique usernames and passwords, smart cards, secure IDs, or any other identity credential that the IT administrator is comfortable deploying. WPA allows flexibility in both the type of credentials that are used and in the selection of an EAP type.

TKIP encryption, 802.1X/EAP authentication and PSK technology in WPA are features that have been brought forward from WPA2. Additionally, WPA2 will provide a new, encryption scheme, the Advanced Encryption Standard (AES). WPA2 offers a graceful transition path from WPA that presents a compelling

case for upgrading to WPA now. WPA2 will offer a highly secure “mixed mode” that supports both WPA and WPA2 client workstations. This will allow for an orderly transition in large enterprises that cannot readily upgrade in a short period of time. Unlike the WEP/WPA mixed mode in WPA devices, WPA2’s mixed mode will support both WPA and WPA2. It delivers a high level of security to enterprises as they make the move to the even higher level of security offered in WPA2. Since Wi-Fi Protected Access (WPA) already provides strong encryption, the transition to WPA2 clients and APs can be done gradually, seamlessly, and with a high level of confidence that security will not be compromised.

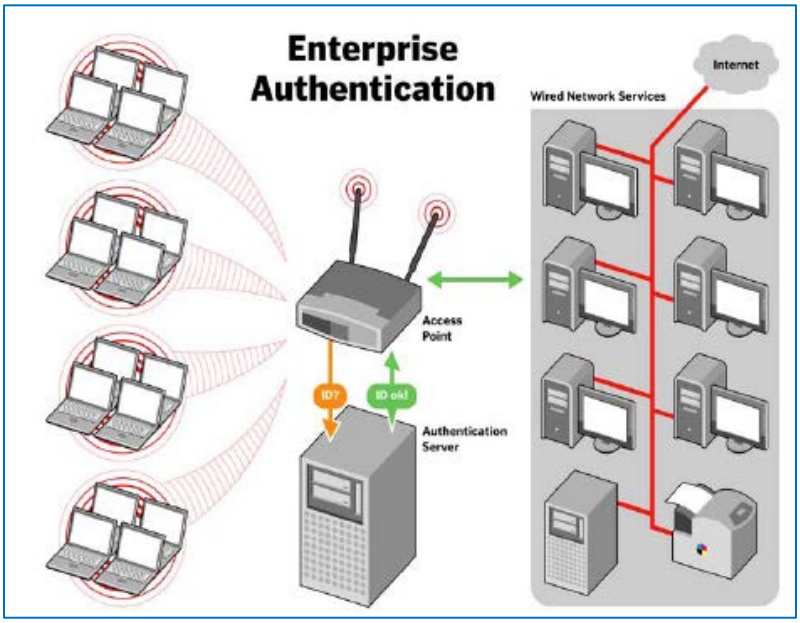

Figure 7-1 Enterprise Authentication

Users in small office and home office (SOHO) environments lack the budget and IT staff to install and maintain RADIUS authentication servers. WPA recognizes this by offering these users the benefits of WPA security through the use of a “pre-shared key” (PSK) or password. The PSK provides home and SOHO users with the same strong TKIP encryption, per packet key construction, and key management that WPA provides in the enterprise. The difference is that here, a password is manually entered on client devices and on the AP or wireless gateway and used for authentication. While not as robust as a full-blown RADIUS, EAP and 802.1X authentication approach, the PSK provides a useful alternative for smaller networks. Upgrading to Wi-Fi Protected Access in home and small office environments is simple. Users can purchase new WPA-enabled equipment or update installed equipment. For most users, the update is as easy as installing a new hardware driver.

Figure 7-2 SOHO Authentication

One of WEP's chief weaknesses was that it used a small static key to initiate encryption. This 40-bit key is entered manually on the AP and on all clients that communicate with the AP. It does not change unless it is manually re-entered on all devices, a daunting labor-intensive task in a large organization. Cryptographic studies have demonstrated that an intruder who collects enough data can threaten a WEP network in three ways: by intercepting and decrypting the data that is being transmitted over the air, by altering the data that is communicated, and by deducing and forging the WEP key to gain unauthorized access to network and Internet services. This could be accomplished in a matter of hours on a busy, corporate WLAN.

Also, WEP lacks a means of authentication, validating user credentials to ensure that only those who should be on the network are allowed to access it. WPA addresses these flaws and brings additional safeguards to Wi-Fi security. WPA uses a greatly enhanced encryption scheme, Temporal Key Integrity Protocol (TKIP). Together with 802.1X/EAP authentication, TKIP employs a key hierarchy that greatly enhances protection. It also adds a Message Integrity Check (MIC, sometimes called "Michael") to protect against packet forgeries.

