AltaiCare

Quick Start Guide

Version 2.2

Date: Jan. 13, 2016

1. Introduction

1.1. AltaiCare Overview

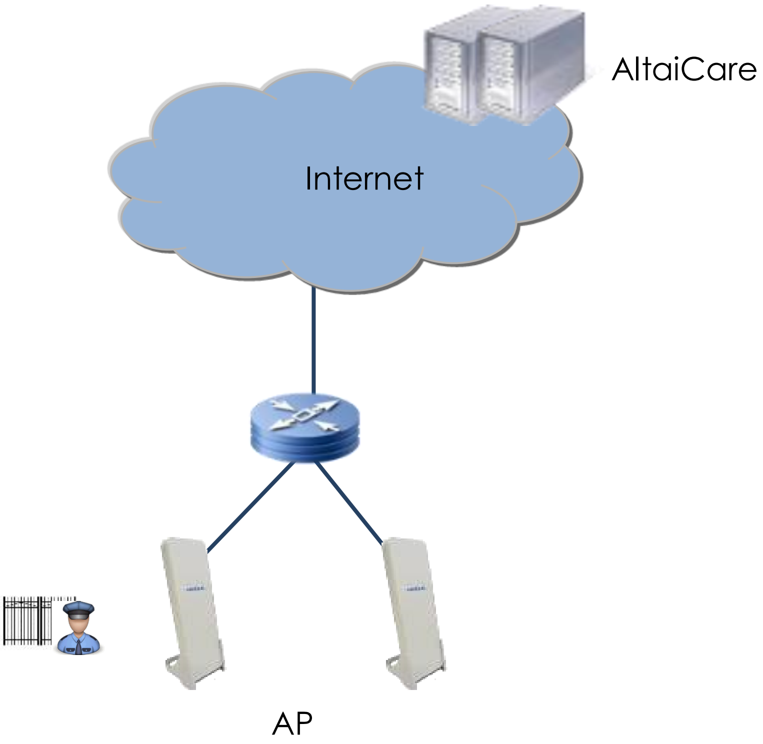
AltaiCare is a cloud-based content, network management, and service control system. The goal is to help customers to deploy their WiFi service as easy as possible, using this All-in-One system.

Feature Highlights:

- Network Management
  - Site-based configuration
  - Zero configuration
  - Interactive performance diagrams
- Service Control
  - Portal/EAP/MAC authentication
  - Customizable local portal
  - Accounting data collection
- Content Management
  - AP based content feeding
  - Altai Beacon based content feeding

1.2. System Overview

The following diagram represents the general setup of AltaiCare system.



As shown in the diagram, AP connects to AltaiCare through Internet. When the AP connects to AltaiCare, it updates its own status, pull configuration and apply the configuration.

When the service control feature is enabled, the AP also serves as a gate keeper in the authentication process (i.e. portal, EAP, MAC authentication).

1.3. AltaiCare Features highlights

Network Map Management

- Indoor Map support

- Outdoor Map support – Google

Fault Management

- Real-time alert list

- Visual fault alert via network map

Configuration Management

- Site based configuration

- Zero configurations

Operation & Administration Management

- Multiple administrator login level (project admin, site admin, site monitor)

- Responsive Web UI, support tablet, and Jumbo screen

Performance Management

- Real time AP and Station Performance Statistics

- Interactive diagrams (AP traffic, Station association, Radio channel usage, Station data rate histogram, RSSI histogram)

- Top usage station and AP list

Service control

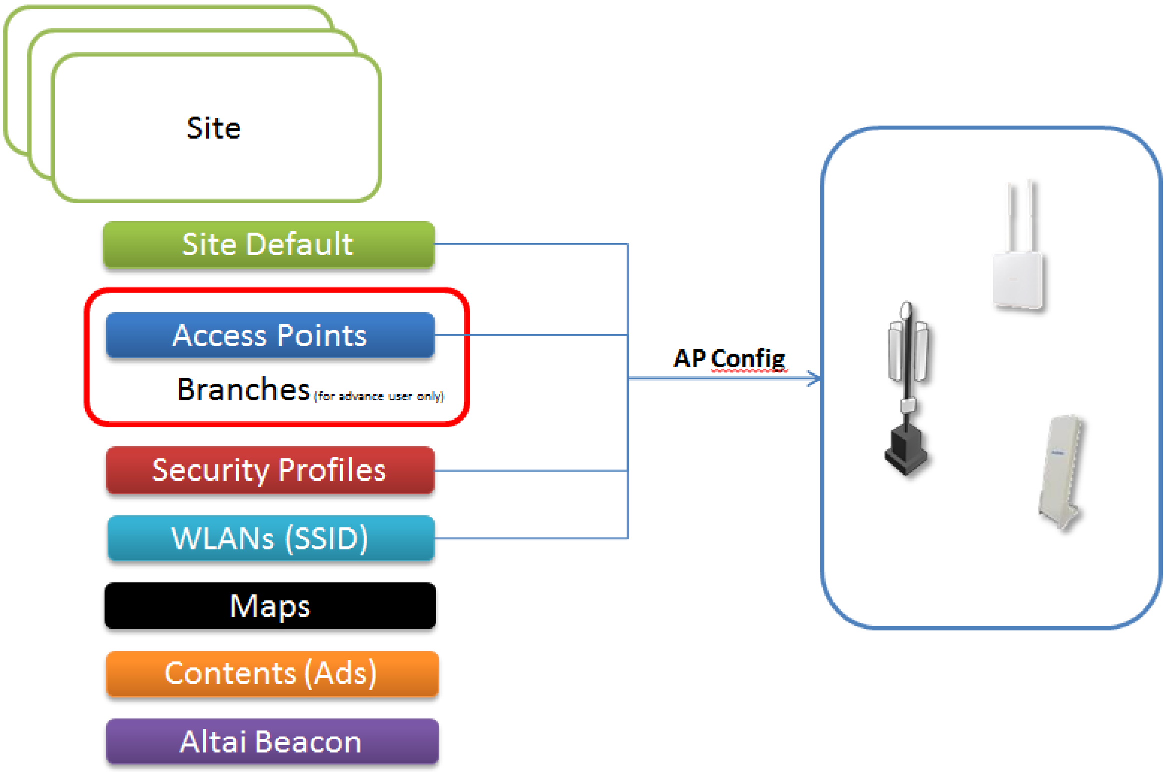
- Portal/EAP Authentication support
- Built-in/External RADIUS Server support
- Built-in/External Accounting support
- Bandwidth Control

2. AltaiCare Management Architecture Overview

2.1. Site-based configuration

Site is the root of AP management in AltaiCare. Each site has its own AP list, WLANs, security profiles, maps…

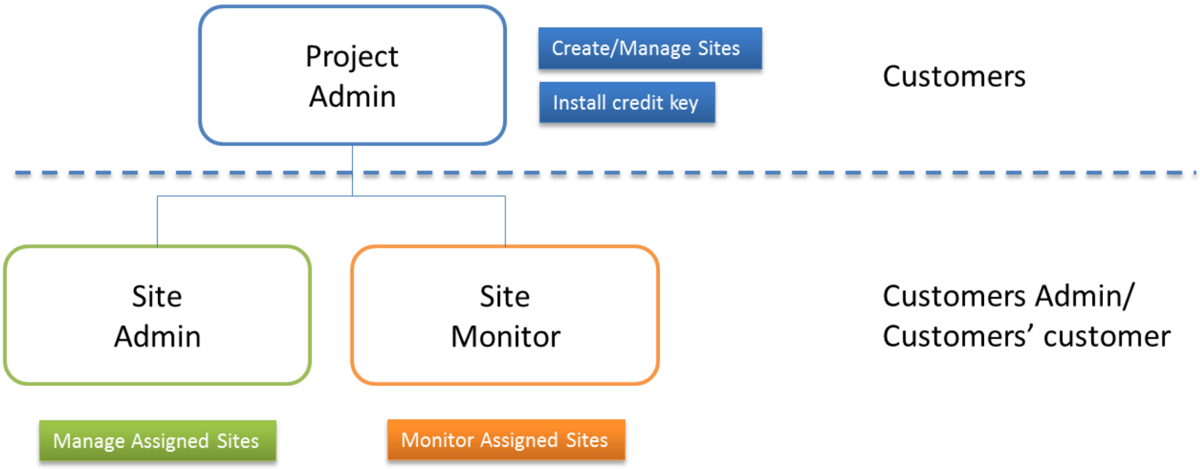
To deploy a new service, administrator needs to create a site for the service location (e.g. a shopping mall, a school). Define security profile and WLAN for that site, and finally register APs into the site. The service will be deployed to the AP automatically.



2.2. Multiple level access control

AltaiCare has three level access control:

- Project admin – Create site, site accounts, manage usage credit
- Site admin – Site administration
- Site monitor – Site monitoring (read only)



Project admin can create sites, and site admin accounts. It also has all access rights to the sites that are under its project.

Site administrator has all access rights of the sites it is being assigned. For example, register AP, create WLAN, security profile etc.

Site monitor can only monitor the site, all operations that will change the network configuration are forbidden.

3. AP Setup Procedure for Working with AltaiCare

3.1. Install firmware that supports AltaiCare

Please download the latest firmware that supports AltaiCare from the following FTP server:

FTP Server:	223.255.161.253
Username:	care
Password:	altaicare123

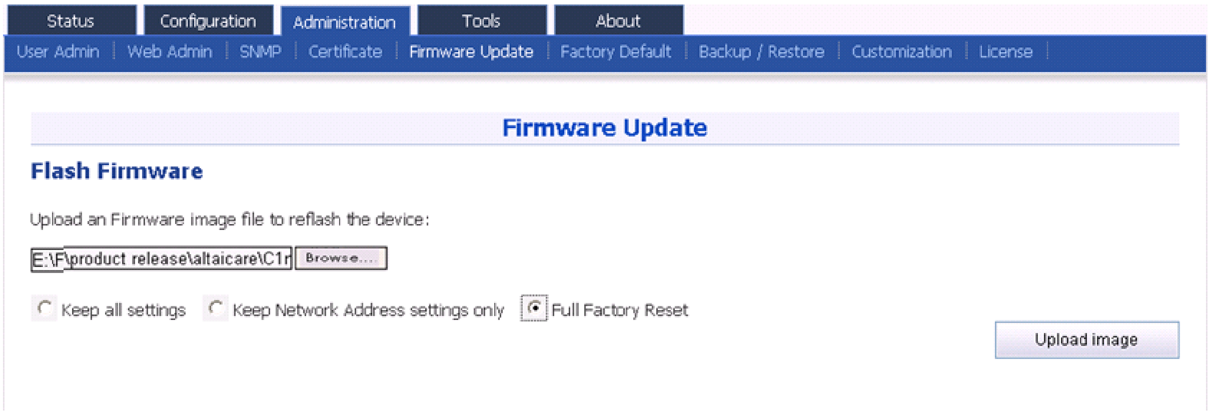
Note: Firmware that supports AltaiCare has a larger file size than that doesn't. If you have older versions of A2 and C1n/C1an which have only 8MB flash size, you will not be able to install this firmware on them, and hence cannot use them with AltaiCare.

Upgrade the AP firmware following the standard AP firmware upgrade procedure.

Procedures:

a. Go to Administration -> Firmware Update

b. Press **Browse** select the firmware



Firmware Update

Flash Firmware

Upload an Firmware image file to reflash the device:

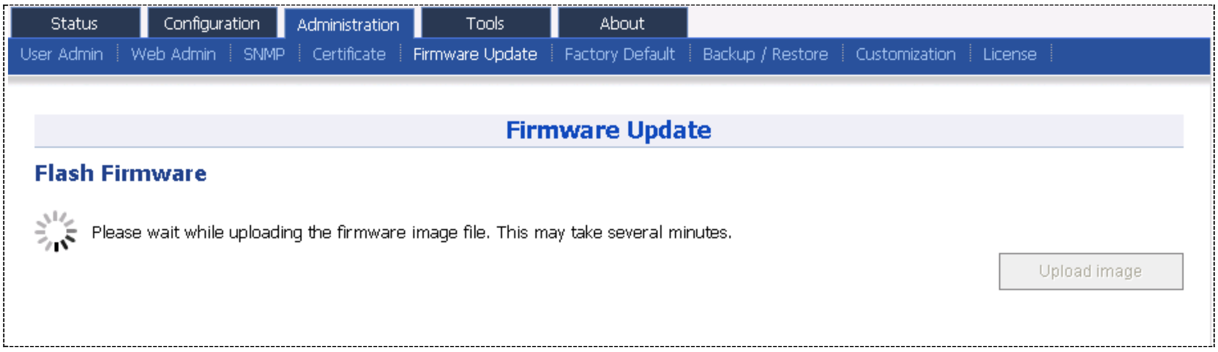
E:\F\product release\altaicare\C1r

○ Keep all settings ○ Keep Network Address settings only ● Full Factory Reset

c. Press **Upload image** to begin the update.

Keep all settings： All configuration will be kept after upgrading or downgrading. **Keep Network Address settings only**：The configuration about the network settings like IP address and VLAN will be kept after upgrading or downgrading.

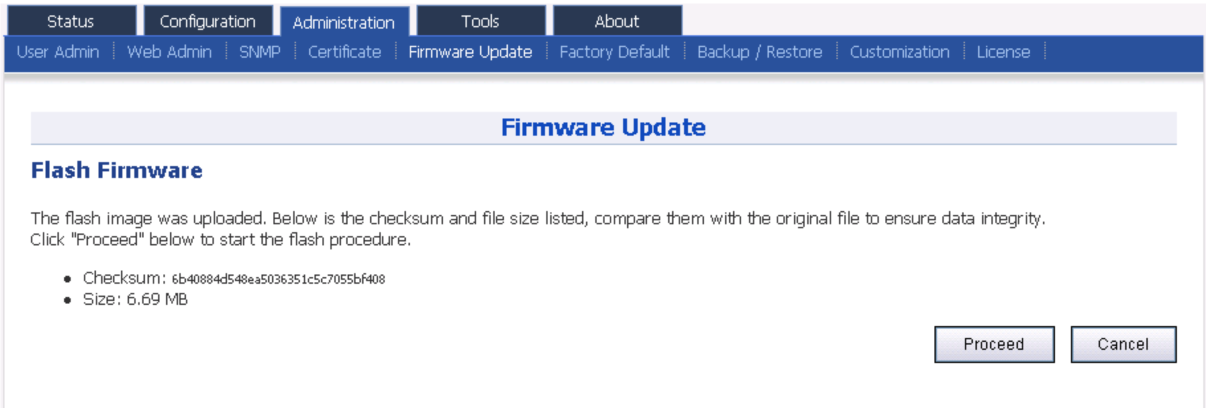
Full Factory Reset : All configuration will be lost and back to factory settings after upgrading or downgrading.



Firmware Update

Flash Firmware

Please wait while uploading the firmware image file. This may take several minutes.



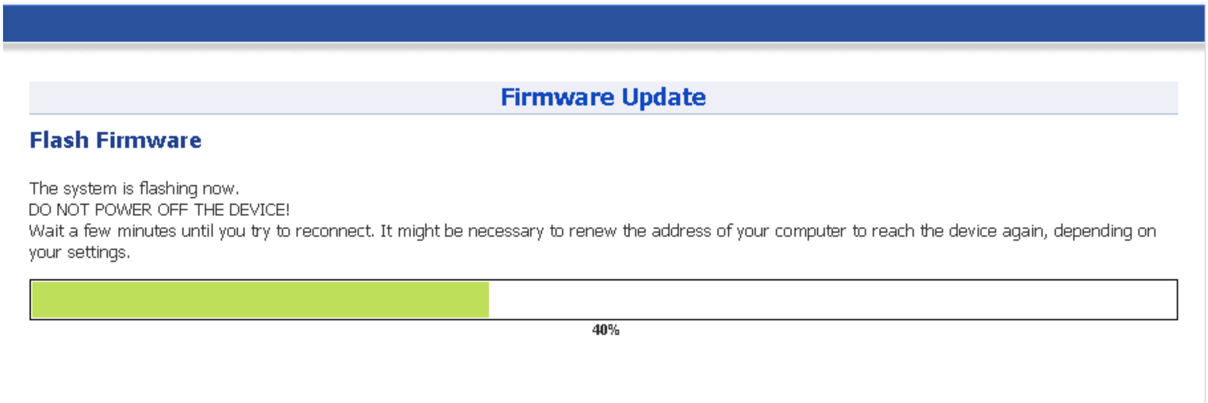
Firmware Update

Flash Firmware

The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity.
Click "Proceed" below to start the flash procedure.

- Checksum: 6b40884d548ea5036351c5c7055bf408
- Size: 6.69 MB

d. Press **Proceed** to execute the update.



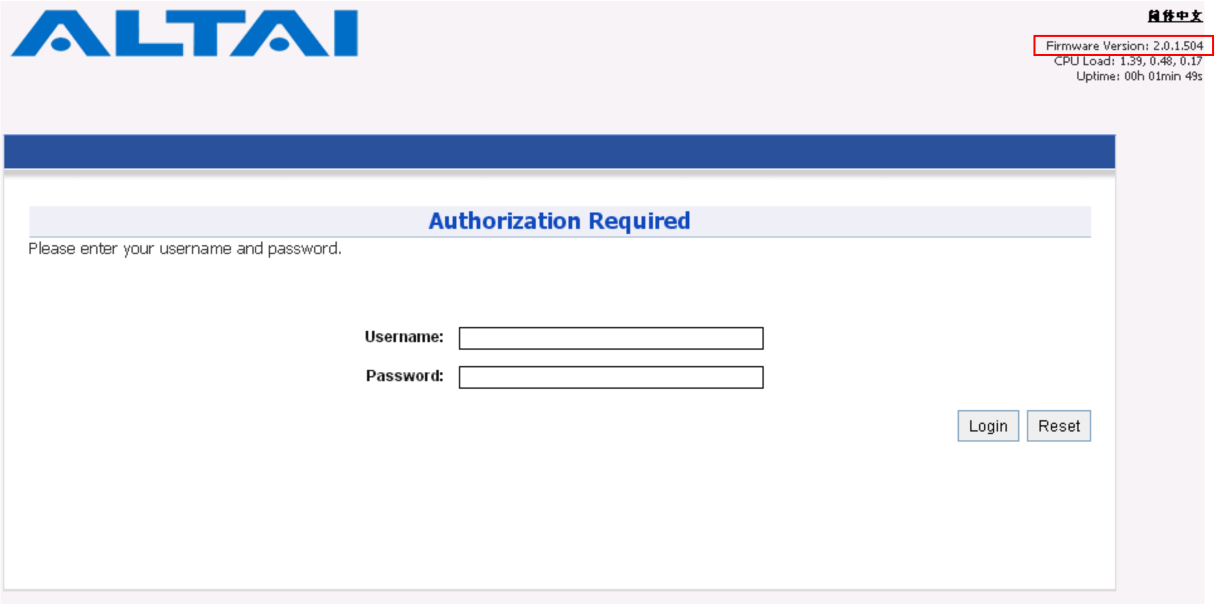
Firmware Update

Flash Firmware

The system is flashing now.
DO NOT POWER OFF THE DEVICE!
Wait a few minutes until you try to reconnect. It might be necessary to renew the address of your computer to reach the device again, depending on your settings.

e. AP will reboot and load the Main page after firmware update.

f. Login with username and password, check the firmware version on the top right corner or go to the "About" page.