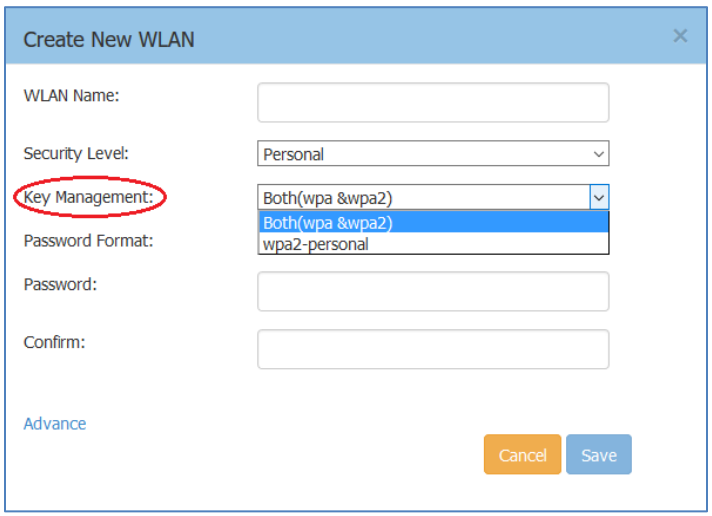

Figure 7-3 Authentication Security Type-Personal

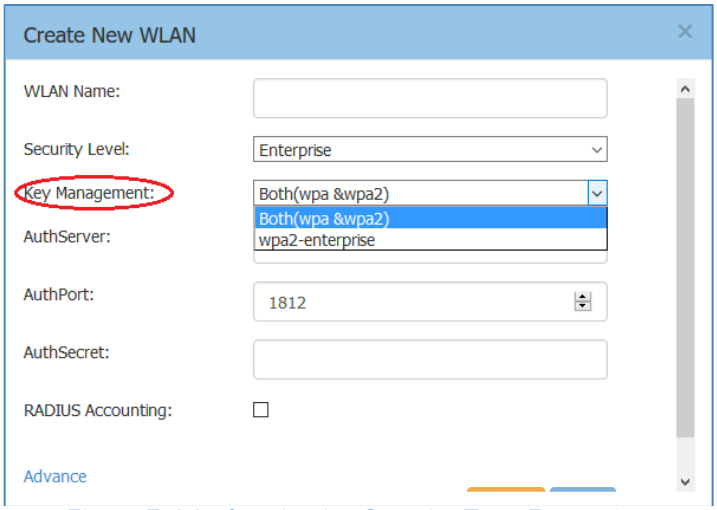

Figure 7-4 Authentication Security Type-Enterprise

How to Configure Captive Portal Authentication

Create a Captive Portal WLAN

Navigate: Dashboard-WLAN window->'New' button.

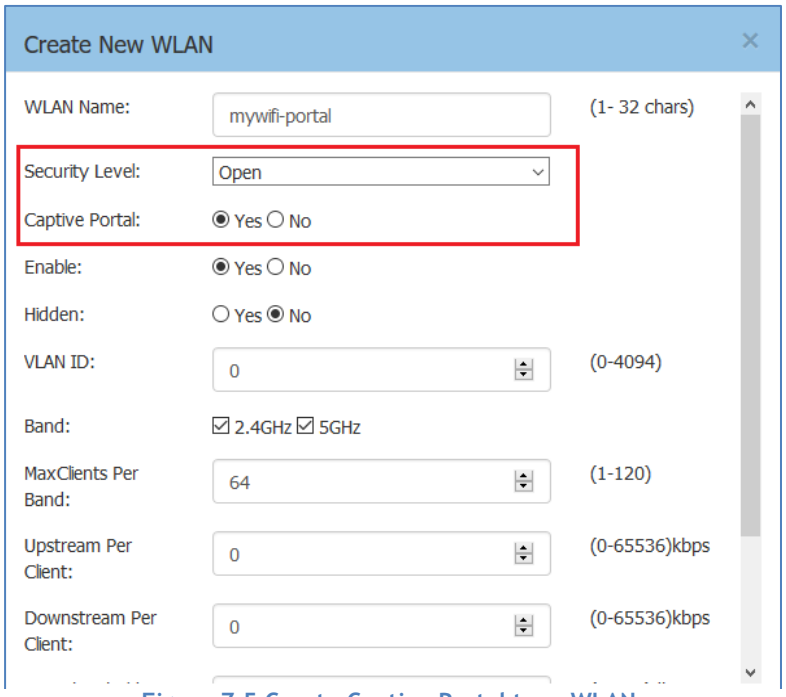

Figure 7-5 Create Captive Portal type WLAN

If you have created the captive portal WLAN, proceed to: Enable Captive Portal Service.

Enable Captive Portal Service

Navigate: Dashboard-Access Page-Authentication Window-Authentication Configuration Window.

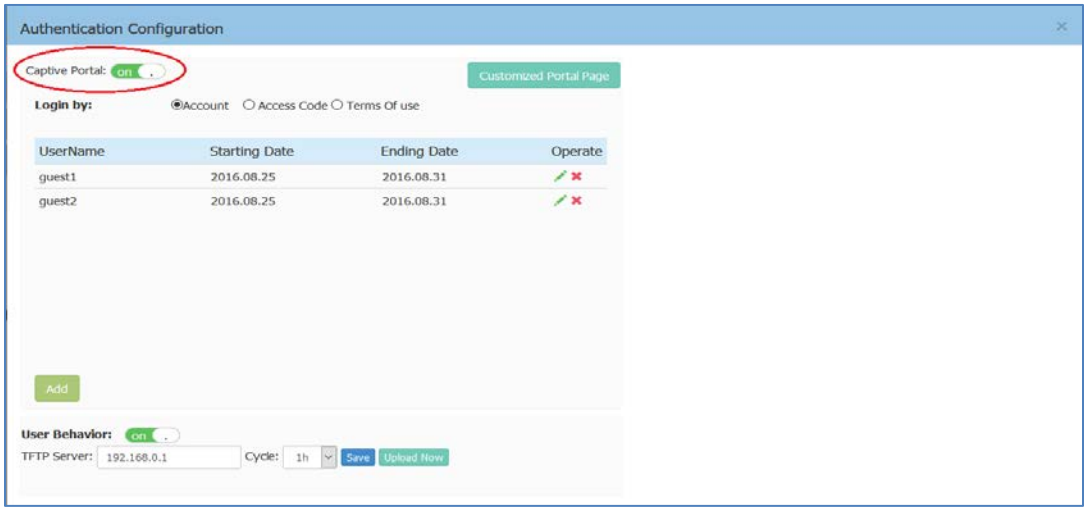

Figure 7-6 Enable Captive Portal Service

After you have enabled the captive portal service, proceed to: Select Your Login Method.

Select Your Login Method

Navigate: Dashboard-Access Page-Authentication Window-Authentication Configuration Window.

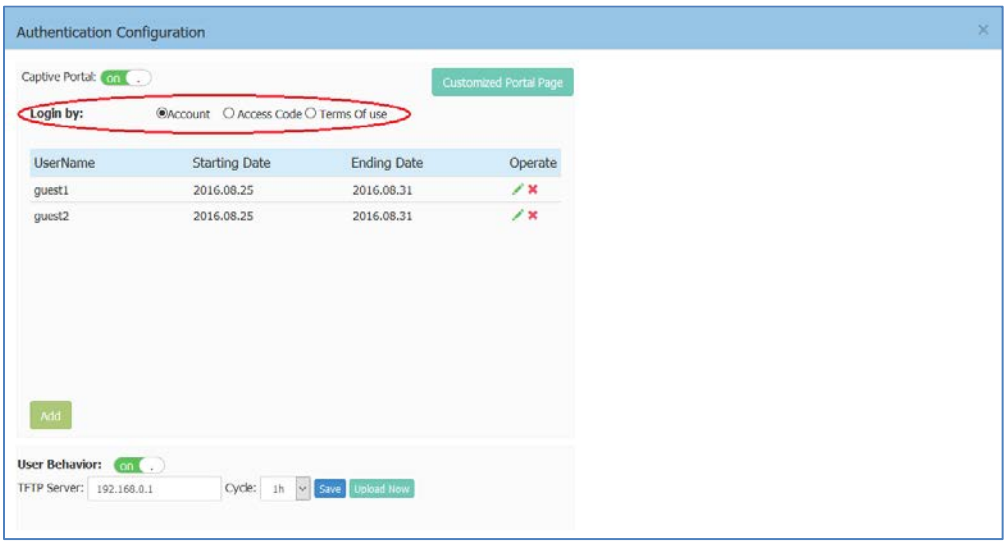

Figure 7-7 Select Your Login Method

After you have selected the login method, proceed to: Create Users or Access Code.

Create Users or Access Code

Navigate: Dashboard-Access Page-Authentication Window-Authentication Configuration Window.

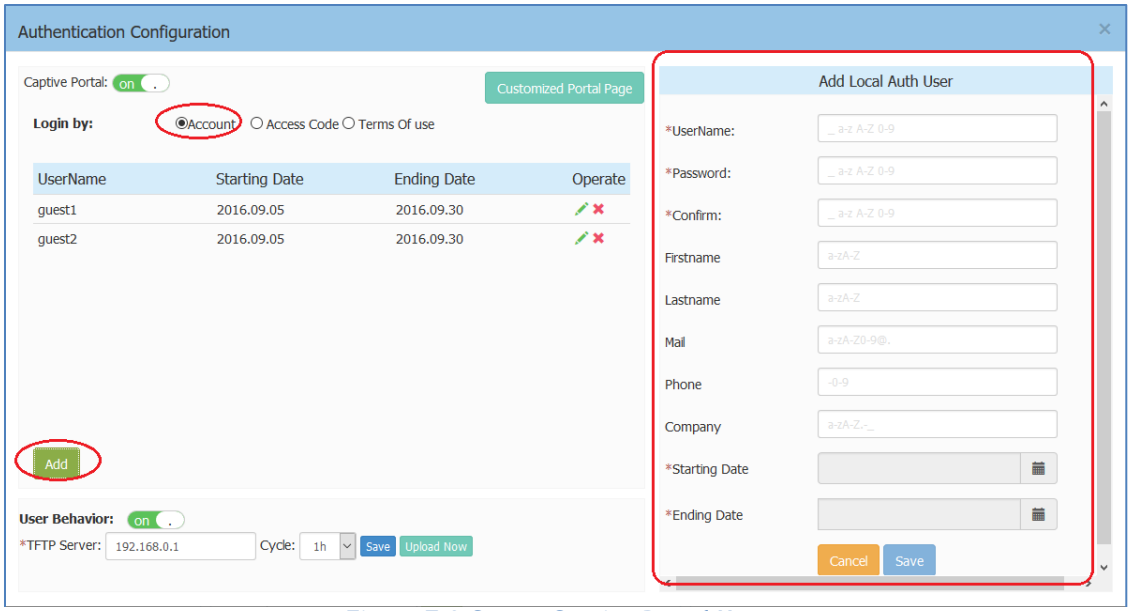

Figure 7-8 Create Captive Portal Users

Note

Note 7-2: If you have selected login by account method for the captive portal authentication, it ONLY supports users in the local user database. It does not support connecting to an external authentication server. You can add user accounts to the local user database, see in Figure 7-8.

Note 7-3: Single user account can be used by multiple devices simultaneously, there are no limits to the number of devices a captive portal user account can connect to the network.