Firmware Version: 2.0.1.504
CPU Load: 1.39, 0.48, 0.17
Uptime: 00h 01min 49s

Authorization Required

Please enter your username and password.

3.2. Enable Thin AP configuration and Select Controller Type

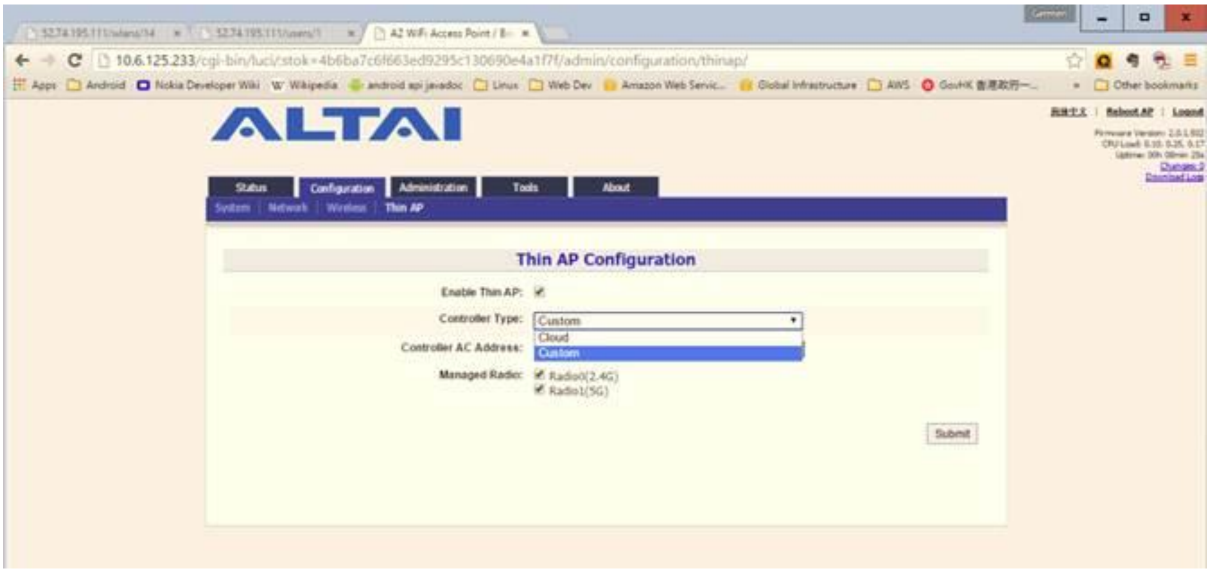
Open AP web admin console, Go to Configuration -> Thin AP.

a. Turn on Thin AP,
b. Select Controller Type
c. Select managed radio
d. Submit, Save & Apply the configuration
e. The AP will try to connect to the AltaiCare server, after the configuration is applied.

Controller Type

Could : AP will automatically connect to care.altaitechnologies.com

Custom : AP can specify the connection AC ip address



10.6.125.233/cgi-bin/luci/;stok=4b6ba7c6f663ed9295c130690e4a1f7f/admin/configuration/thinap/

Thin AP Configuration

Enable Thin AP: ☑

Controller Type: Custom (Cloud / Custom)

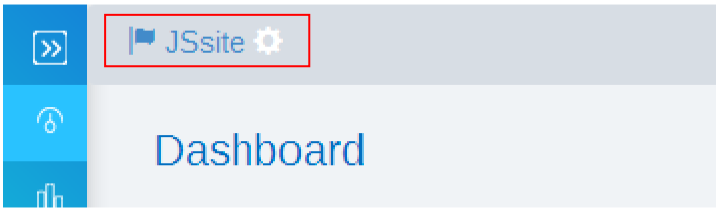
Controller AC Address:

Managed Radio: ☑ Radio0(2.4G) ☑ Radio1(5G)

4. WLAN Service Configuration

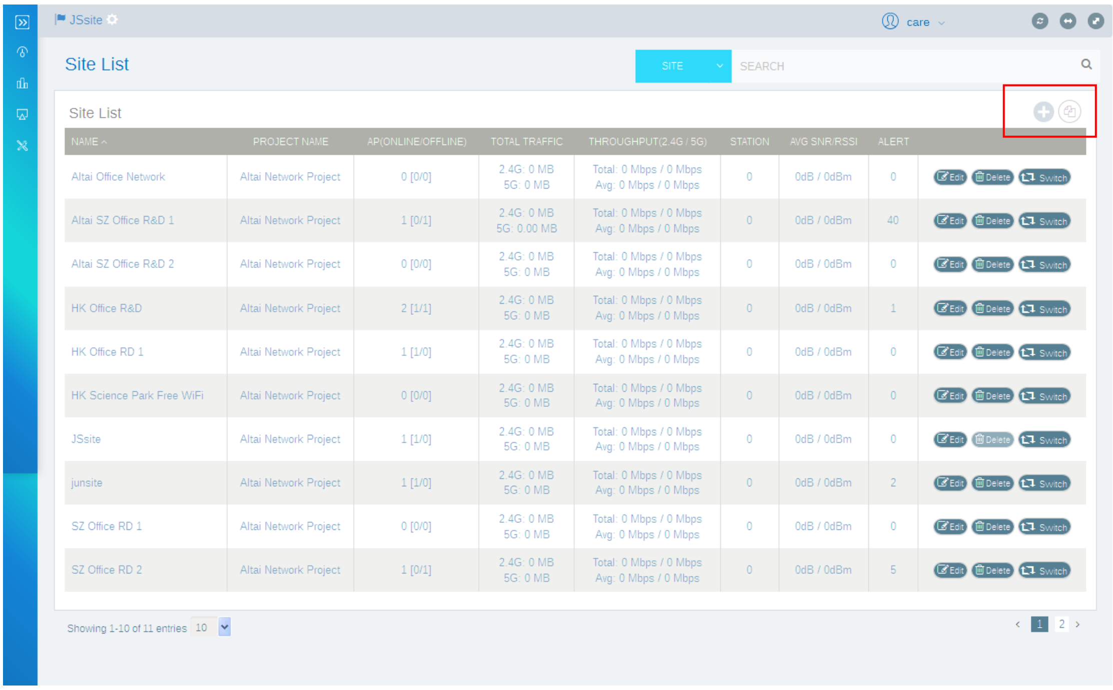
4.1. Create site in AltaiCare (for project admin only)

On top of the AltaiCare management console is showing the current site after the user login. Users can use the icon next to it to show the site list and switch to the site that they want to manage/monitor.



<u>Create site in AltaiCare Procedures:</u>

1. Click button on the right of current site's name.
2. Use the button on right top corner of the site list to create a site.



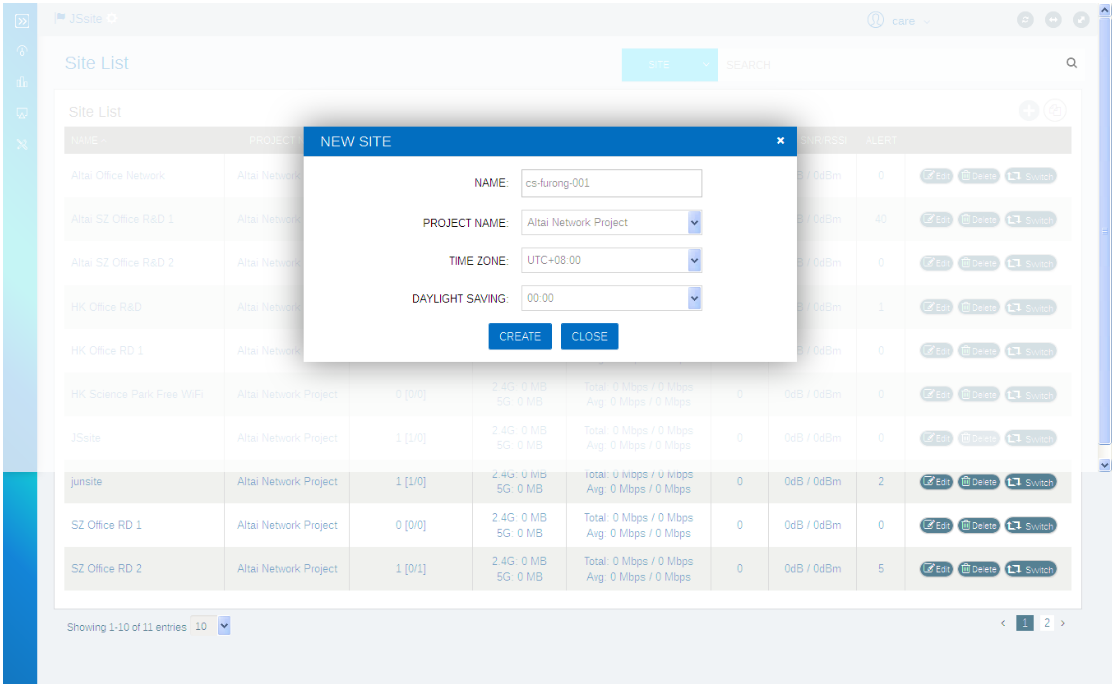
Site List

NAME ^	PROJECT NAME	AP(ONLINE/OFFLINE)	TOTAL TRAFFIC	THROUGHPUT(2.4G / 5G)	STATION	AVG SNR/RSSI	ALERT	
Altai Office Network	Altai Network Project	0 [0/0]	2.4G: 0 MB 5G: 0 MB	Total: 0 Mbps / 0 Mbps Avg: 0 Mbps / 0 Mbps	0	0dB / 0dBm	0	Edit Delete Switch
Altai SZ Office R&D 1	Altai Network Project	1 [0/1]	2.4G: 0 MB 5G: 0.00 MB	Total: 0 Mbps / 0 Mbps Avg: 0 Mbps / 0 Mbps	0	0dB / 0dBm	40	Edit Delete Switch
Altai SZ Office R&D 2	Altai Network Project	0 [0/0]	2.4G: 0 MB 5G: 0 MB	Total: 0 Mbps / 0 Mbps Avg: 0 Mbps / 0 Mbps	0	0dB / 0dBm	0	Edit Delete Switch
HK Office R&D	Altai Network Project	2 [1/1]	2.4G: 0 MB 5G: 0 MB	Total: 0 Mbps / 0 Mbps Avg: 0 Mbps / 0 Mbps	0	0dB / 0dBm	1	Edit Delete Switch
HK Office RD 1	Altai Network Project	1 [1/0]	2.4G: 0 MB 5G: 0 MB	Total: 0 Mbps / 0 Mbps Avg: 0 Mbps / 0 Mbps	0	0dB / 0dBm	0	Edit Delete Switch
HK Science Park Free WiFi	Altai Network Project	0 [0/0]	2.4G: 0 MB 5G: 0 MB	Total: 0 Mbps / 0 Mbps Avg: 0 Mbps / 0 Mbps	0	0dB / 0dBm	0	Edit Delete Switch
JSsite	Altai Network Project	1 [1/0]	2.4G: 0 MB 5G: 0 MB	Total: 0 Mbps / 0 Mbps Avg: 0 Mbps / 0 Mbps	0	0dB / 0dBm	0	Edit Delete Switch
junsite	Altai Network Project	1 [1/0]	2.4G: 0 MB 5G: 0 MB	Total: 0 Mbps / 0 Mbps Avg: 0 Mbps / 0 Mbps	0	0dB / 0dBm	2	Edit Delete Switch
SZ Office RD 1	Altai Network Project	0 [0/0]	2.4G: 0 MB 5G: 0 MB	Total: 0 Mbps / 0 Mbps Avg: 0 Mbps / 0 Mbps	0	0dB / 0dBm	0	Edit Delete Switch
SZ Office RD 2	Altai Network Project	1 [0/1]	2.4G: 0 MB 5G: 0 MB	Total: 0 Mbps / 0 Mbps Avg: 0 Mbps / 0 Mbps	0	0dB / 0dBm	5	Edit Delete Switch

Showing 1-10 of 11 entries 10

‹ 1 2 ›

3. Input the name and the time zone settings for the new site, and click "CREATE"



NEW SITE

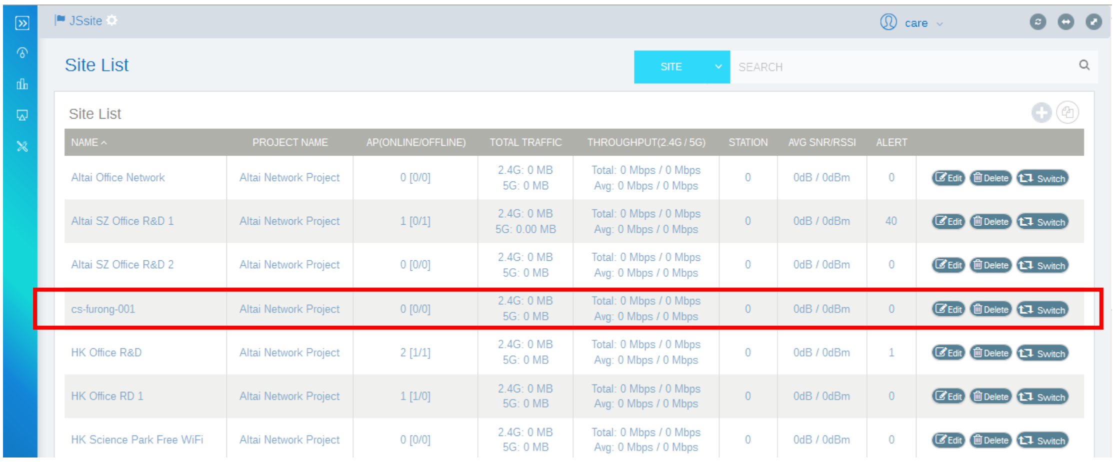
NAME: cs-furong-001

PROJECT NAME: Altai Network Project

TIME ZONE: UTC+08:00

DAYLIGHT SAVING: 00:00

4. The new site will be appear in the list



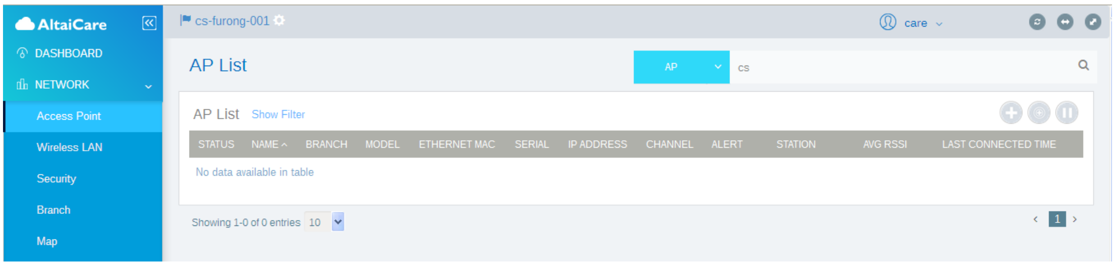
Site List

NAME ^	PROJECT NAME	AP(ONLINE/OFFLINE)	TOTAL TRAFFIC	THROUGHPUT(2.4G / 5G)	STATION	AVG SNR/RSSI	ALERT	
Altai Office Network	Altai Network Project	0 [0/0]	2.4G: 0 MB 5G: 0 MB	Total: 0 Mbps / 0 Mbps Avg: 0 Mbps / 0 Mbps	0	0dB / 0dBm	0	Edit Delete Switch
Altai SZ Office R&D 1	Altai Network Project	1 [0/1]	2.4G: 0 MB 5G: 0.00 MB	Total: 0 Mbps / 0 Mbps Avg: 0 Mbps / 0 Mbps	0	0dB / 0dBm	40	Edit Delete Switch
Altai SZ Office R&D 2	Altai Network Project	0 [0/0]	2.4G: 0 MB 5G: 0 MB	Total: 0 Mbps / 0 Mbps Avg: 0 Mbps / 0 Mbps	0	0dB / 0dBm	0	Edit Delete Switch
cs-furong-001	Altai Network Project	0 [0/0]	2.4G: 0 MB 5G: 0 MB	Total: 0 Mbps / 0 Mbps Avg: 0 Mbps / 0 Mbps	0	0dB / 0dBm	0	Edit Delete Switch
HK Office R&D	Altai Network Project	2 [1/1]	2.4G: 0 MB 5G: 0 MB	Total: 0 Mbps / 0 Mbps Avg: 0 Mbps / 0 Mbps	0	0dB / 0dBm	1	Edit Delete Switch
HK Office RD 1	Altai Network Project	1 [1/0]	2.4G: 0 MB 5G: 0 MB	Total: 0 Mbps / 0 Mbps Avg: 0 Mbps / 0 Mbps	0	0dB / 0dBm	0	Edit Delete Switch
HK Science Park Free WiFi	Altai Network Project	0 [0/0]	2.4G: 0 MB 5G: 0 MB	Total: 0 Mbps / 0 Mbps Avg: 0 Mbps / 0 Mbps	0	0dB / 0dBm	0	Edit Delete Switch

4.2. Register an AP in a site

Procedures:

1. Select **NETWORK->Access Point** On the navigation bar

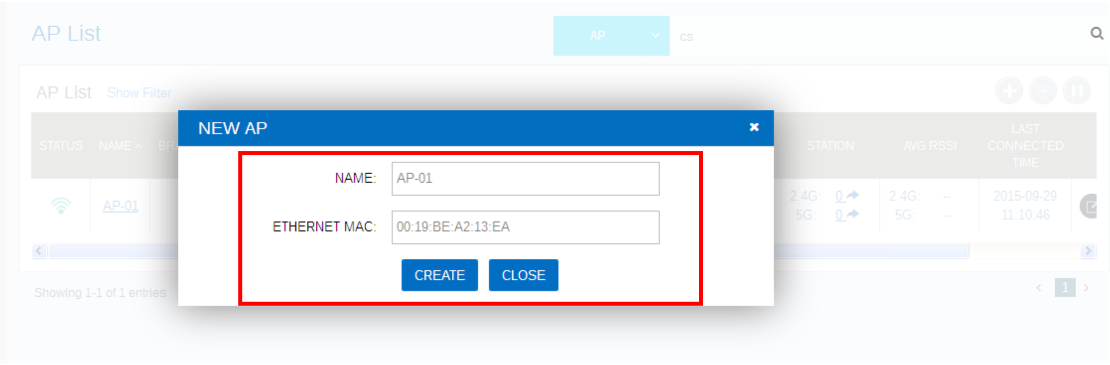


AP List Show Filter

STATUS	NAME ^	BRANCH	MODEL	ETHERNET MAC	SERIAL	IP ADDRESS	CHANNEL	ALERT	STATION	AVG RSSI	LAST CONNECTED TIME
No data available in table											

Showing 1-0 of 0 entries 10

2. Use the ⊕ button on right top corner of the AP list to register an AP, input the AP name and Ethernet MAC (eg. NAME:AP-01, ETHERNET MAC: 00:19:BE:A2：12：EA)



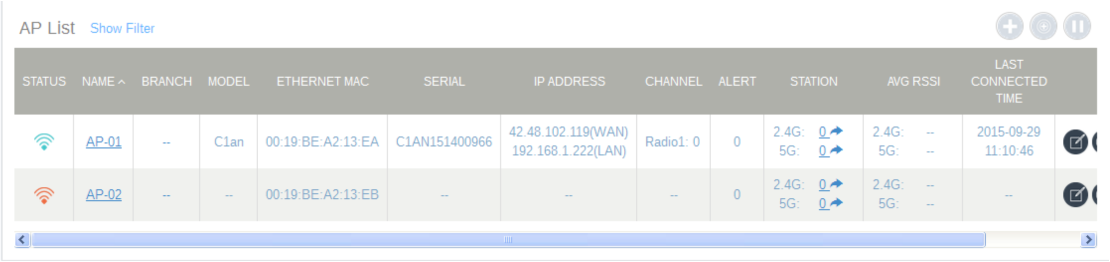
NEW AP

NAME: AP-01

ETHERNET MAC: 00:19:BE:A2:13:EA

CREATE   CLOSE

3. Click the “CREATE” button
4. IF the AP is registered to AltaiCare, AP MODEL/ SERIAL/ IP ADDRESS/ CHANNEL/ ALERT/ STATION/ AVG RSSI / LAST CONNECTED TIME information will be showed.