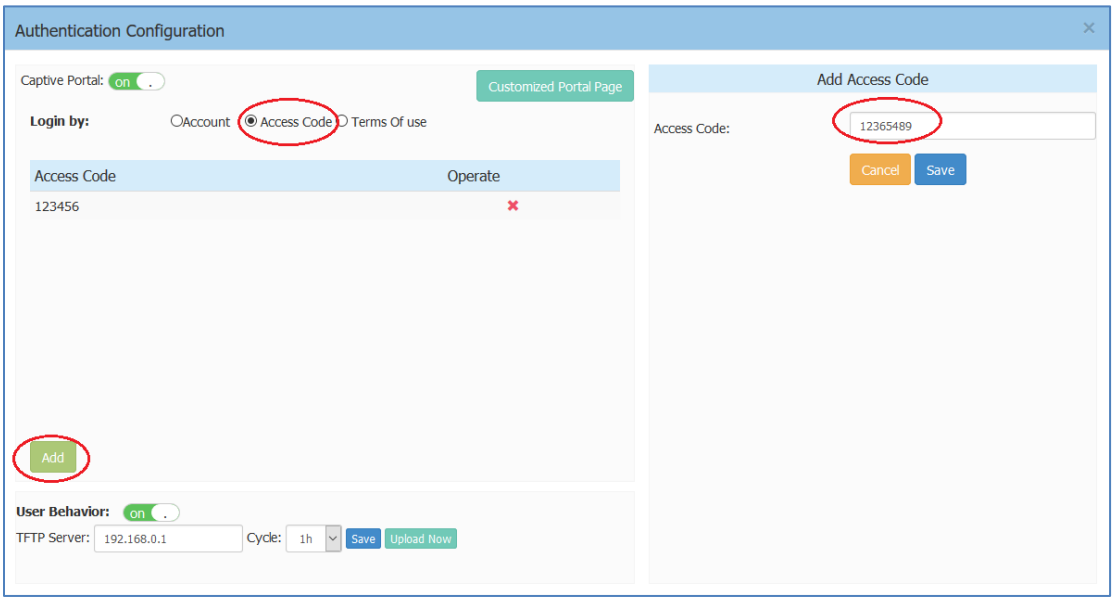

Figure 7-9 Create Access Code

Customize Your Splash Page (Optional)

Navigate: Dashboard-Access Page-Authentication Window-Authentication Configuration Window-Customized Portal Page Panel.

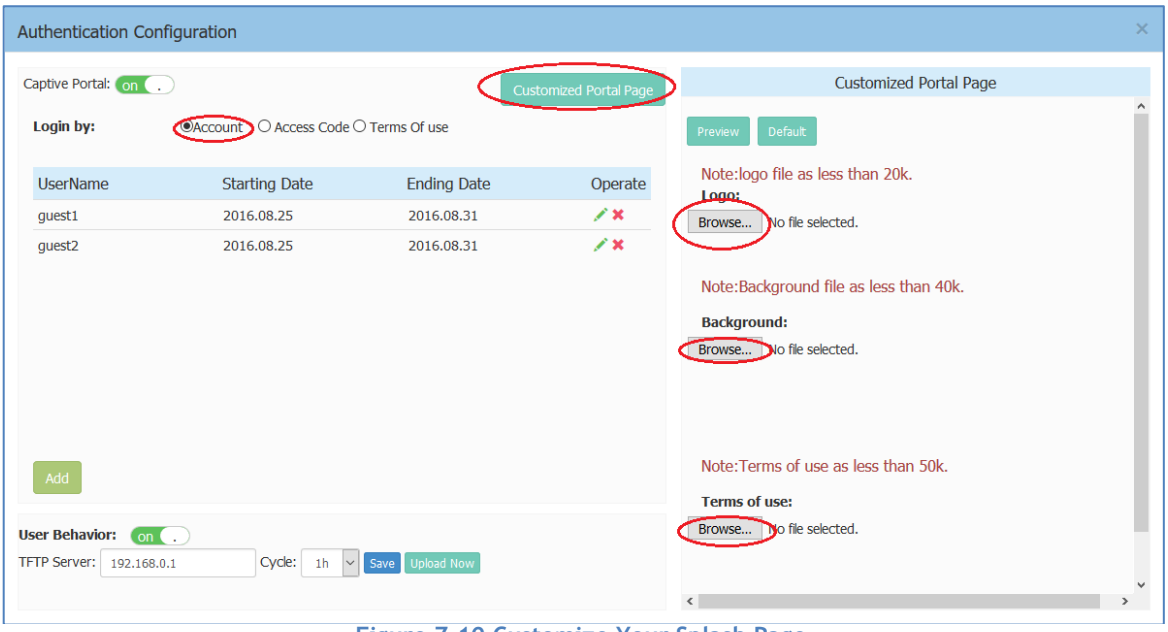

Figure 7-10 Customize Your Splash Page

Log User Behavior (Optional)

Navigate: Dashboard-Access Page-Authentication Window-Authentication Configuration Window

The user behaviors including online and offline are logged and sent to the specified TFTP server. The detailed information of the user behavior can refer to: Authentication Configuration Window.

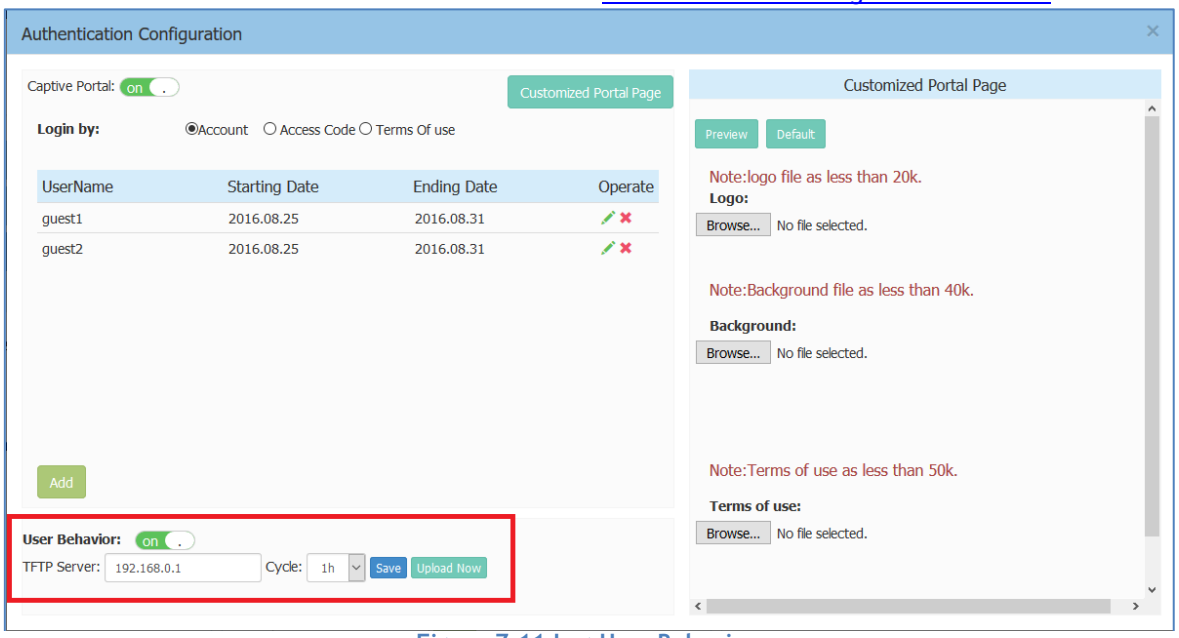

Figure 7-11 Log User Behavior

Specify Your Walled Garden (Optional)

Navigate: Dashboard-Access Page-Black List & Whitelist Window-Walled Garden Tab.

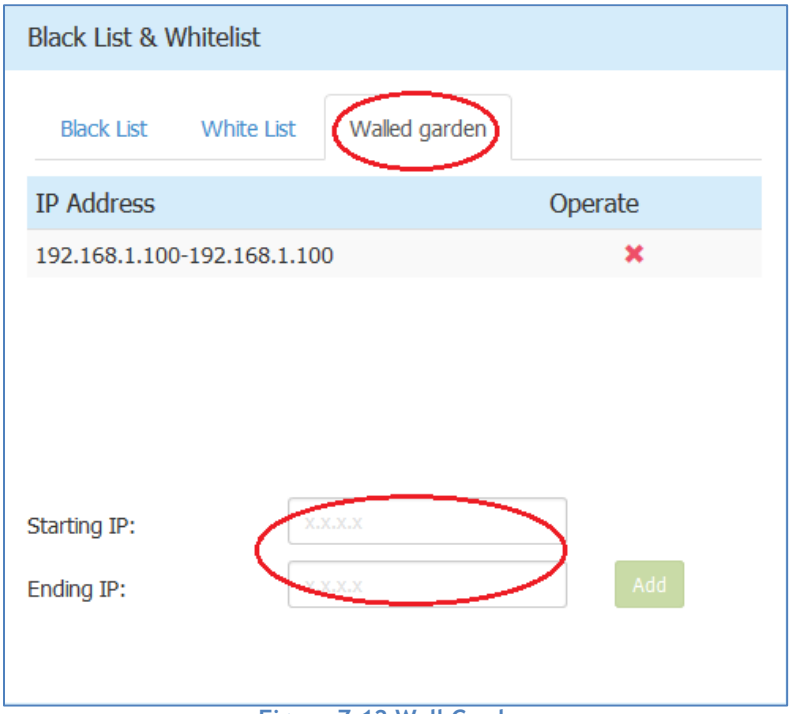

Figure 7-12 Wall Garden

Specify Your Captive Portal Whitelist (Optional)

Navigate: Dashboard-Access Page-Black List & Whitelist Window-White List Tab.

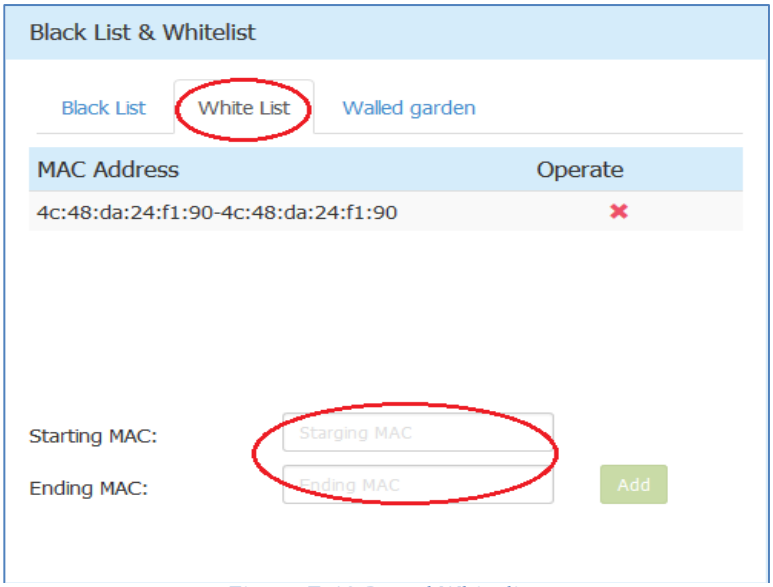

Figure 7-13 Portal Whitelist

8 Tools

Tools are several commands provided for diagnosing and troubleshooting. The commands are applied to a single AP in the group. You can select an AP from the group and execute a command to discover the running information of the AP, such as system health, wireless health and reboot reason. Illustrated in Figure 8-1 and Figure 8-2.