AP List   Show Filter

STATUS	NAME ^	BRANCH	MODEL	ETHERNET MAC	SERIAL	IP ADDRESS	CHANNEL	ALERT	STATION	AVG RSSI	LAST CONNECTED TIME

	AP-01	--	C1an	00:19:BE:A2:13:EA	C1AN151400966	42.48.102.119(WAN)
						192.168.1.222(LAN)
							Radio1: 0	0	2.4G: 0
									5G: 0
										2.4G: --
										5G: --
											2015-09-29
											11:10:46

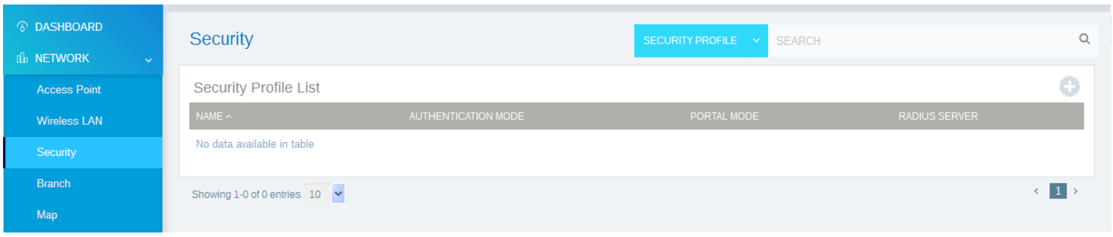
	AP-02	--	--	00:19:BE:A2:13:EB	--	--	--	0	2.4G: 0 5G: 0	2.4G: -- 5G: --	--

5. Click different function button” ” can perform different function to the AP, eg, edit/reboot/update firmware/remove

4.3. Create security profile

Procedures:

1. Go to **NETWORK**->**Security** On the navigation bar

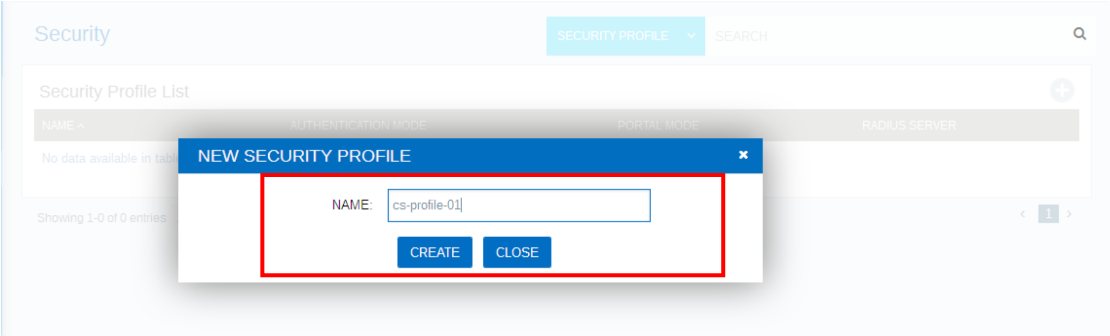


Security Profile List

NAME ^	AUTHENTICATION MODE	PORTAL MODE	RADIUS SERVER
No data available in table			

Showing 1-0 of 0 entries 10

2. Use the ⊕ button on right top corner of the Security Profile List to create security profile, input security profile name

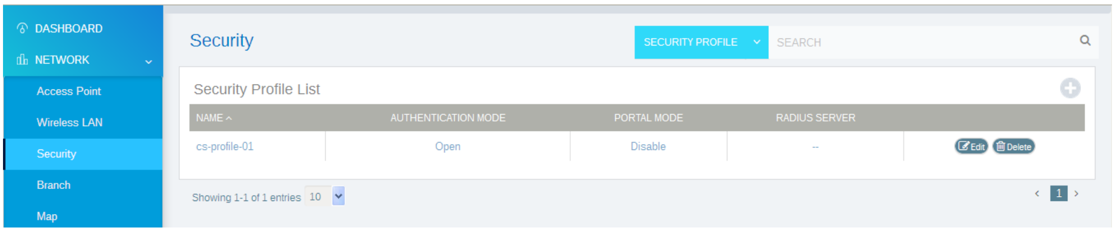


No data available in table

NAME: cs-profile-01

Showing 1-0 of 0 entries

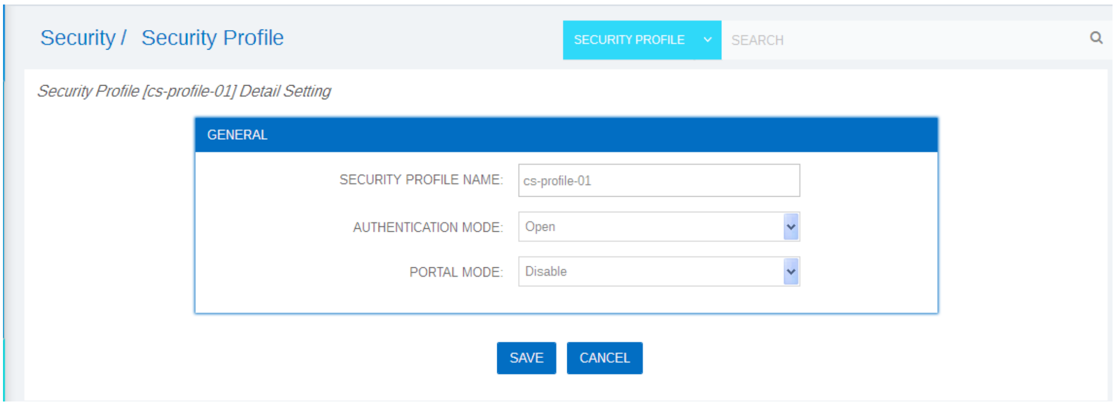
3. Click the “CREATE” button



NAME	AUTHENTICATION MODE	PORTAL MODE	RADIUS SERVER	
cs-profile-01	Open	Disable	--	Edit Delete

Showing 1-1 of 1 entries 10

4. Click the “Edit” button to edit the security profile



Security Profile [cs-profile-01] Detail Setting

SECURITY PROFILE NAME: cs-profile-01

AUTHENTICATION MODE: Open

PORTAL MODE: Disable

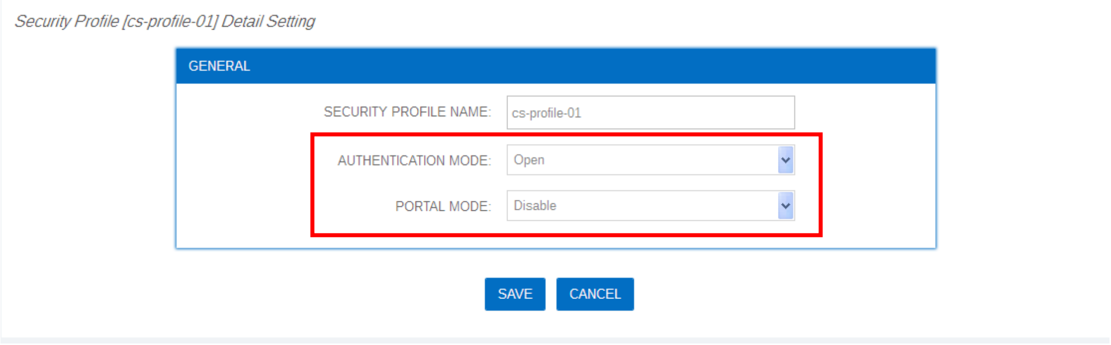
Authentication Mode includes:Open, WPA and WPA-PSK. When the Authentcation mode is set to open or WPA-PSK, PORTAL mode can be set Enable.

5. Authentication and Accounting

Before the Authentication and Accounting configuration, you need to create the profile Security, you can refer to the 4.3 chapter

5.1. AUTHENTICATION MODE-OPEN; PORTAL MODE-Disable

In this mode, there is no authentication and cipher for client to access a WLAN.



Security Profile [cs-profile-01] Detail Setting

GENERAL

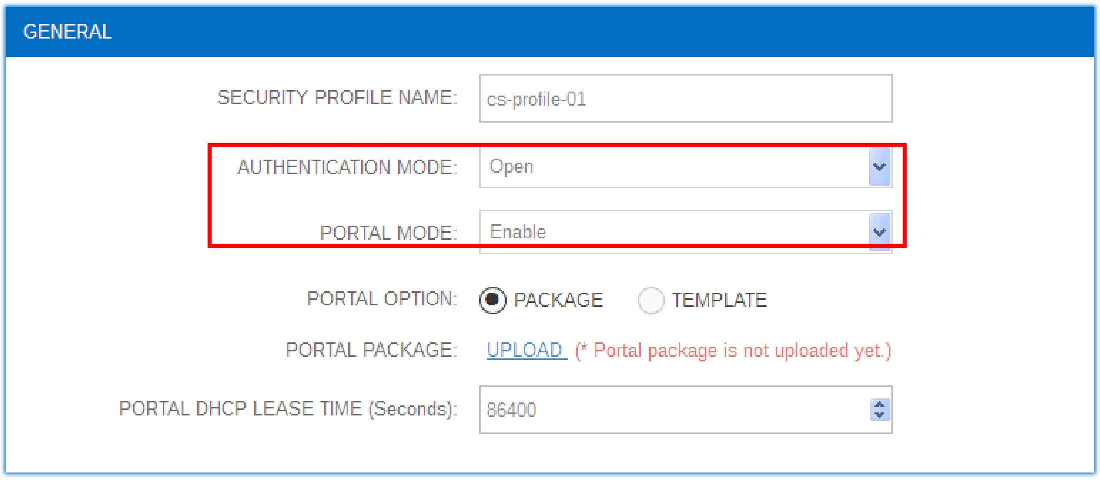
SECURITY PROFILE NAME: cs-profile-01

AUTHENTICATION MODE: Open

PORTAL MODE: Disable

5.2. AUTHENTICATION MODE-OPEN; PORTAL MODE-Enable

In this mode, when clients connect to a WLAN, a captive portal page will popup.



GENERAL

SECURITY PROFILE NAME: cs-profile-01

AUTHENTICATION MODE: Open

PORTAL MODE: Enable

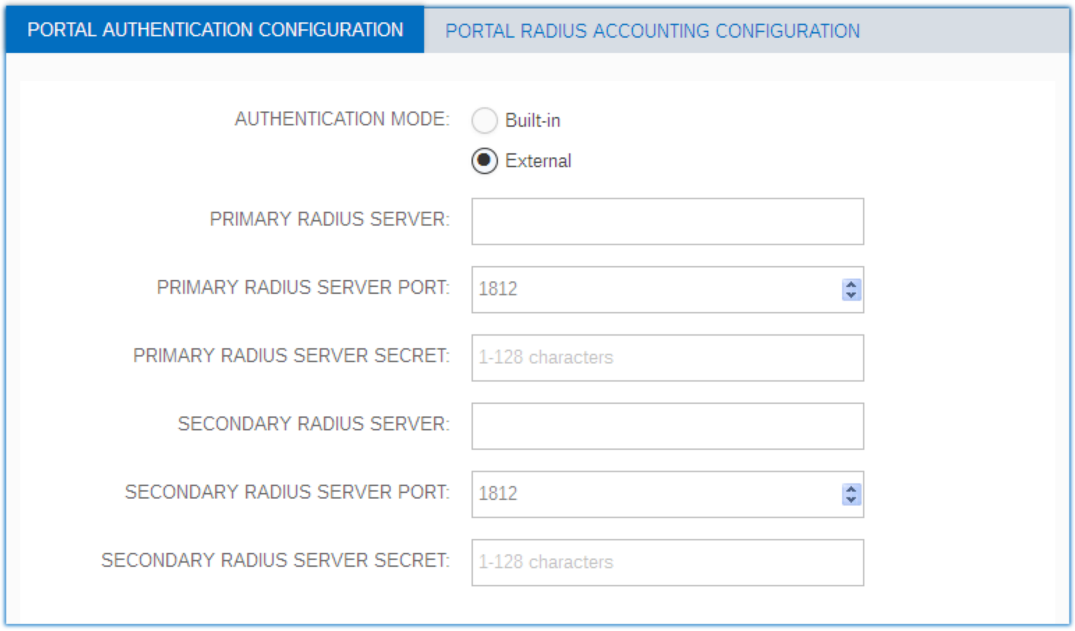
PORTAL OPTION: ● PACKAGE ○ TEMPLATE

PORTAL PACKAGE: UPLOAD (* Portal package is not uploaded yet.)

PORTAL DHCP LEASE TIME (Seconds): 86400

PORTAL OPTION: "PACKAGE" or "TEMPLATE" can be selected. When PACKAGE is selected, Click "UPLOAD" link can upload PORTAL PACKAGE, When TEMPLATE is selected, Click "UPDATE" link can update PORTAL TEMPLATE

PORTAL DHCP LEASE TIME (Seconds): Set portal DHCP lease time value



PORTAL AUTHENTICATION CONFIGURATION | PORTAL RADIUS ACCOUNTING CONFIGURATION

AUTHENTICATION MODE: ○ Built-in ● External

PRIMARY RADIUS SERVER:

PRIMARY RADIUS SERVER PORT: 1812

PRIMARY RADIUS SERVER SECRET: 1-128 characters

SECONDARY RADIUS SERVER:

SECONDARY RADIUS SERVER PORT: 1812

SECONDARY RADIUS SERVER SECRET: 1-128 characters

AUTHENTICATION MODE: Built-in and External can be selected, "Built-in" means AltaiCare work as an authentication server, "External" means use an external radius server do the authentication work.

PRIMARY RADIUS SERVER: Set primary radius server IP address

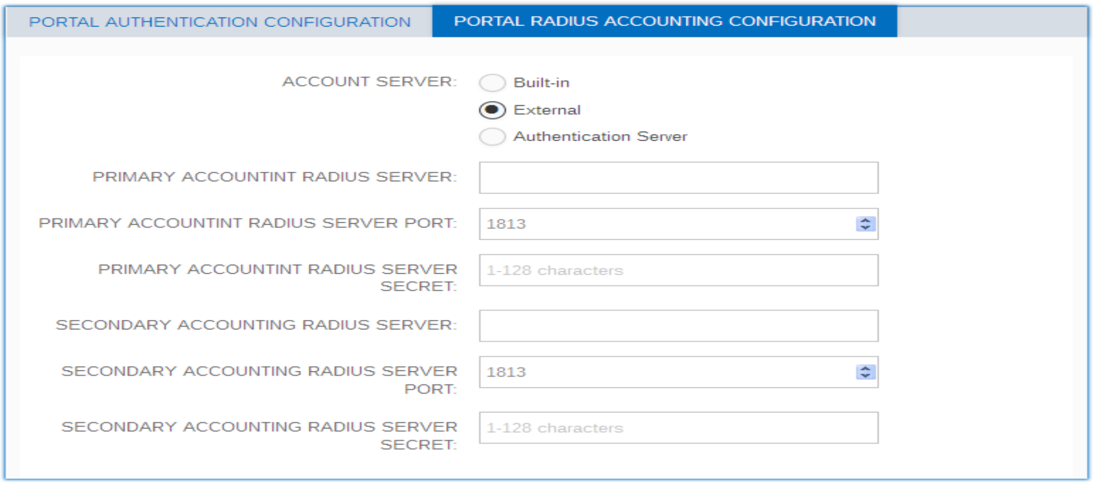
PRIMARY RADIUS SERVER PORT: Set primary Radius server port

PRIMARY RADIUS SERVER SECRET: Set primary Radius secret

SECONDARY RADIUS SERVER: Set secondary radius server IP address

SECONDARY RADIUS SERVER PORT: Set secondary Radius server port

SECONDARY RADIUS SERVER SECRET: Set secondary Radius secret



PORTAL AUTHENTICATION CONFIGURATION | PORTAL RADIUS ACCOUNTING CONFIGURATION

ACCOUNT SERVER: ○ Built-in ● External ○ Authentication Server

PRIMARY ACCOUNTINT RADIUS SERVER:

PRIMARY ACCOUNTINT RADIUS SERVER PORT: 1813

PRIMARY ACCOUNTINT RADIUS SERVER SECRET: 1-128 characters

SECONDARY ACCOUNTING RADIUS SERVER:

SECONDARY ACCOUNTING RADIUS SERVER PORT: 1813

SECONDARY ACCOUNTING RADIUS SERVER SECRET: 1-128 characters

ACCOUNT SERVER: Select account server mode, "Built-in" means AltaiCare work as an account server and execute the accounting, "External" means use an external account server do the accounting work, "Authentication Server" specify the authentication server port.