Figure 8-1 Tools in Dashboard

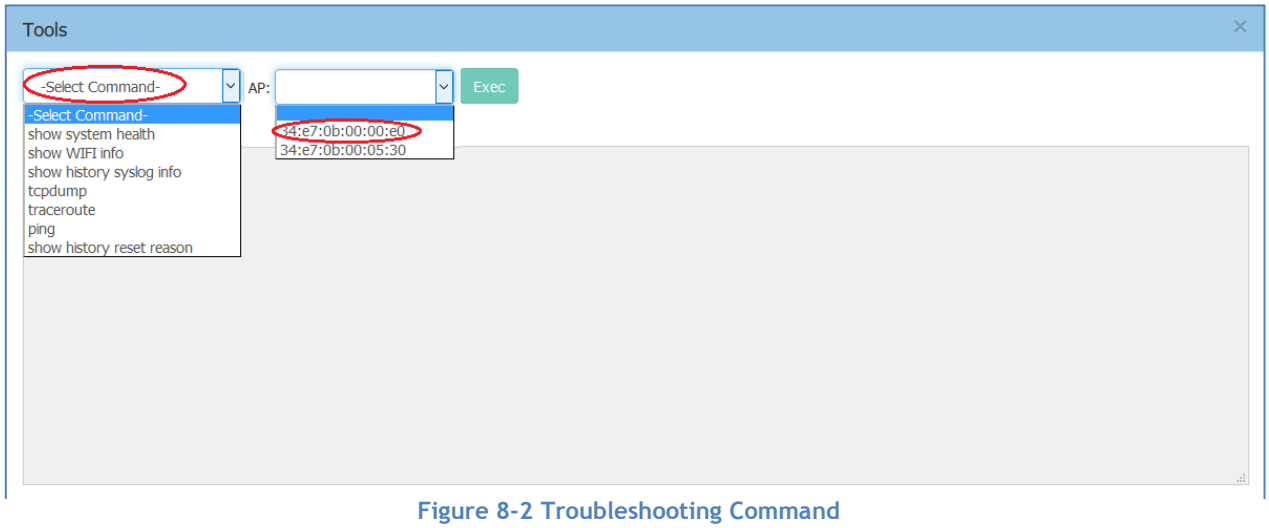

Figure 8-2 Troubleshooting Command

Table8-1 describes the commands for troubleshooting.

Command	purpose
Show system heath	Show system CPU and memory usage information of specified AP
Show WIFI Info	Show wireless interface information of specified AP

Show history Syslog info	Show historic Syslog messages generated in last time system running (Before this time system up) of specified AP
traceroute	Traceroute from specified AP to another host in the network
Ping	Ping operation from specified AP to another host in the network
Show history reset reason	Show historic reboot reason of specified AP

Reset the AP to Factory Default Settings

Press and hold the reset button for approximately 5 seconds then release. The LED will turn off and then turn red as the AP reboots to the factory default settings.

A. End-User Software License Agreement

ALCATEL-LUCENT ENTERPRISE USA, INC. ("ALU E")
SOFTWARE LICENSE AGREEMENT

IMPORTANT

Please read the terms and conditions of this license agreement carefully before installing or downloading this software. The installation and use of the software is subject to these terms and conditions (Agreement).
In this Agreement:

"Licensee" or You, Your and Yourself, means: the legal person or entity that by its authorized agents or representatives installs and/or uses, the Software.

"Software" (as defined in Section 1 below) for its own use and not for resale or distribution.

"Licensor" means Alcatel-Lucent Enterprise USA, Inc. or one of its Affiliated Companies or authorized distributors entitled to distribute the Software.

"Affiliated Companies" means any entity Controlling, Controlled by or under common Control, directly or indirectly, with Alcatel-Lucent Enterprise USA, Inc., "Control" means the ability to determine the management policies of a company or other entity through ownership of a majority of shares, by control of the board of management, by agreement or otherwise

Provided that You accept the terms and conditions of this Software License Agreement (the "Agreement") in accordance with the following paragraph and pay all applicable "License Fees", the Software shall be licensed subject to, and the use of the Software shall be governed by, this Agreement, except to the extent that a separate valid license agreement has been previously entered into between Licensee and Licensor that sets forth the terms and conditions for the use and license of the Software for the number of users for which, and on the platform on which Licensee is installing it, on terms and conditions equivalent to this Agreement ("Separate Agreement").
Notwithstanding anything to the contrary herein, if Licensee has entered into a Separate Agreement, the Software is licensed subject to the terms and conditions of the Separate Agreement and the provisions of the Separate Agreement shall supersede and replace any and all conflicting terms and conditions of this Agreement, even if Licensee clicks the accept button below. In such case, for the avoidance of doubt, the Separate Agreement and this Agreement shall not be deemed two concurrent agreements, and only the Separate Agreement shall be deemed entered into between Licensee and ALU E with respect to the Software.

IN THE EVENT WHERE NO SEPARATE AGREEMENT IS CURRENTLY IN FORCE, BY CLICKING THE ACCEPT BUTTON OR INSTALLING OR USING THE SOFTWARE, LICENSEE IS CONSENTING TO BE BOUND BY THE PROVISIONS OF THIS AGREEMENT AND IS BECOMING A PARTY TO THIS AGREEMENT. IF LICENSEE DOES NOT AGREE TO THE TERMS OF THIS AGREEMENT, CLICK THE BOX ADJACENT TO THE STATEMENT "I DO NOT ACCEPT THE LICENSE AGREEMENT" AND PROMPTLY DELETE ANY FILE CONTAINING THE SOFTWARE AND RETURN THE UNUSED SOFTWARE TO THE PARTY FROM WHOM YOU OBTAINED THE SOFTWARE. IF YOU HAVE ANY QUESTIONS ABOUT ANY PART OF THIS AGREEMENT PLEASE CONTACT YOUR ALE REPRESENTATIVE. LICENSEE IS ENCOURAGED TO SEEK LEGAL REVIEW OF THIS AGREEMENT PRIOR TO ACCEPTING IT.

1. License Grant and Restrictions of Use. This is a license, not a sales agreement, between the Licensee and ALU. Subject to Licensee paying all applicable fees, and subject to the terms set forth in this License Agreement ("Agreement"), ALU E or any of its Affiliated Companies, or, its local authorized Reseller or its authorized distributors from whom you purchased a license to use the software ("Licensor"), grants you this non- exclusive, non-transferable license to use the software program(s) delivered with this Agreement in

machine-readable form (the "Software"), and any documentation delivered with the Software (the "Documentation"). You shall not, and you shall not authorize other persons or entities to: (i) directly or indirectly, by electronic or other means, reproduce (except one copy for archival purposes), publish, distribute, rent, lease, sell, sublicense, assign or otherwise transfer the Software and Documentation or any part thereof or this Agreement; (ii) reverse-engineer, decompile, disassemble, merge, modify, use for competitive analysis, create derivative works of, or translate the Software or use any part of the Software outside the scope of the intended use of the Software; (iii) use the Software and Documentation for any purpose other than internal business purposes and not permit sublicensing, time sharing, rental, facility management, service bureau or application development use of the Software nor permit publication or distribution of results of any benchmark tests run on the Software without the express written permission of Licensor, or (iv) remove or obscure any copyright, trademark or other proprietary notices or legends from any portion of the Software, the Documentation or any associated documentation.

This license solely enables you to install the Software on one or more server computers and to use the Software on that concurrent number and type of server computers for which you have paid Licensor the applicable license fees. The Software is considered to be in use when it resides in memory or is otherwise stored on a machine. The Software might not be usable by you until you have obtained a license key that enables the Software. By obtaining a license key for the Software, you ratify your assent to this Agreement. You agree to ensure that anyone who uses the Software or Documentation does so only for your authorized use and complies with the terms of this Agreement. You may not use the Software to provide time-sharing, service bureau or other similar types of services to third parties.

If you use the Software within a country in the European Union, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. You agree to notify Licensor of any such intended examination of the Software and may procure support and assistance from Licensor

2. Confidentiality. Licensor considers the Software to contain valuable trade secrets of ALU E, or it’s licensors, the unauthorized disclosure of which could cause irreparable harm to ALU E or it’s licensors. Except as expressly set forth herein, Licensee agrees to use reasonable efforts not to disclose the Software to any third party and not to use the Software other than for the purpose authorized by this License Agreement. This confidentiality obligation shall continue after any termination of this License Agreement.

3. Indemnity. Licensee agrees to indemnify, defend and hold Licensor harmless from any claim, lawsuit, legal proceeding, settlement or judgment (including without limitation Licensor's reasonable United States and local attorneys' and expert witnesses' fees and costs) arising out of or in connection with the unauthorized copying, marketing, performance or distribution of the Licensed Materials.

4. Limited Warranty. Unless a longer period is mandated by law, Licensor warrants that for a period of 90 days from the date of shipment of the media containing the Software to you, the Software, if operated as instructed, will perform substantially in accordance with the accompanying user documentation. Licensor's obligation under this warranty shall be limited as set forth below. Licensor does not warrant that the Software is totally free from error or omission or that its operation will be uninterrupted. All warranty obligations are void if the Software has been improperly installed or, except as allowed by applicable law, has been modified by a party other than Licensor.

EXCEPT FOR THE WARRANTIES SET FORTH ABOVE, THE LICENSED MATERIALS ARE LICENSED "AS IS" AND LICENSOR AND ITS SUPPLIERS AND/OR AUTHORIZED REPRESENTATIVES DISCLAIM ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING (WITHOUT LIMITATION) ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, THAT SOFTWARE ERRORS (IF ANY) WILL BE CORRECTED, AND THAT THE SOFTWARE WILL OPERATE UNINTERRUPTED OR ERROR FREE. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES SO THE ABOVE EXCLUSIONS MAY NOT APPLY TO LICENSEE. THIS WARRANTY GIVES LICENSEE SPECIFIC LEGAL RIGHTS. LICENSEE MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE.

a. Specific Disclaimer for High Risk Activities: The Software are not designed or intended for use in high-risk activities, including, without limitation, nuclear facilities, aircraft navigation or aircraft communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the Components could lead directly to death, personal injury, or severe physical or environmental damage ("High Risk Activities"). Licensor and its suppliers and/or authorized representatives specifically disclaim any express or implied warranty of fitness for High Risk Activities.