PRIMARY RADIUS SERVER: Set primary radius server IP address

PRIMARY RADIUS SERVER PORT: Set primary Radius server port

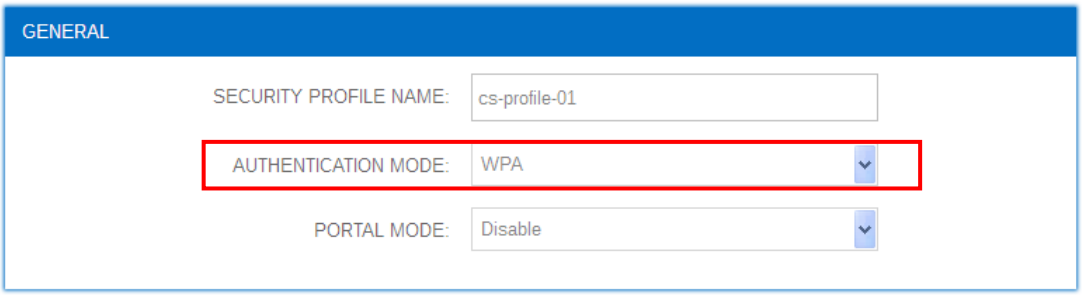
PRIMARY RADIUS SERVER SECRET: Set primary Radius secret

SECONDARY RADIUS SERVER: Set secondary radius server IP address

SECONDARY RADIUS SERVER PORT: Set secondary Radius server port

SECONDARY RADIUS SERVER SECRET: Set secondary Radius secret

5.3. AUTHENTICATION MODE-WPA; PORTAL MODE-Disable



GENERAL

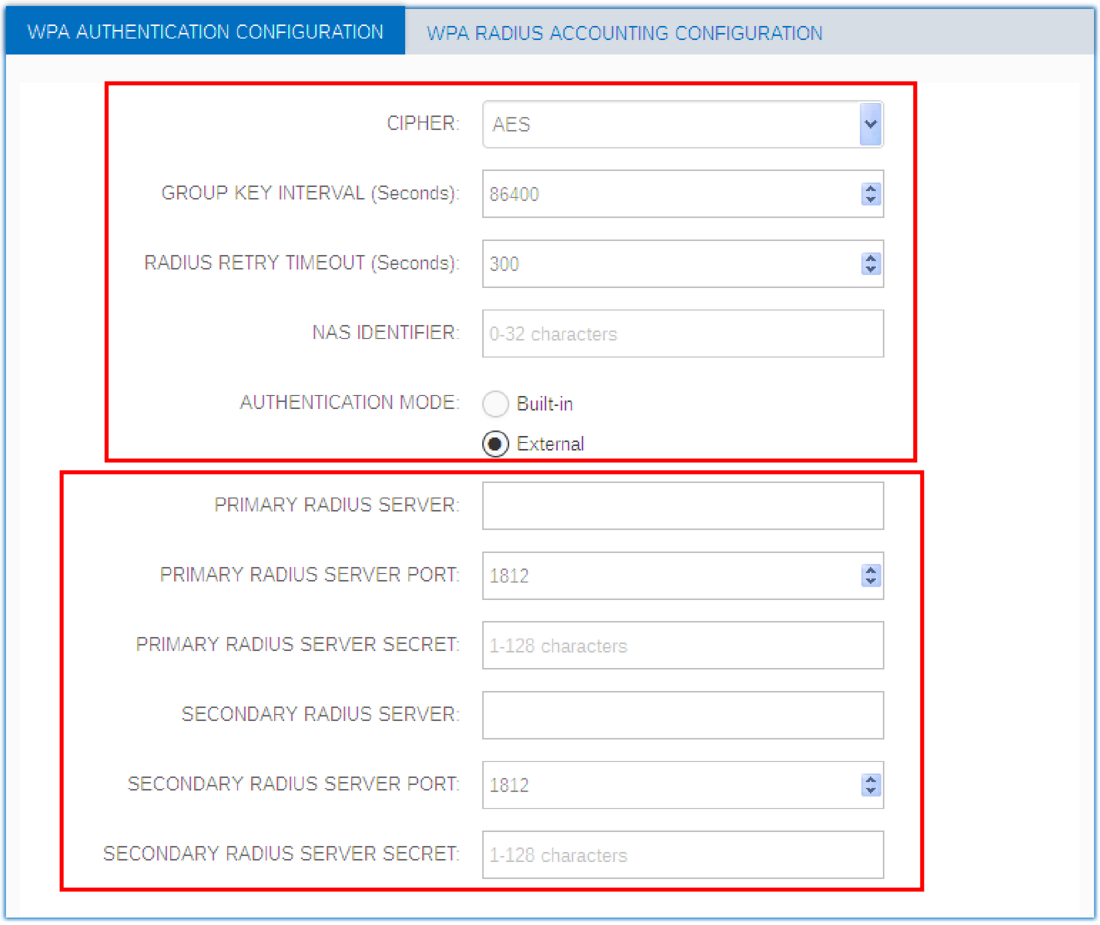
SECURITY PROFILE NAME: cs-profile-01

AUTHENTICATION MODE: WPA

PORTAL MODE: Disable

AUTHENTICTION MODE : WPA

WPA AUTHENTICATION CONFIGURATION



WPA AUTHENTICATION CONFIGURATION
WPA RADIUS ACCOUNTING CONFIGURATION

CIPHER: AES

GROUP KEY INTERVAL (Seconds): 86400

RADIUS RETRY TIMEOUT (Seconds): 300

NAS IDENTIFIER: 0-32 characters

AUTHENTICATION MODE: ○ Built-in ● External

PRIMARY RADIUS SERVER:

PRIMARY RADIUS SERVER PORT: 1812

PRIMARY RADIUS SERVER SECRET: 1-128 characters

SECONDARY RADIUS SERVER:

SECONDARY RADIUS SERVER PORT: 1812

SECONDARY RADIUS SERVER SECRET: 1-128 characters

CIPHER: AES and TKIP can be choired

GROUP KEY INTERVAL (Seconds): Set the group key interval value, default value is 86400

RADIUS RETRY TIMEOUT (Seconds): Set radius retry timeout value

NAS IDENTIFIER: In put the NAS ID information

AUTHENTICATION MODE: "Built-in" indicates the AltaiCare system work as raidus server and execute the authentication, "External" means use an external radius server

PRIMARY RADIUS SERVER: Set primary radius server IP address

PRIMARY RADIUS SERVER PORT: Set primary Radius server port

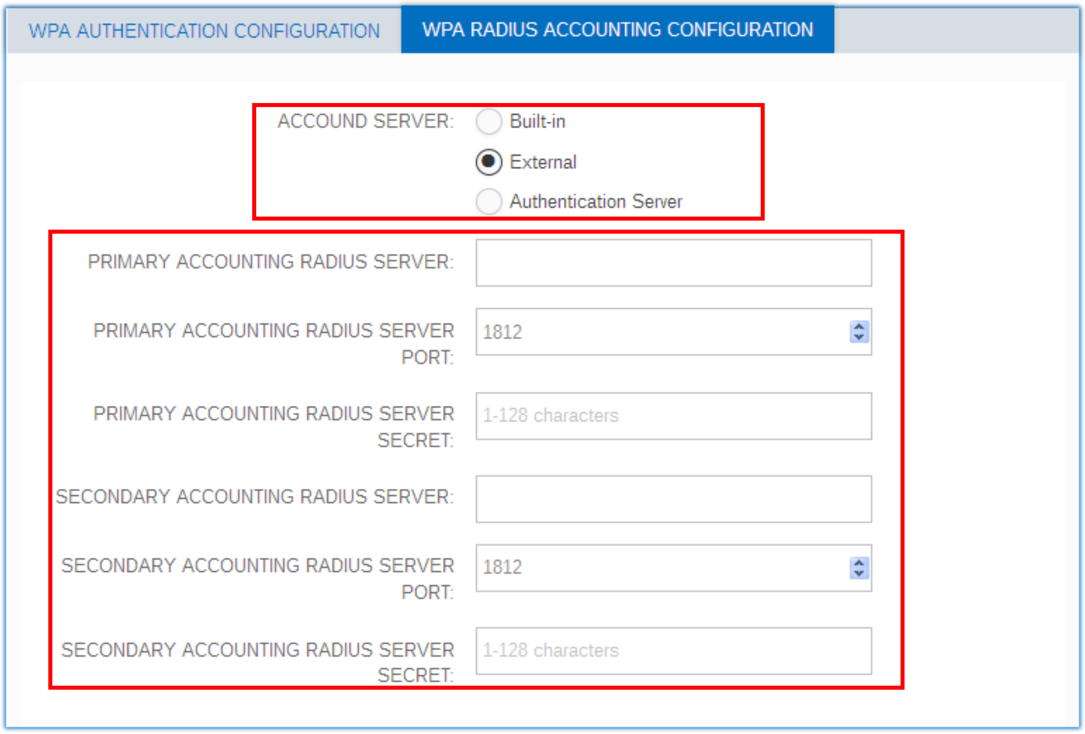
PRIMARY RADIUS SERVER SECRET: Set primary Radius secret

SECONDARY RADIUS SERVER: Set secondary radius server IP address

SECONDARY RADIUS SERVER PORT: Set secondary Radius server port

SECONDARY RADIUS SERVER SECRET: Set secondary Radius secret

WPA RADIUS ACCOUNTING CONFIGURATION



WPA AUTHENTICATION CONFIGURATION | WPA RADIUS ACCOUNTING CONFIGURATION

ACCOUND SERVER: ○ Built-in ● External ○ Authentication Server

PRIMARY ACCOUNTING RADIUS SERVER:

PRIMARY ACCOUNTING RADIUS SERVER PORT: 1812

PRIMARY ACCOUNTING RADIUS SERVER SECRET: 1-128 characters

SECONDARY ACCOUNTING RADIUS SERVER:

SECONDARY ACCOUNTING RADIUS SERVER PORT: 1812

SECONDARY ACCOUNTING RADIUS SERVER SECRET: 1-128 characters

ACCOUND SERVER: Select account server mode, "Built-in" means AltaiCare work as an account server and execute the accounting, "External" means use an external account server do the accounting work, "Authentication Server" specify the authentication server port.

PRIMARY ACCOUNTING RADIUS SERVER: Set primary accounting server IP address

PRIMARY ACCOUNTING RADIUS SERVER PORT: Set primary accounting server port

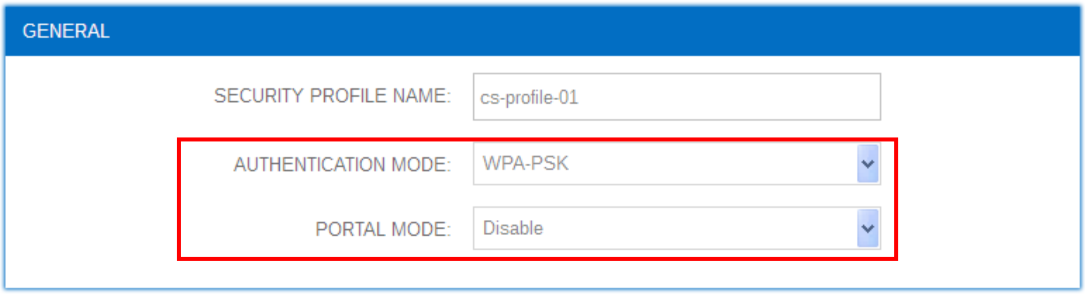
PRIMARY ACCOUNTING RADIUS SERVER SECRET: Set primary accounting secret

SECONDARY ACCOUNTING RADIUS SERVER: Set secondary accounting server IP address

SECONDARY ACCOUNTING RADIUS SERVER PORT: Set secondary accounting server port

SECONDARY ACCOUNTING RADIUS SERVER SECRET: Set secondary accounting secret

5.4. AUTHENTICATION MODE-WPA-PSK; PORTAL MODE-Disable



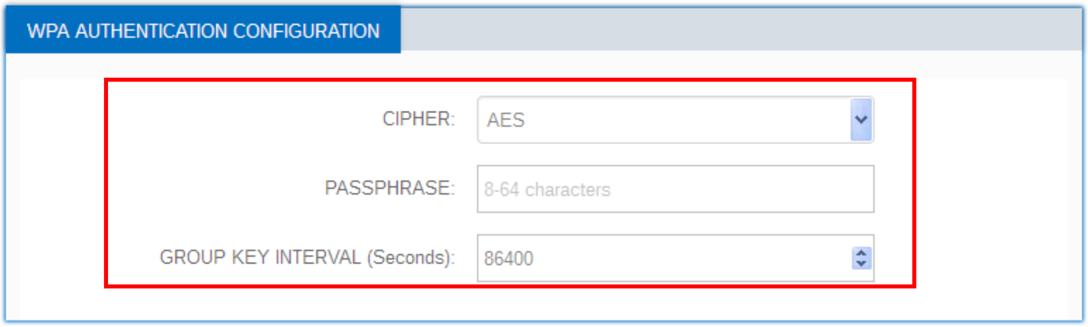
GENERAL

SECURITY PROFILE NAME: cs-profile-01

AUTHENTICATION MODE: WPA-PSK

PORTAL MODE: Disable

WPA AUTHENTICATION CONFIGURATION



WPA AUTHENTICATION CONFIGURATION

CIPHER: AES

PASSPHRASE: 8-64 characters

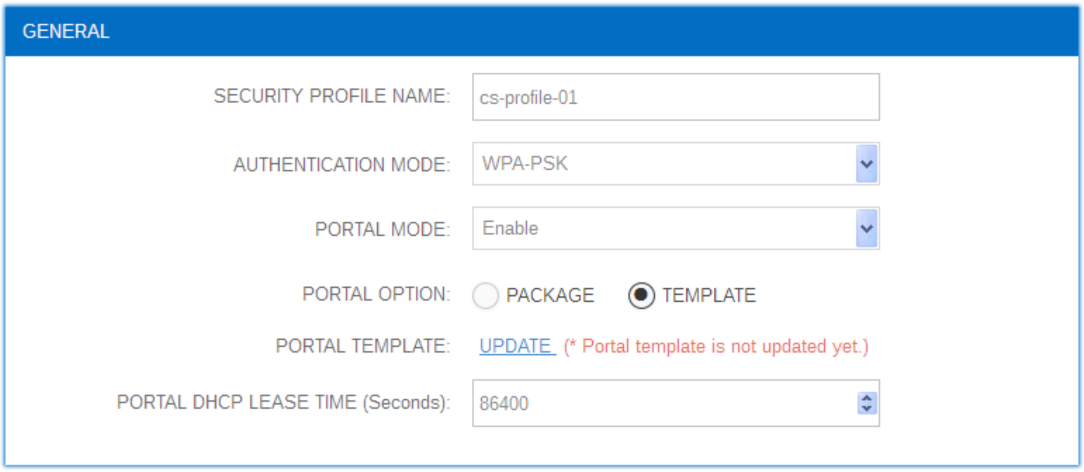
GROUP KEY INTERVAL (Seconds): 86400

CIPHER: AES and TKIP can be choired

PASSPHRASE: In put the passphrase

GROUP KEY INTERVAL (Seconds): Set the group key interval value, default value is 86400

5.5. AUTHENTICATION MODE-WPA-PSK; PORTAL MODE-Enable



GENERAL

SECURITY PROFILE NAME: cs-profile-01

AUTHENTICATION MODE: WPA-PSK

PORTAL MODE: Enable

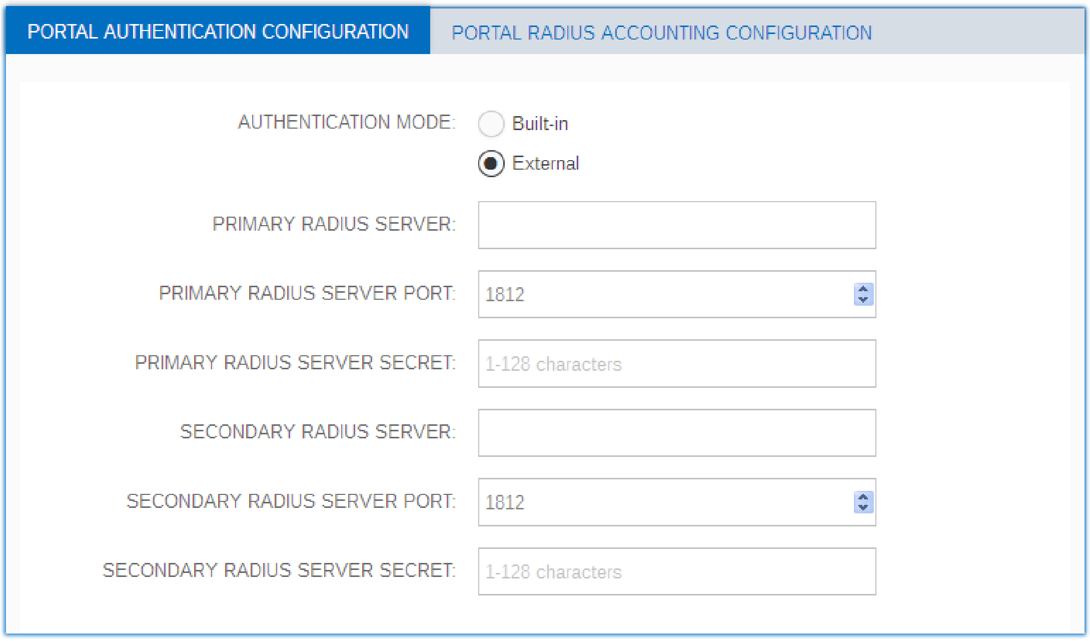
PORTAL OPTION: ○ PACKAGE ● TEMPLATE

PORTAL TEMPLATE: UPDATE (* Portal template is not updated yet.)

PORTAL DHCP LEASE TIME (Seconds): 86400

PORTAL OPTION: "PACKAGE" or "TEMPLATE" can be selected. When PACKAGE is selected, Click "UPLOAD" link can upload PORTAL PACKAGE, When TEMPLATE is selected, Click "UPDATE" link can update PORTAL TEMPLATE

PORTAL DHCP LEASE TIME (Seconds): Set portal DHCP lease time value



PORTAL AUTHENTICATION CONFIGURATION | PORTAL RADIUS ACCOUNTING CONFIGURATION

AUTHENTICATION MODE: ○ Built-in ● External

PRIMARY RADIUS SERVER:

PRIMARY RADIUS SERVER PORT: 1812

PRIMARY RADIUS SERVER SECRET: 1-128 characters

SECONDARY RADIUS SERVER:

SECONDARY RADIUS SERVER PORT: 1812

SECONDARY RADIUS SERVER SECRET: 1-128 characters

AUTHENTICATION MODE: Built-in and External can be selected, "Built-in" means AltaiCare work as an authentication server, "External" means use an external radius server do the authentication work.

PRIMARY RADIUS SERVER: Set primary radius server IP address

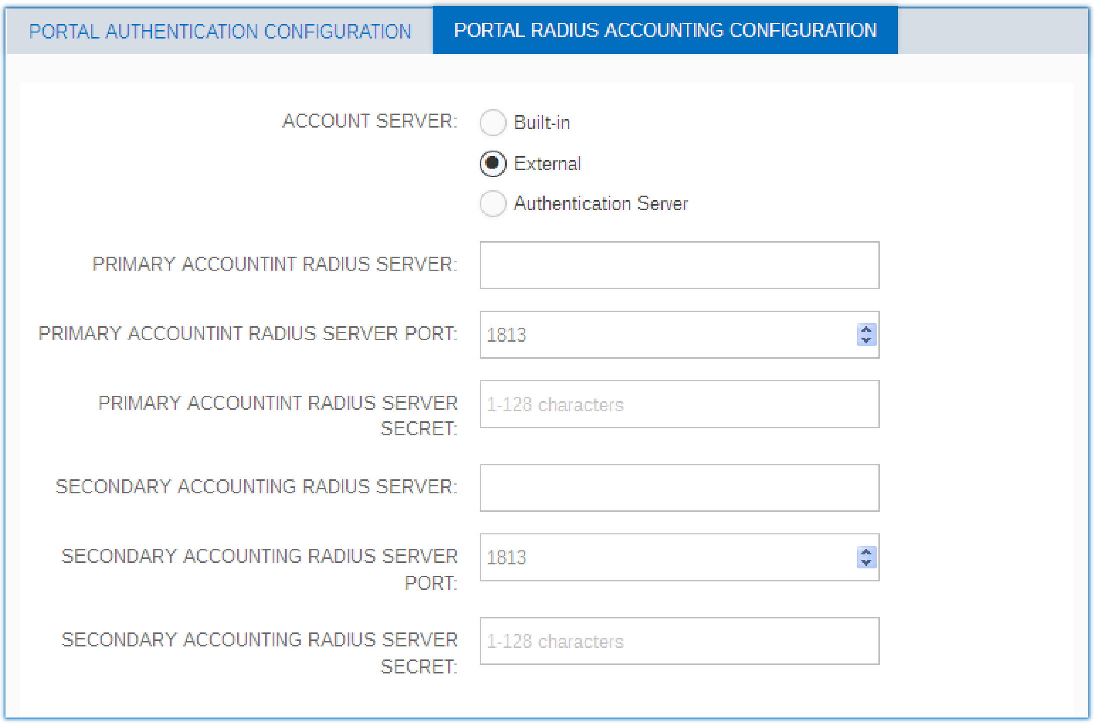
PRIMARY RADIUS SERVER PORT: Set primary Radius server port

PRIMARY RADIUS SERVER SECRET: Set primary Radius secret

SECONDARY RADIUS SERVER: Set secondary radius server IP address

SECONDARY RADIUS SERVER PORT: Set secondary Radius server port

SECONDARY RADIUS SERVER SECRET: Set secondary Radius secret



PORTAL AUTHENTICATION CONFIGURATION | PORTAL RADIUS ACCOUNTING CONFIGURATION

ACCOUNT SERVER: ○ Built-in ● External ○ Authentication Server

PRIMARY ACCOUNTINT RADIUS SERVER:

PRIMARY ACCOUNTINT RADIUS SERVER PORT: 1813

PRIMARY ACCOUNTINT RADIUS SERVER SECRET: 1-128 characters

SECONDARY ACCOUNTING RADIUS SERVER:

SECONDARY ACCOUNTING RADIUS SERVER PORT: 1813

SECONDARY ACCOUNTING RADIUS SERVER SECRET: 1-128 characters

ACCOUNT SERVER: Select account server mode, "Built-in" means AltaiCare work as an account server and execute the accounting, "External" means use an external account server do the accounting work, "Authentication Server" specify the authentication server port.

PRIMARY RADIUS SERVER: Set primary radius server IP address

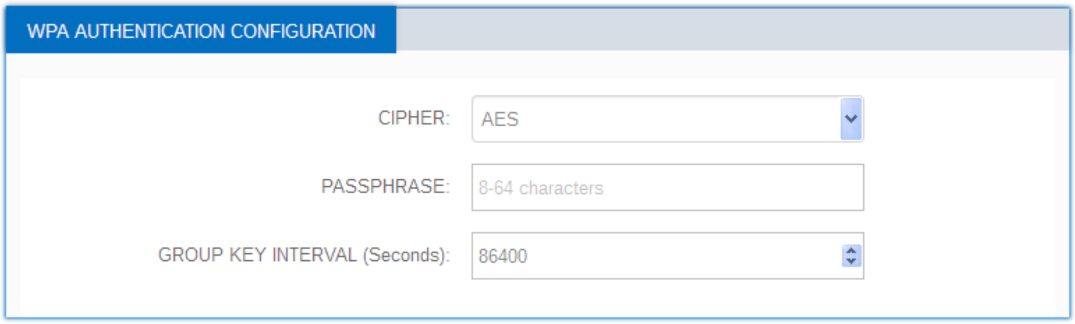
PRIMARY RADIUS SERVER PORT: Set primary Radius server port

PRIMARY RADIUS SERVER SECRET: Set primary Radius secret

SECONDARY RADIUS SERVER: Set secondary radius server IP address

SECONDARY RADIUS SERVER PORT: Set secondary Radius server port

SECONDARY RADIUS SERVER SECRET: Set secondary Radius secret



WPA AUTHENTICATION CONFIGURATION

CIPHER: AES

PASSPHRASE: 8-64 characters

GROUP KEY INTERVAL (Seconds): 86400

CIPHER: AES and TKIP can be choired

PASSPHRASE: In put the passphrase

GROUP KEY INTERVAL (Seconds): Set the group key interval value, default value is 86400

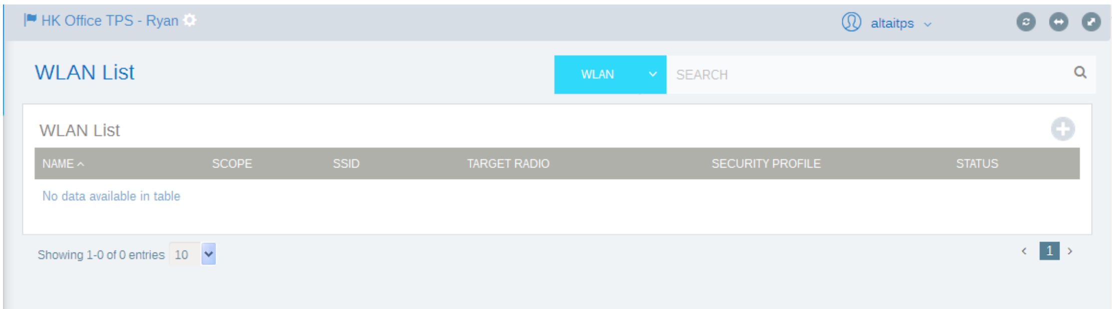
6. Service/Bandwidth Control

Bandwidth control is realized by wireless LAN, First of all, you need to create the Wireless LAN.

6.1. Set bandwidth limit when creating WLAN

Procedures:

1. Select **NETWORK**->**Wireless LAN** On the navigation bar



HK Office TPS - Ryan

altaitps

WLAN List

WLAN

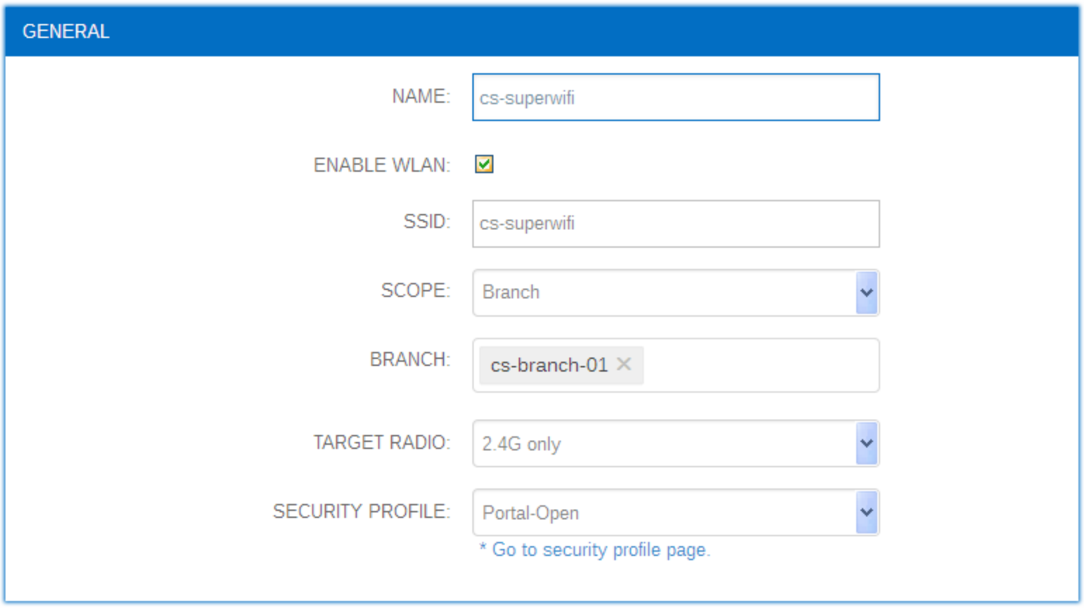
SEARCH

WLAN List

NAME	SCOPE	SSID	TARGET RADIO	SECURITY PROFILE	STATUS
No data available in table					

Showing 1-0 of 0 entries 10

2. Click the ⊕ button on right top corner of the WLAN list to add a new WLAN, input NAME/ SSID/ SCOPE (can select branch)/ TARGET RADIO/ SECURITY PROFILE



GENERAL

NAME: cs-superwifi

ENABLE WLAN: ☑

SSID: cs-superwifi

SCOPE: Branch

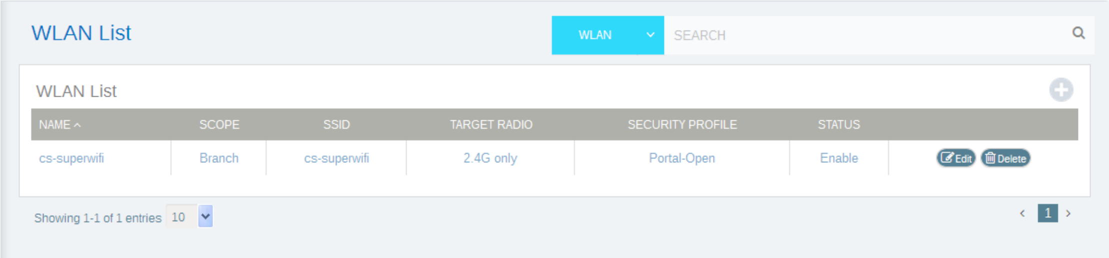
BRANCH: cs-branch-01 ×

TARGET RADIO: 2.4G only

SECURITY PROFILE: Portal-Open

* Go to security profile page.

3. Click the "CREATE" button
4. In WLAN List we will see the new WLAN, eg, cs-superwifi



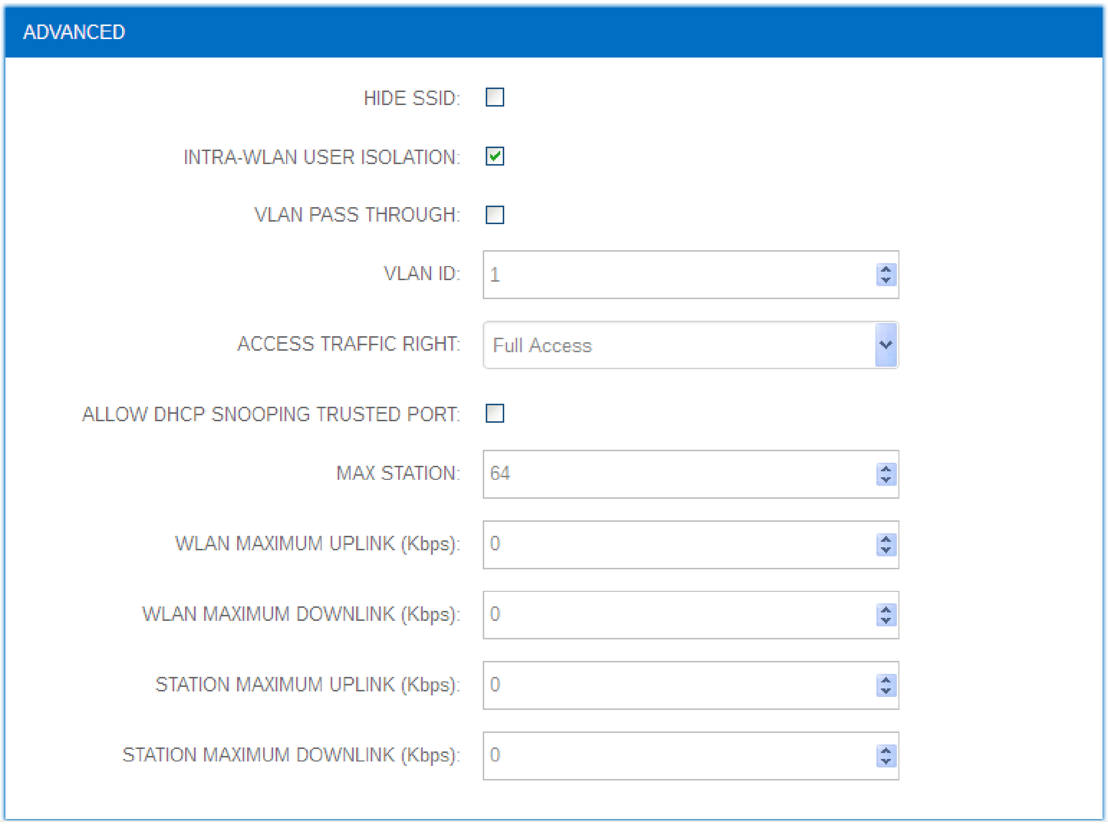
WLAN List

WLAN List

NAME	SCOPE	SSID	TARGET RADIO	SECURITY PROFILE	STATUS	
cs-superwifi	Branch	cs-superwifi	2.4G only	Portal-Open	Enable	Edit Delete

Showing 1-1 of 1 entries 10

5. Click Edit button can edit the WLAN



ADVANCED

HIDE SSID: □

INTRA-WLAN USER ISOLATION: ☑

VLAN PASS THROUGH: □

VLAN ID: 1

ACCESS TRAFFIC RIGHT: Full Access

ALLOW DHCP SNOOPING TRUSTED PORT: □

MAX STATION: 64

WLAN MAXIMUM UPLINK (Kbps): 0

WLAN MAXIMUM DOWNLINK (Kbps): 0

STATION MAXIMUM UPLINK (Kbps): 0

STATION MAXIMUM DOWNLINK (Kbps): 0

HIDE SSID: Hide this SSID or not

INTRA-WLAN USER ISOLATION: Allow or block intra-WLAN user communication

VLAN PASS THROUGH: VLAN pass through for this WLAN

VLAN ID: Set the service VLAN ID

ACCESS TRAFFIC RIGHT: Access traffic right controls associated stations the ability to permit or deny AP management

ALLOW DHCP SNOOPING TRUST PORT: DHCP snooping prevents illegal DHCP servers from offering IP address on untrusted wireless port

MAX STATION: Set the maximum station value

WLAN MAXIMUM UPLINK (Kbps): Set the WLAN uplink bandwidth limitation

WLAN MAXIMUM DOWNLINK (Kbps): Set the WLAN downlink bandwidth limitation

STATION MAXIMUM UPLINK (Kbps): Set the station uplink bandwidth limitation

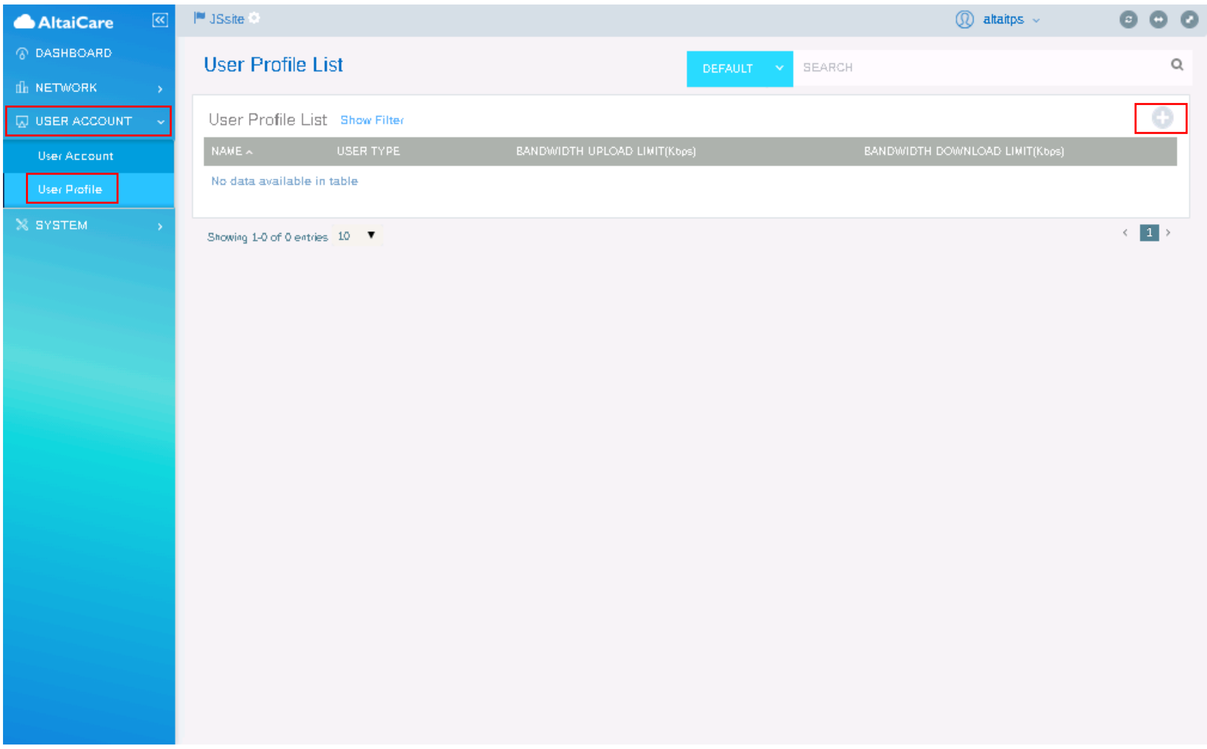
STATION MAXIMUM DOWNLINK (Kbps): Set the station downlink bandwidth limitation

6.2. User Service Control – Profile and Account Creation

AltaiCare supports built-in user database for portal and WPA authentications to implement a variety of user service, i.e. prepaid or subscription models; data limit and time limit; and bandwidth control. Administrators can create User Profile and User Account for this kind of purposes.

Procedures:

1. Go to select **USER ACCOUNT**->**User Profile** on the navigation panel to create a new user profile.



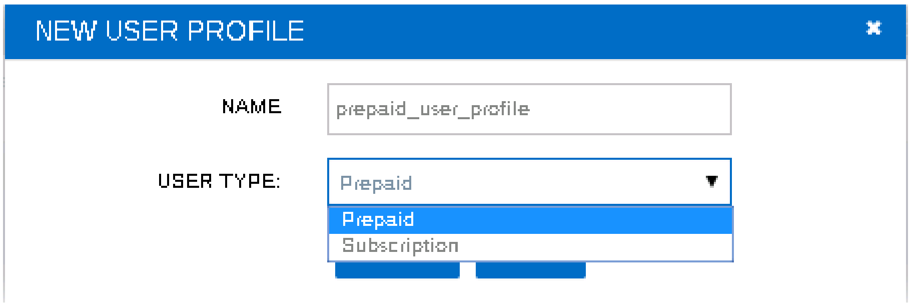
User Profile List

User Profile List

NAME	USER TYPE	BANDWIDTH UPLOAD LIMIT(Kbps)	BANDWIDTH DOWNLOAD LIMIT(Kbps)
No data available in table			

Showing 1-0 of 0 entries 10

2. Click a “Plus” sign as shown in the above screenshot to create a new user profile.

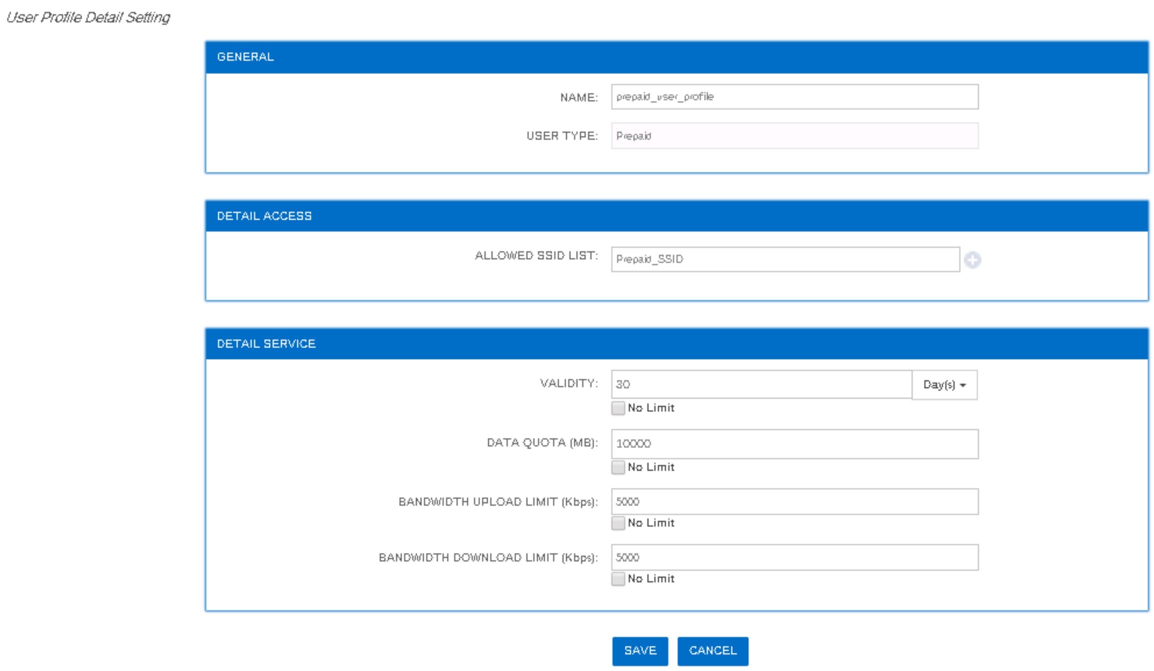


NEW USER PROFILE

NAME prepaid_user_profile

USER TYPE: Prepaid

3. Fill in the "NAME" and "USER TYPE" fields in the pop-up window "NEW USER PROFILE" for user profile configuration. Administrators can have two options for "USER TYPE": 1) Prepaid; and 2) Subscription. The first option "Prepaid" can let administrators provide and configure the prepaid service like session time control, data limit and bandwidth control. The second option "Subscription" can let administrators provide and configure the postpaid service plan like monthly data limit and bandwidth control.
4. Click "CREATE" to create the new user profile.
5. Administrators can edit the profile with more service control configuration by clicking "Edit".
6. Below is the screenshot for the configuration of prepaid model.