5. Limitation of Liability. Licensor's cumulative liability to Licensee or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this License Agreement shall not exceed the license fee paid to LICENSOR for the Licensed Materials. IN NO EVENT SHALL LICENSOR AND ITS SUPPLIERS AND/OR AUTHORIZED REPRESENTATIVES BE LIABLE FOR ANY INDIRECT, INCIDENTAL, PUNITIVE, CONSEQUENTIAL, SPECIAL, OR EXEMPLARY DAMAGES, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR INTERRUPTION OR COMPUTER FAILURE OR MALFUNCTION OR LOSS OF PROFITS OR REVENUES, GOODWILL, INFORMATION OR DATA, OR ANY OTHER PECUNIARY LOSS, WHATSOEVER, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE), ARISING IN ANY WAY OUT OF THE USE OR MISUSE OF THE LICENSED MATERIALS, OR THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION TO INCIDENTAL OR CONSEQUENTIAL DAMAGES MAY NOT APPLY TO LICENSEE.

6. Taxes and Duties. Licensee will be responsible to pay any sales, use, value added, consumption or goods and services tax, import duties, or any other taxes or charges which may be applicable to this product or license.

7. Export Control. This product is subject to the jurisdiction of the United States. Licensee may not export or re-export the Licensed Materials, without complying with all United States export laws and regulations, including but not limited to (i) obtaining prior authorization from the U.S. Department of Commerce if a validated export license is required, and (ii) obtaining "written assurances" from licensees, if required.

8. Support and Maintenance. Except as may be provided in a separate agreement between Licensor and Licensee, if any, Licensor is under no obligation to maintain or support the copies of the Licensed Materials made and distributed hereunder and Licensor has no obligation to furnish Licensee with any further assistance, documentation or information of any nature or kind.

9. Term. This License Agreement is effective upon Licensee installing or downloading the Software and shall continue until terminated. Licensee may terminate this License Agreement at any time by returning the Licensed Materials and all copies thereof and extracts therefrom to Licensor and certifying to Licensor in writing that all Licensed Materials and all copies thereof and extracts therefrom have been returned or erased by the memory of Licensee's computer or made non-readable. Licensor may terminate this License Agreement upon the breach by Licensee of any term hereof. Upon such termination by Licensor, Licensee agrees to return to Licensor or destroy the Licensed Materials and all copies and portions thereof.

10. Governing Law. This License Agreement shall be construed and governed in accordance with the laws of the State of California and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

11. Severability. Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, this Agreement will remain in effect with the term omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

12. No Waiver. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

13. Notes to United States Government Users. Software and documentation are provided with restricted rights. Use, duplication or disclosure by the government is subject to (i) restrictions set forth in GSA ADP

Schedule Contract with ALU's reseller or distributor.(s), or (ii) restrictions set forth in subparagraph (c) (1) and (2) of 48 CFR 52.227-19, as applicable.

14. Third Party Materials. Licensee is notified that the Software contains or may be accompanied by or packaged with third party software and materials licensed to Licensor by certain Suppliers and/or Authorized Representatives. Some Suppliers and/or Authorized Representatives are third party beneficiaries to this License Agreement with full rights of enforcement. Please refer to the file entitled "Third Party Licenses and Notices" in the user's documentation residing on the media for the Suppliers and/or Authorized Representatives license and notice terms. You agree to accept the license terms, including Warranty terms, of any and all such third party end user license agreements included in the Software or Documentation.

15. The Asset Management feature may be chosen during installation, it collects and stores information such as; the make, model and serial number of Licensee’s devices, the device software version numbers and system uptime information and such other information that would, in Licensors sole discretion, be utilized to improve the customer experience. The information helps us to diagnose potential problems, if any, in the software. We may or may not use the diagnostic information, in our sole discretion, to provide support solutions, including updates, upgrades or services packs, if any are made generally available. We will not use the Asset Management feature to track, collect or upload any data that personally identifies You (such as your name, address, email address) except Customer information provided to us by You. Licensee may opt-out of providing this data during installation of the Software by, as the case may be, checking or un-checking the box adjacent to the Asset Management feature option. If the box next to the Asset Management feature option is not checked the option will not be activated. If You decide to activate the Asset Management feature after full installation, You may do so by following the instructions on the Preference page for Asset Management in You OmniVista 2500 client. Your use of the software constitutes your acknowledgment and agreement to the terms of use.

16. Entire Agreement. This Agreement is the complete and exclusive agreement between the parties with respect to the subject matter hereof, superseding and replacing any and all prior agreements, communications, and understandings (both written and oral) regarding such subject matter. This Agreement may only be modified, or any rights under it waived, by a written document executed by Officers of both parties. Any provisions of either purchase order, invoice, or similar document submitted by Licensee to Licensor, which are in addition to or inconsistent with the terms and conditions of this Agreement will be deemed stricken from such document.

17. Notices. If Licensee has any questions concerning this product or would like to otherwise contact ALU E, please write to:
Alcatel-Lucent Enterprise USA, Inc., 26801 West Agoura Road, Calabasas, CA 91301
ATTN: Sales.