User Profile Detail Setting

GENERAL

NAME: prepaid_user_profile

USER TYPE: Prepaid

DETAIL ACCESS

ALLOWED SSID LIST: Prepaid_SSID

DETAIL SERVICE

VALIDITY: 30 Day(s)
□ No Limit

DATA QUOTA (MB): 10000
□ No Limit

BANDWIDTH UPLOAD LIMIT (Kbps): 5000
□ No Limit

BANDWIDTH DOWNLOAD LIMIT (Kbps): 5000
□ No Limit

ALLOWED SSID LIST: Assign the prepaid service to the pre-configured SSID

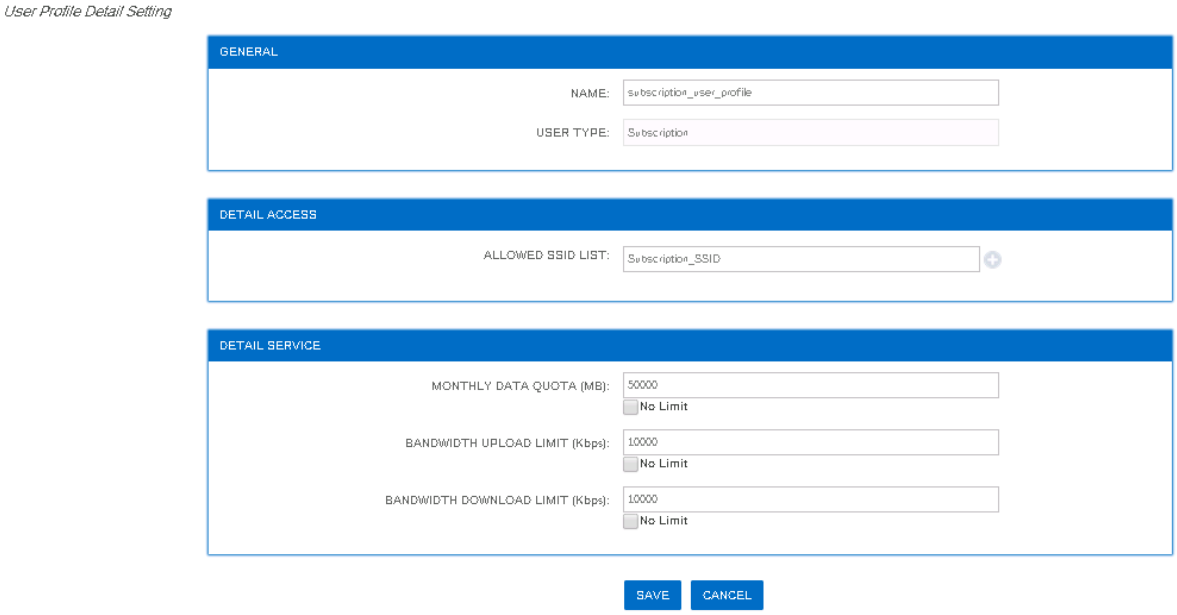
VALIDITY: Set time limit in Day(s), Hour(s) or Minute(s) to the users who apply this user profile. This option will be greyed out if the box of "No Limit" is checked

DATA QUOTA (MB): Set data limit in MB to the users who apply this user profile. This option will be greyed out if the box of "No Limit" is checked

BANDWIDTH UPLOAD LIMIT (kbps): Set uplink speed in kbps to the users who apply this user profile. This option will be greyed out if the box of "No Limit" is checked

BANDWIDTH DOWNLOAD LIMIT (kbps): Set downlink speed in kbps to the users who apply this user profile. This option will be greyed out if the box of "No Limit" is checked

7. Below is the screenshot for the configuration of subscription model.



User Profile Detail Setting

GENERAL

NAME: subscription_user_profile

USER TYPE: Subscription

DETAIL ACCESS

ALLOWED SSID LIST: Subscription_SSID

DETAIL SERVICE

MONTHLY DATA QUOTA (MB): 50000
□ No Limit

BANDWIDTH UPLOAD LIMIT (Kbps): 10000
□ No Limit

BANDWIDTH DOWNLOAD LIMIT (Kbps): 10000
□ No Limit

ALLOWED SSID LIST: Assign the subscription (postpaid) service plan to the pre-configured SSID

MONTHLY DATA QUOTA (MB): Set monthly data limit in MB to the subscribers who apply this service plan. This option will be greyed out if the box of "No Limit" is checked

BANDWIDTH UPLOAD LIMIT (kbps): Set uplink speed in kbps to the subscribers who apply this service plan. This option will be greyed out if the box of "No Limit" is checked

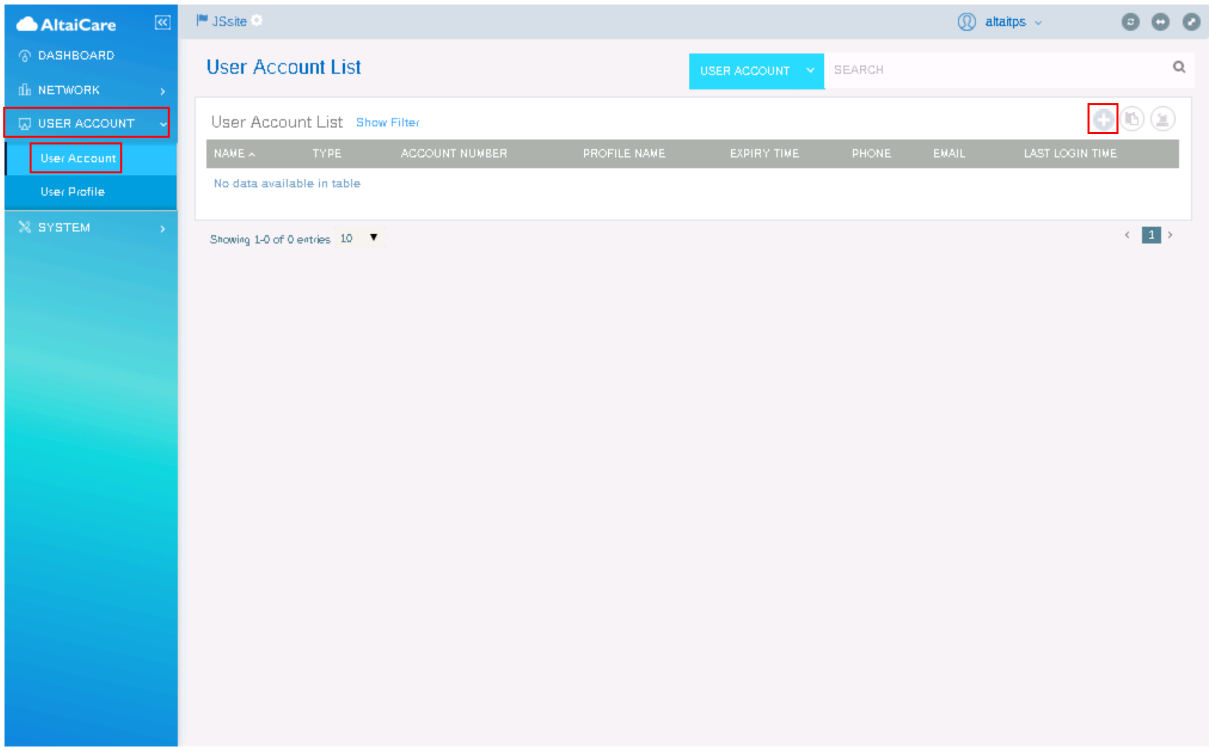
BANDWIDTH DOWNLOAD LIMIT (kbps): Set downlink speed in kbps to the subscribers who apply this service plan. This option will be greyed out if the box of "No Limit" is checked

8. Click "SAVE" to finish the configuration of the user profile.

After creating the User Profile, administrators can add user accounts with the user profiles just created in the "User Account" section.

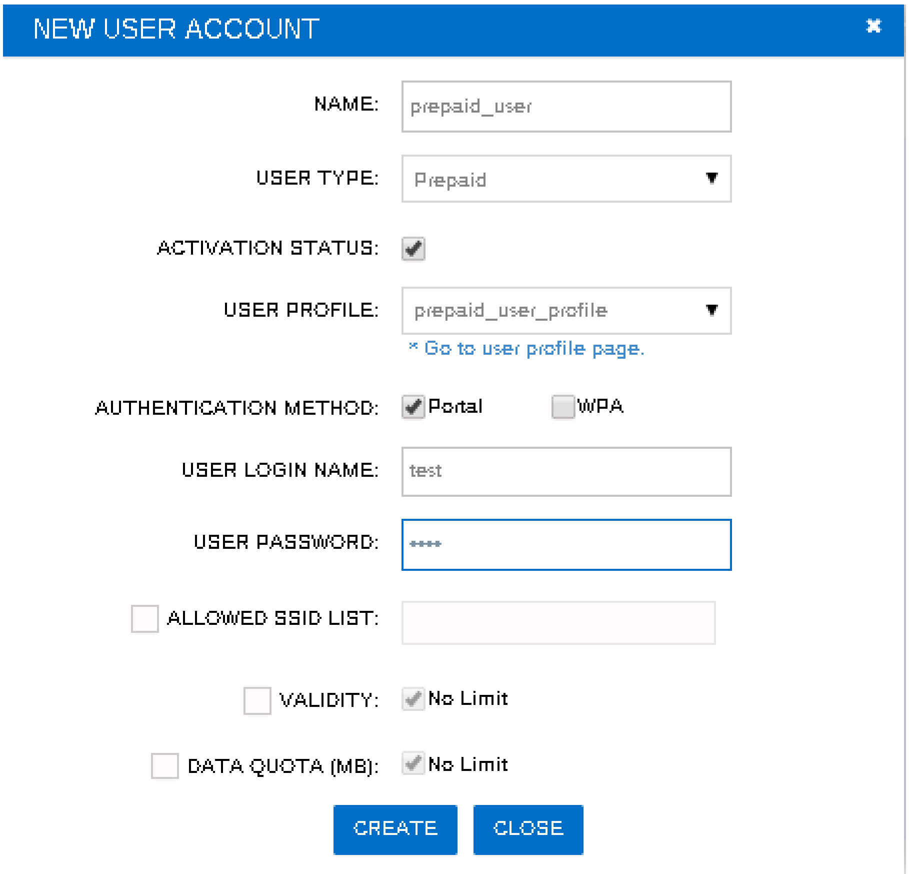
Procedures:

1. Go to select **USER ACCOUNT**->**User Account** on the navigation panel to create a new user account.



2. Click a "Plus" sign as shown in the above screenshot to create a new user account.

3. A pop-up window "NEW USER ACCOUNT" is for user account configuration. Below is the screenshot for the configuration of user account under prepaid model.



NEW USER ACCOUNT

NAME:	prepaid_user
USER TYPE:	Prepaid ▼
ACTIVATION STATUS:	☑
USER PROFILE:	prepaid_user_profile ▼ * Go to user profile page.
AUTHENTICATION METHOD:	☑ Portal ☐ WPA
USER LOGIN NAME:	test
USER PASSWORD:	••••
☐ ALLOWED SSID LIST:	
☐ VALIDITY:	☑ No Limit
☐ DATA QUOTA (MB):	☑ No Limit

NAME: Name for the user account

USER TYPE: Prepaid/Subscription for the user account

ACTIVATION STATUS: With the box checked, the account will be activated; otherwise, the service will be deactivated.

USER PROFILE: Assign the user profile just created to the user account

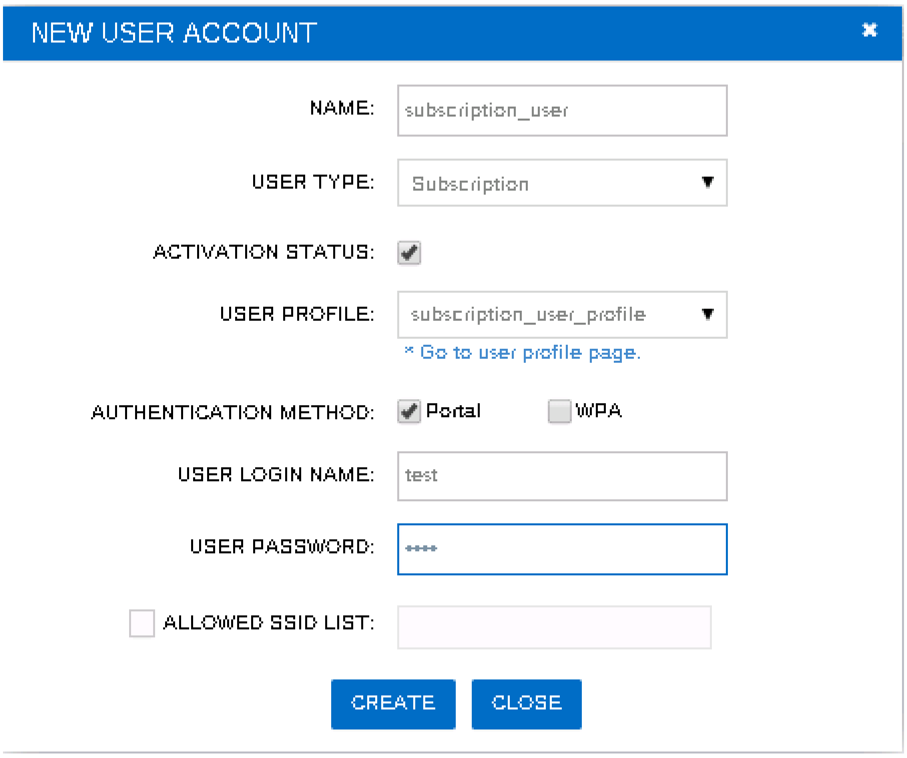
AUTHENTICATION METHOD: Two option available for using the user data base service: 1) Portal; and 2) WPA

USER LOGIN NAME: user login name for the above selected authentication method

USER PASSWORD: user password for the above selected authentication method

The settings of **ALLOWED SSID LIST**, **VALIDITY**, **DATA QUOTA (MB)** are optional. If the boxes to the left of the concerned items are checked, those settings will be overwritten by the configuration of the User Profile; otherwise, administrators can assign specific settings in those items by unchecking the boxes for specific users.

4. Similar configuration can be set up for subscription based user account. Below is the screenshot for the configuration of user account under subscription (postpaid) model.



NEW USER ACCOUNT

NAME: subscription_user

USER TYPE: Subscription

ACTIVATION STATUS: ☑

USER PROFILE: subscription_user_profile

* Go to user profile page.

AUTHENTICATION METHOD: ☑ Portal ☐ WPA

USER LOGIN NAME: test

USER PASSWORD: ••••

☐ ALLOWED SSID LIST:

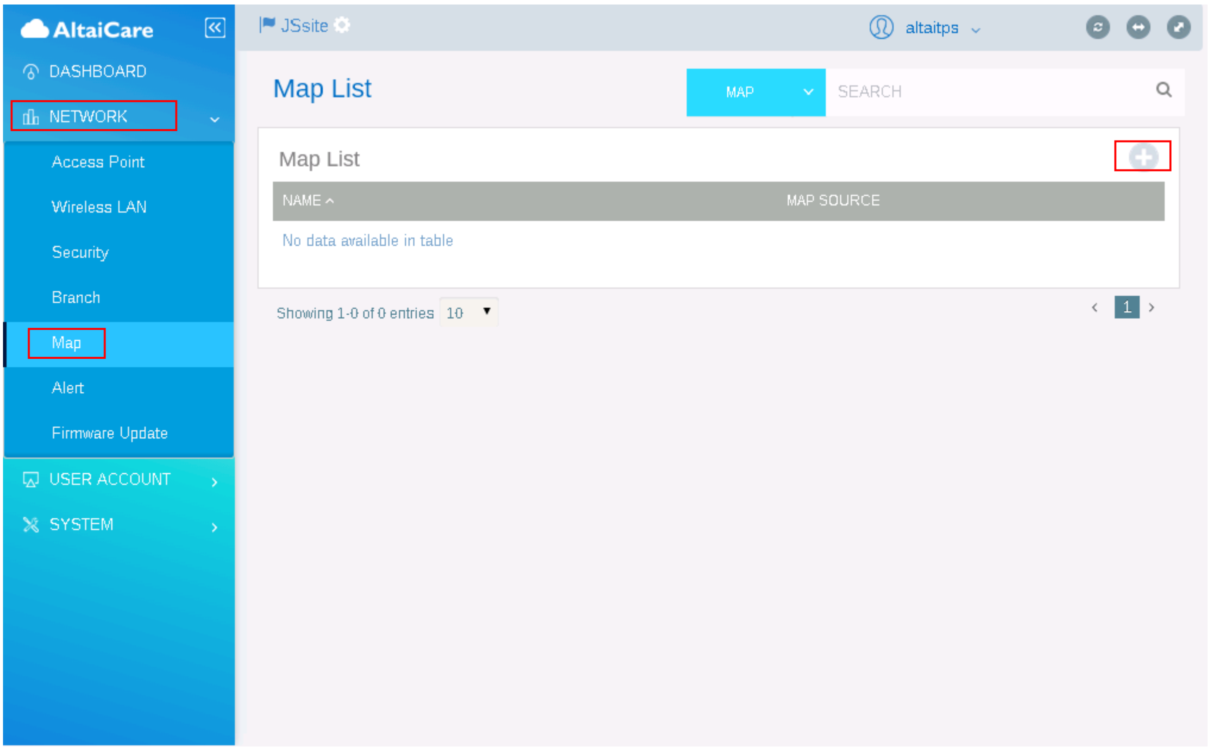
7. Map Management

AltaiCare supports Map Management which allows the users to insert maps for easier AP management and monitoring.

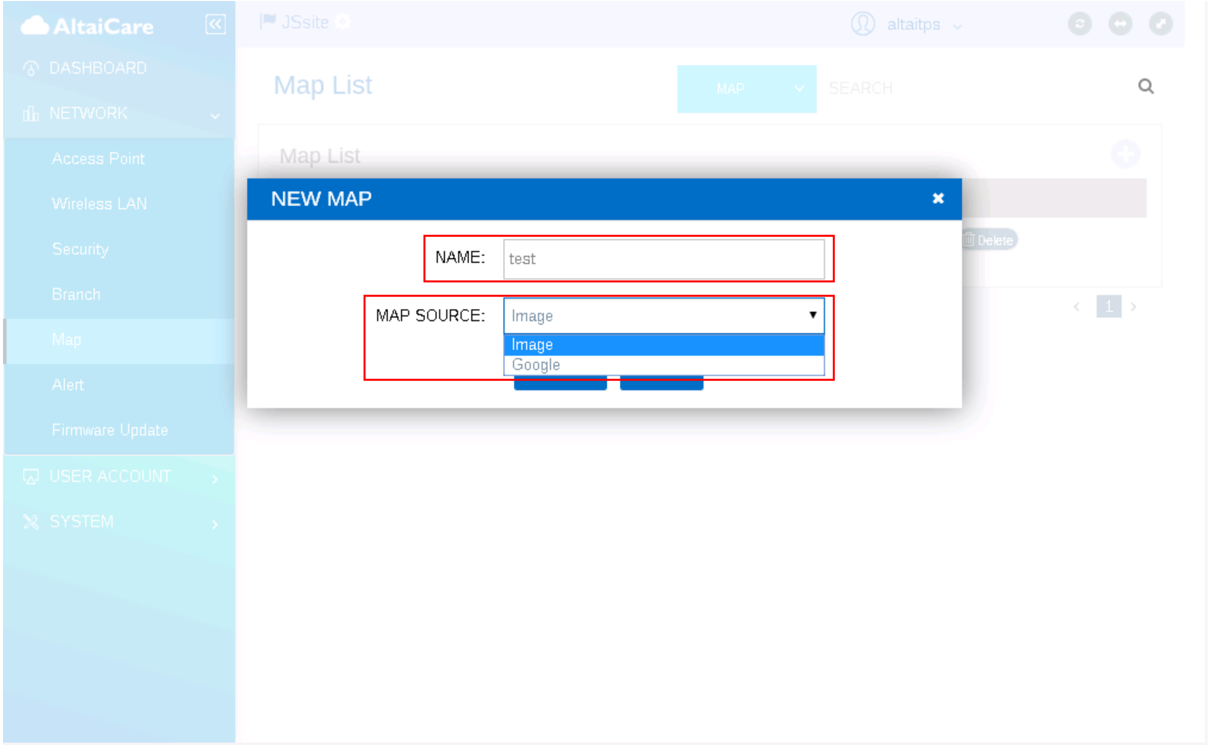
7.1. Map Entry Creation

Procedures:

1. Go to Select **NETWORK**->**Map** on the navigation panel.



2. Click a "Plus" sign as shown in the above screenshot to create a new map entry.
3. Fill in the "NAME" and "MAP Source" fields in the pop-up window "NEW MAP" for map entry configuration. Administrators can have two options for "MAP Source": 1) Image; and 2) Google. The first option "Image" can let administrators upload their preferred maps, i.e. indoor building layout. The second option "Google" can let administrators select Google Map as a map image source.



NAME: test

MAP SOURCE: Image

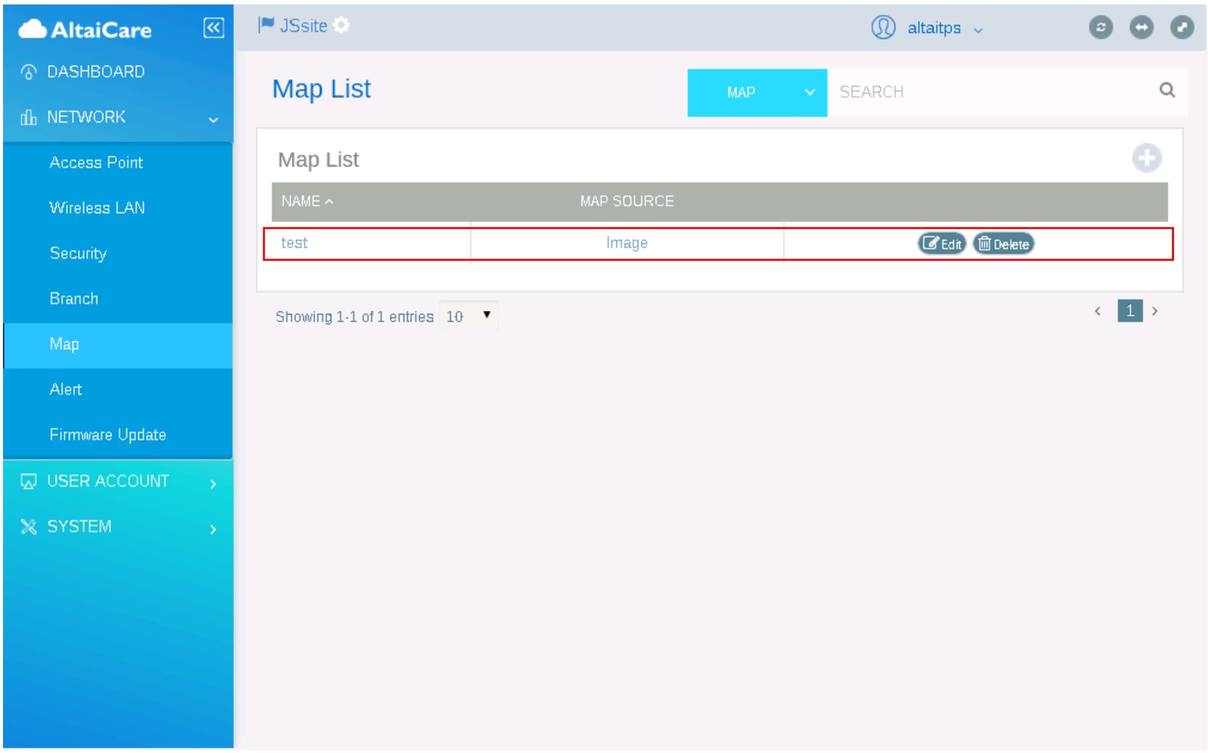
4. Click “CREATE” to finish the setting on the new map entry.

7.2. Map Insertion and Configuration

There will be a new map entry created just after the procedures as described in Section 7.1.

Procedures for the option of “uploaded Image” as Map Source:

1. Click “Edit” to insert the required map image.

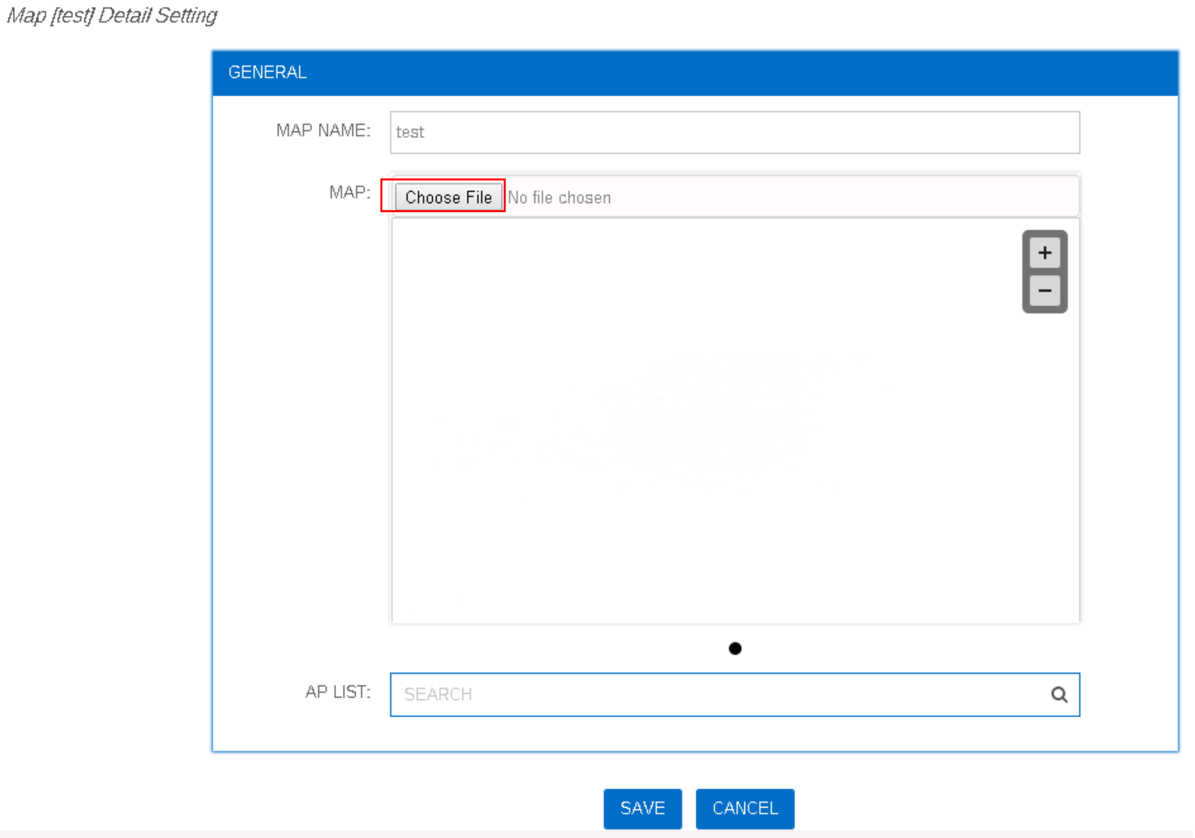


Map List

NAME ^	MAP SOURCE
test	Image

Showing 1-1 of 1 entries 10

2. Click "Choose File" to upload the required image. Be reminded that the image size should not exceed 1024KB.



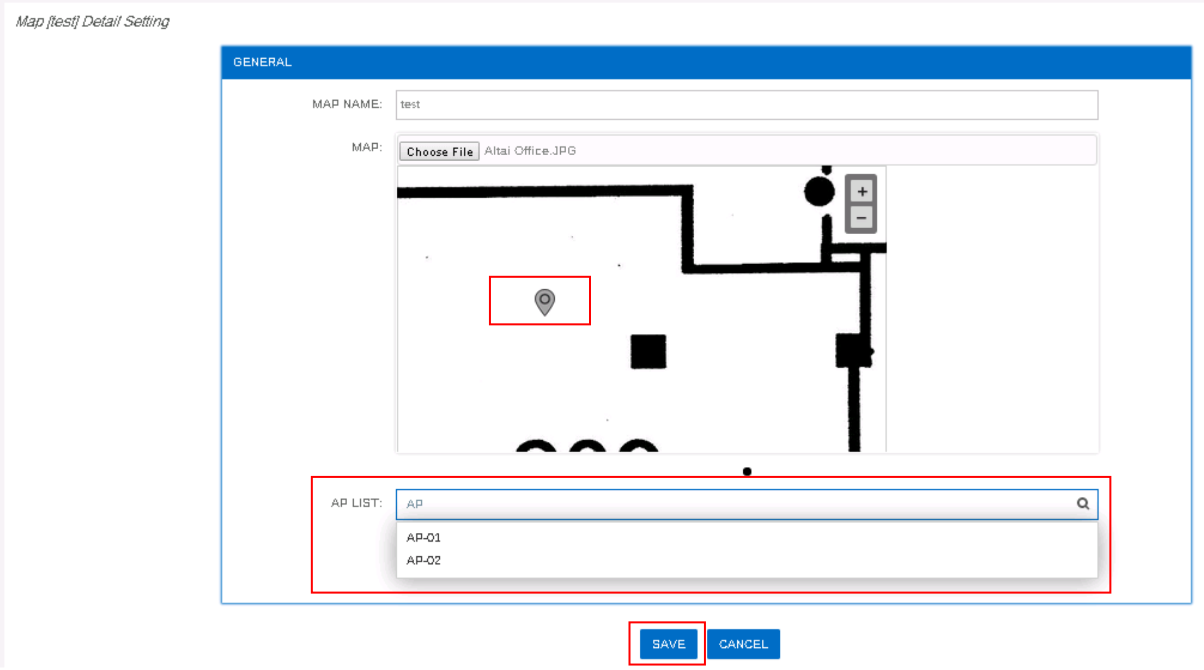
Map [test] Detail Setting

MAP NAME: test

MAP:

AP LIST:

3. Put AP on the map. Administrators can make use of the search box which supports wildcard searching with AP-related information, i.e. AP MAC address, AP name… to select the target AP and put it on the map. An AP icon will be created immediately on the map. Administrators can drag the AP icon on the map for its desired location.



Map [test] Detail Setting

GENERAL

MAP NAME: test

MAP: Choose File Altai Office.JPG

AP LIST: AP

AP-01

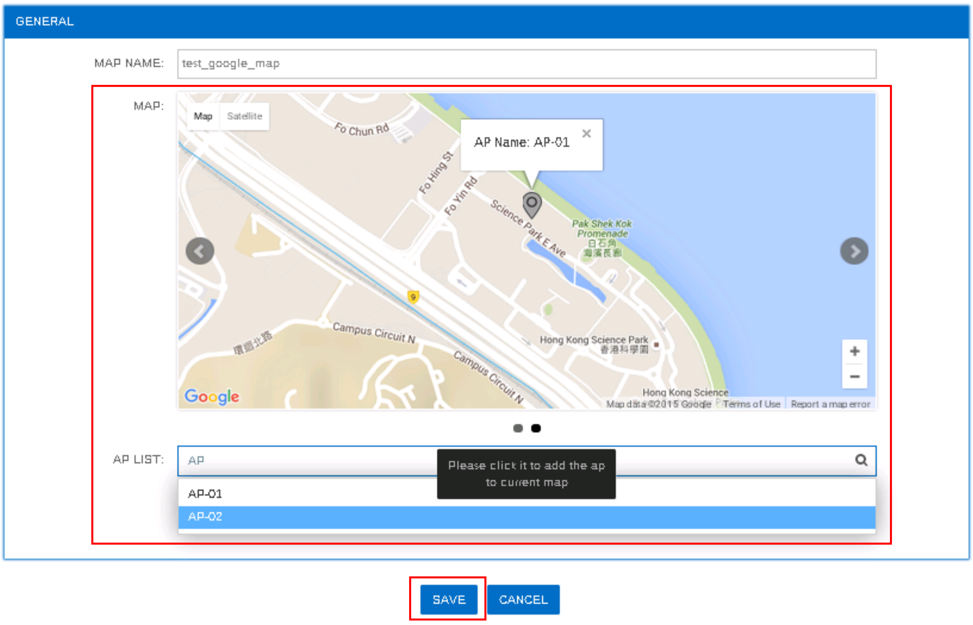
AP-02

4. Click “SAVE” to finish the map configuration.

Procedures for the option of “Google Map” as Map Source:

1. Administrators can follow similar procedures as described above for “Google Map” configuration.

Map [test_google_map] Detail Setting



GENERAL

MAP NAME: test_google_map

MAP:

AP Name: AP-01

AP LIST: AP

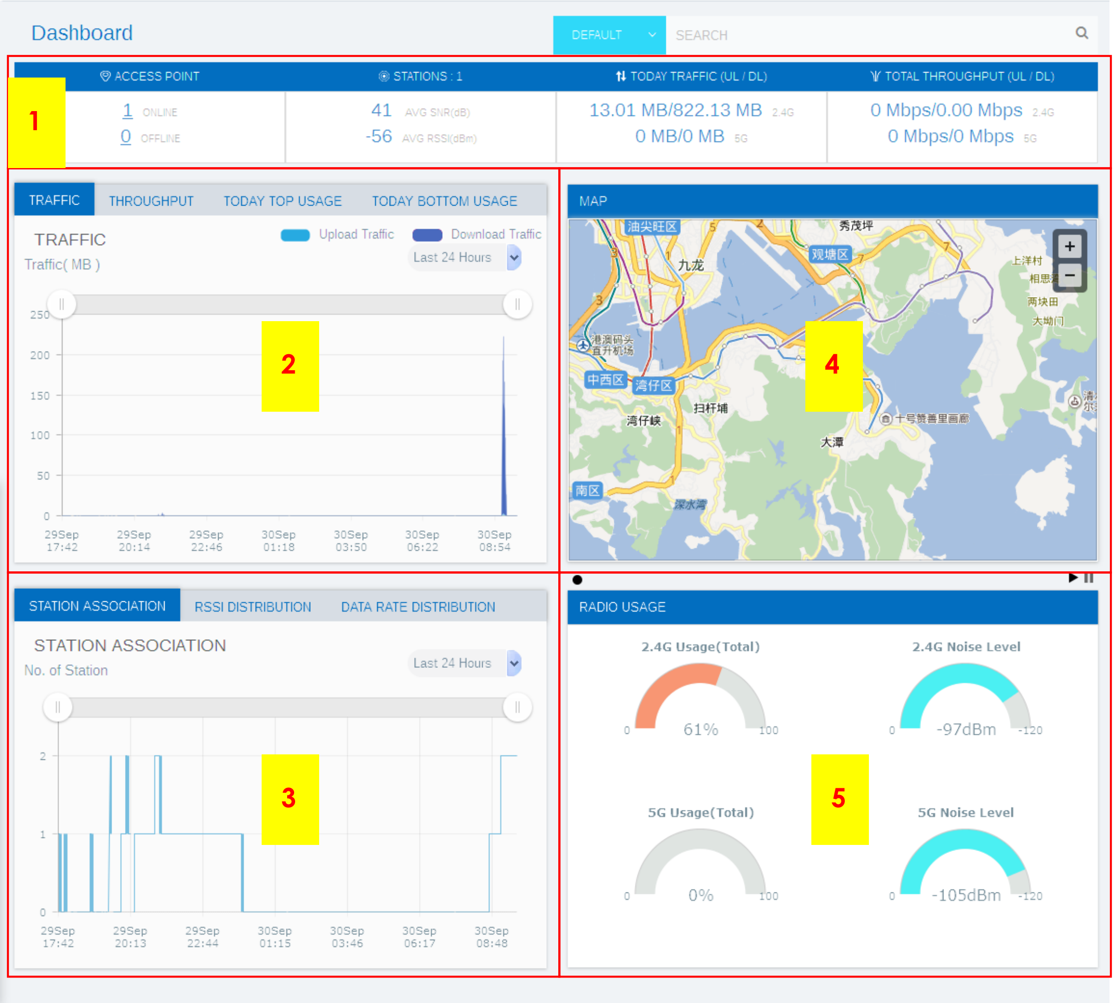
AP-01

AP-02

Please click it to add the ap to current map

8. Performance Monitoring (Dashboard)

Go to **DASHBOARD** on the navigation panel. This page will show the global view for the whole network for monitoring.



Dashboard

DEFAULT | SEARCH

ACCESS POINT	STATIONS : 1	TODAY TRAFFIC (UL / DL)	TOTAL THROUGHPUT (UL / DL)
1 ONLINE 0 OFFLINE	41 AVG SNR(dB) -56 AVG RSSI(dBm)	13.01 MB/822.13 MB 2.4G 0 MB/0 MB 5G	0 Mbps/0.00 Mbps 2.4G 0 Mbps/0 Mbps 5G

There are five sub-panels to show summarize the site-based network status: 1) overall current network statistics; 2) network historical statistics; 3) station association statistics; 4) site map viewer; and 5) radio environment statistics.

Panel 1: Current Network Statistics:

This panel can give Administrators a quick view to check the current network statistics including: 1) number of online/offline AP; 2) current number of stations with average uplink signal strength; 3) today total traffic usage, and 4) current total throughput of the site.

Panel 2: Network Historical Statistics:

There are four windows in this panel: 1) Traffic; 2) Throughput; 3) Today Top Usage; and 4) Today Bottom Usage to summarize the overall network historical statistics.

Traffic and Throughput statistics are mainly represented by charts in different scales: last 24 hours, last 1 month or last 12 months. Administrators can even make use of the time span control to look for granular details of the statistics of total network traffic amount and throughput.

The last two windows will sort out the 5 AP with the top/bottom usage in that day of operation.

Panel 3: Station Association Statistics:

This panel has three windows to show different station association statistics. The first window is about the number of station association number in the past 24 hours, 1 month or 12 months. Administrators can make use of the time span control to look for granular details of the variation of the number of associated client over the time.

The second and third windows are about current distribution of station uplink RSSI and data rate.

Panel 4: Site Map Viewer:

For easier AP management and monitoring, the dashboard provides a window for map viewing. Administrators can switch to different maps for different sites monitoring.

Panel 5: Radio Environment Statistics:

This panel summarizes the wireless condition for the whole site like 2.4G/5G air time percentage and noise level which are particularly useful for wireless-oriented troubleshooting.

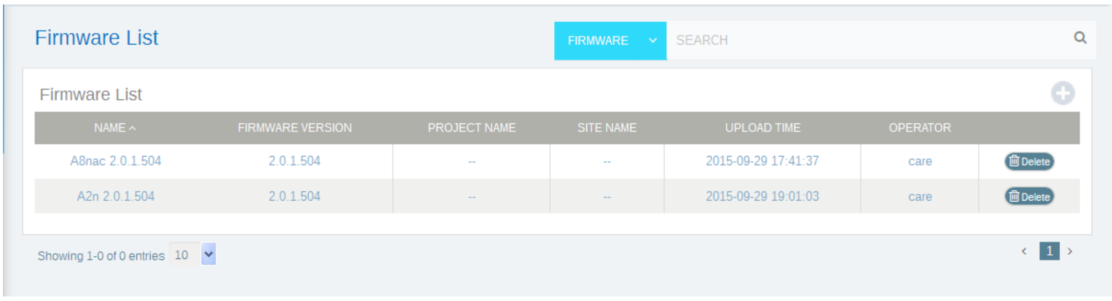
All the statistics are refreshed automatically in Dashboard, to refresh manually please use the refresh button on the top-right corner.

9. System

9.1. Firmware Management

Procedures:

1. Select **SYSTEM**->**Firmware** On the navigation bar



Firmware List

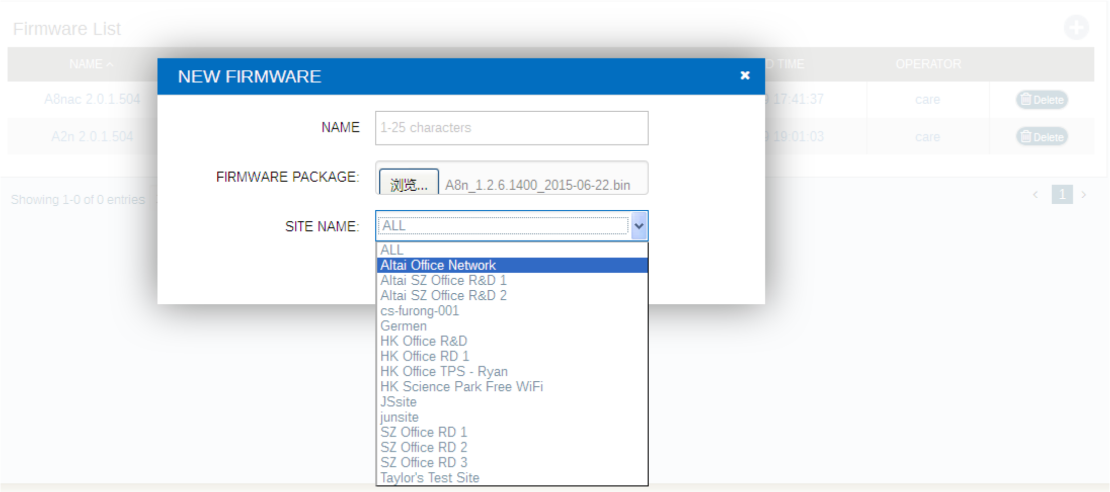
FIRMWARE | SEARCH

Firmware List

NAME ^	FIRMWARE VERSION	PROJECT NAME	SITE NAME	UPLOAD TIME	OPERATOR	
A8nac 2.0.1.504	2.0.1.504	--	--	2015-09-29 17:41:37	care	Delete
A2n 2.0.1.504	2.0.1.504	--	--	2015-09-29 19:01:03	care	Delete

Showing 1-0 of 0 entries 10

2. Use the ⊕ button on right top corner of the Firmware List to add a new firmware



NEW FIRMWARE

NAME: 1-25 characters

FIRMWARE PACKAGE: 浏览... A8n_1.2.6.1400_2015-06-22.bin

SITE NAME: ALL

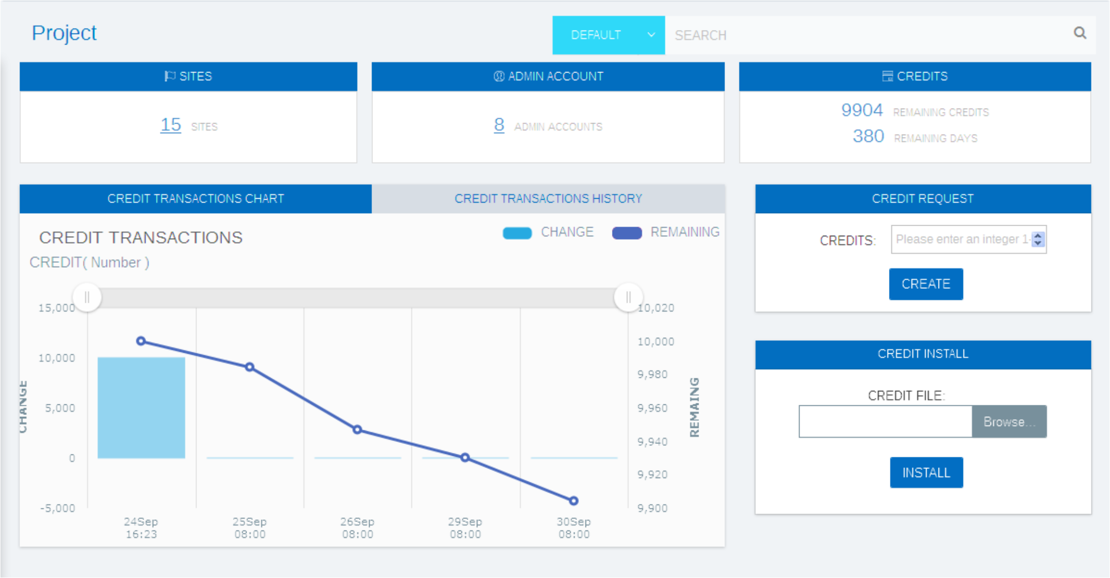
- ALL
- Altai Office Network
- Altai SZ Office R&D 1
- Altai SZ Office R&D 2
- cs-furong-001
- Germen
- HK Office R&D
- HK Office RD 1
- HK Office TPS - Ryan
- HK Science Park Free WiFi
- JSsite
- junsite
- SZ Office RD 1
- SZ Office RD 2
- SZ Office RD 3
- Taylor's Test Site

3. Select the site that the firmware apply to

9.2. Project

Procedures:

1. Select **SYSTEM**->**Project** On the navigation bar, here can see the project detail information.



Project

DEFAULT | SEARCH

SITES: 15 SITES

ADMIN ACCOUNT: 8 ADMIN ACCOUNTS

CREDITS: 9904 REMAINING CREDITS, 380 REMAINING DAYS

CREDIT TRANSACTIONS CHART | CREDIT TRANSACTIONS HISTORY

CREDIT REQUEST

CREDITS: Please enter an integer 1

CREATE

CREDIT INSTALL

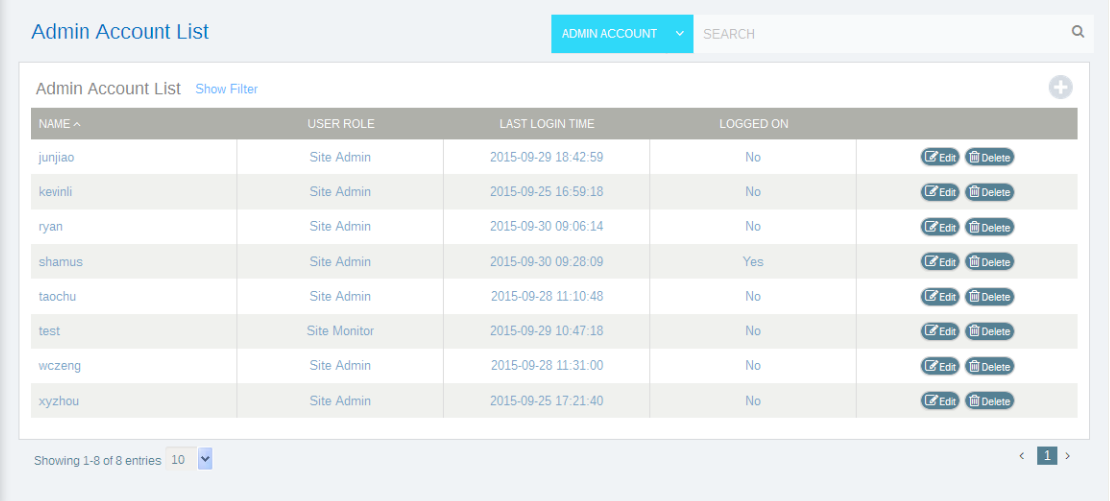
CREDIT FILE: Browse...

INSTALL

9.3. Admin Account

Procedures:

1. Select SYSTEM->Admin Account On the navigation bar



Admin Account List

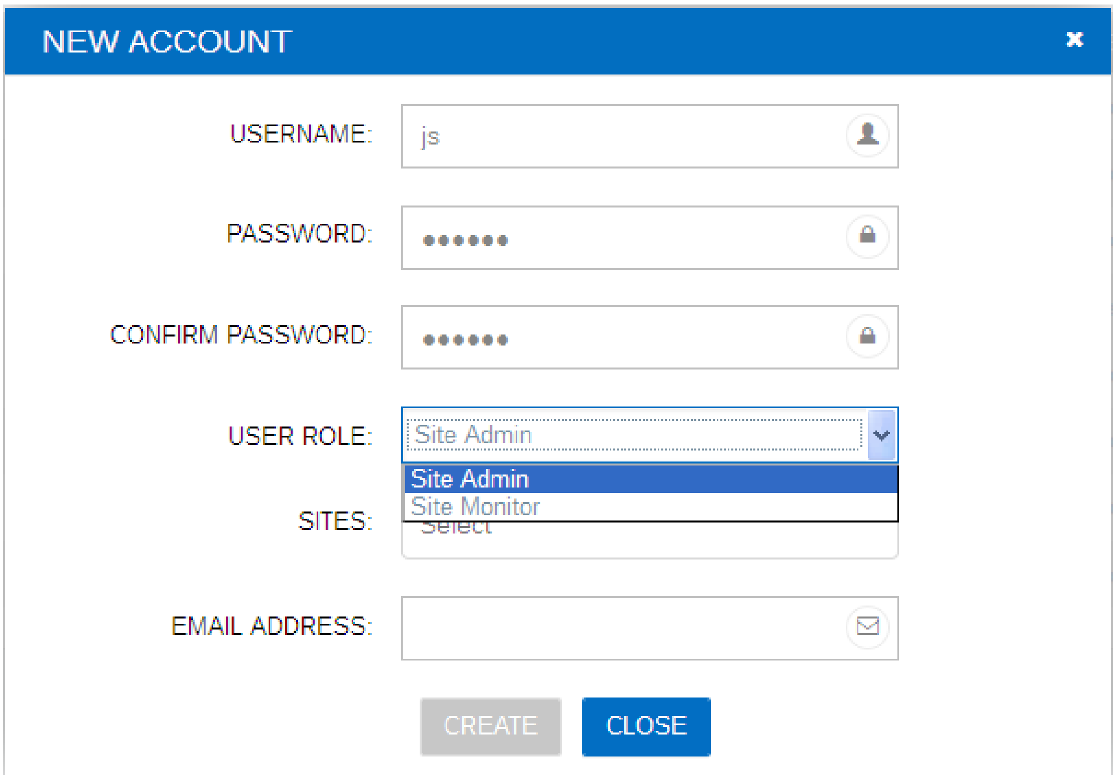
ADMIN ACCOUNT | SEARCH

Admin Account List Show Filter

NAME ^	USER ROLE	LAST LOGIN TIME	LOGGED ON	
junjiao	Site Admin	2015-09-29 18:42:59	No	Edit Delete
kevinli	Site Admin	2015-09-25 16:59:18	No	Edit Delete
ryan	Site Admin	2015-09-30 09:06:14	No	Edit Delete
shamus	Site Admin	2015-09-30 09:28:09	Yes	Edit Delete
taochu	Site Admin	2015-09-28 11:10:48	No	Edit Delete
test	Site Monitor	2015-09-29 10:47:18	No	Edit Delete
wczeng	Site Admin	2015-09-28 11:31:00	No	Edit Delete
xyzhou	Site Admin	2015-09-25 17:21:40	No	Edit Delete

Showing 1-8 of 8 entries 10 ‹ 1 ›

2. Use the ⊕ button on right top corner of the Admin Account List to add a new admin account



NEW ACCOUNT

USERNAME: js

PASSWORD: ●●●●●●

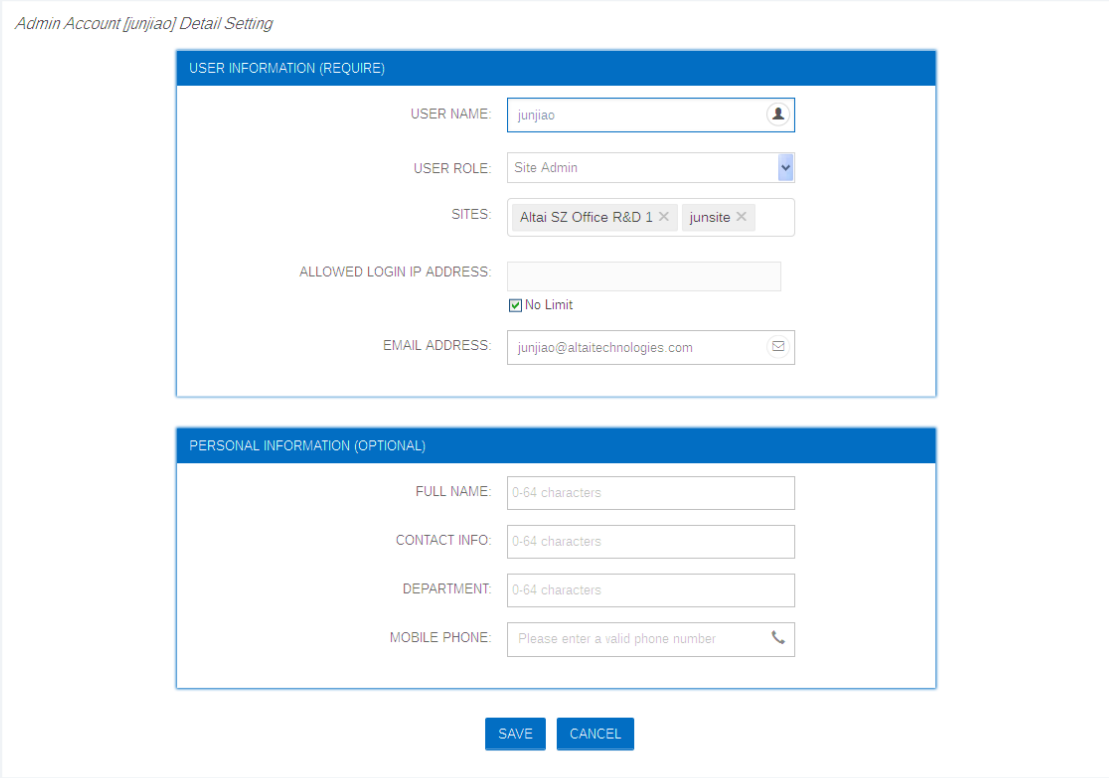
CONFIRM PASSWORD: ●●●●●●

USER ROLE: Site Admin

SITES: Select

EMAIL ADDRESS:

3. Click CREATE to add this admin user
4. Click the Edit button can edit the admin user infomation



Admin Account [junjiao] Detail Setting

USER INFORMATION (REQUIRE)

USER NAME: junjiao

USER ROLE: Site Admin

SITES: Altai SZ Office R&D 1 ✕ junsite ✕

ALLOWED LOGIN IP ADDRESS:

☑ No Limit

EMAIL ADDRESS: junjiao@altaitechnologies.com

PERSONAL INFORMATION (OPTIONAL)

FULL NAME: 0-64 characters

CONTACT INFO: 0-64 characters

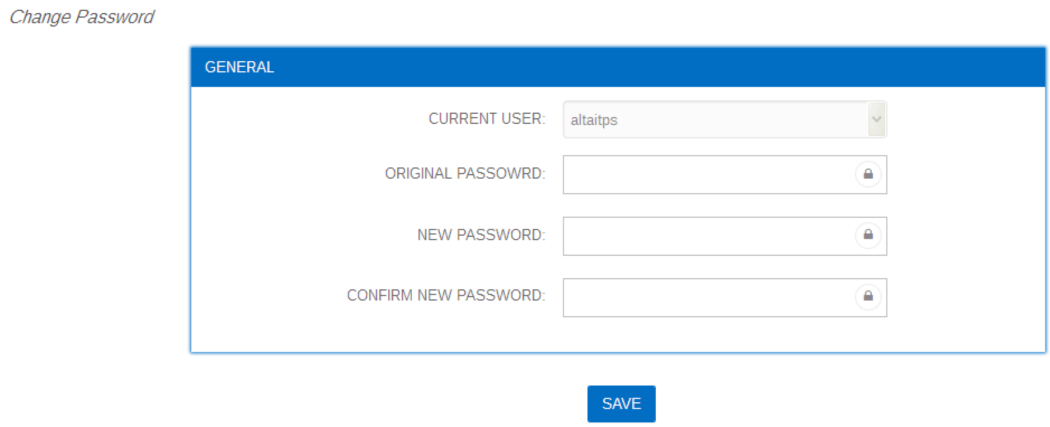
DEPARTMENT: 0-64 characters

MOBILE PHONE: Please enter a valid phone number

9.4. Change Password

Procedures:

1. Select **SYSTEM**->**Change Password** On the navigation bar



Change Password

GENERAL

CURRENT USER: altaitps

ORIGINAL PASSOWRD:

NEW PASSWORD:

CONFIRM NEW PASSWORD:

2. Here we can change the current user password