AltaiCare Training

Version 2.1
August, 2017

ALTAI Super WiFi

Training Content

Item	Topic	Duration	Presented By	Participants	Prerequisite	Preparation Required
1	**AltaiCare Overview**	3 hr	TPS, Altai	Engineers	Basic networking and WiFi knowledge required	1 pcs of AP, AltaiCare account, Internet access for demo if needed
1.1	Wireless Network Management Feature Highlights					
1.2	Service Control Feature Highlights					
2	**Case Study**					
2.1	Typical Network Topology					
2.2	Call Flow for Built-In Portal Auth					
2.3	Call Flow for Built-In RADIUS Auth (WPA)					
2.4	Portal Template Types					
3	**Before You Begin – AP Configuration**					
3.1	Access to AP WebUI					
3.2	Step 1: Network Setting					
3.3	Step 2 (Optional): Management VLAN Setting (Applicable to local VLAN environment only)					
3.4	Step 3: Enable Remote Management					
3.5	Step 4: Save & Apply AP Configuration Change					
4	**Getting Started**					
4.1	AltaiCare Hierarchy Overview					
4.2	Multiple Level Access Control					
4.3	AltaiCare Credit System and Policy					
4.4	Access to AltaiCare					
4.5	AltaiCare Web Interface					
4.6	Wireless Management Overview					
4.7	Service Management Overview					
4.8	Project Management Overview					

Training Content

Item	Topic	Duration	Presented By	Participants	Prerequisite	Preparation Required
5	**Basic Configuration**	3 hr	TPS, Altai	Engineers	Basic networking and WiFi knowledge required	1 pcs of AP, AltaiCare account, Internet access for demo if needed
5.1	Configuration Procedures					
5.2	Step 1: Create new Site					
5.3	Step 2: Create new Service Domain					
5.4	Step 3: Create Admin Account for Site/Service Domain					
5.5	Step 4: Create User Group					
5.6	Step 5: Create User Account					
5.7	Step 5a: Create Single User Account					
5.8	Step 5b: Create Single MAC Account					
5.9	Step 5c: Batch import (in .CSV file) of user accounts					
5.10	Step 5d: Voucher-based user account batch generation					
5.11	Step 6a: Custom Template Portal Setup					
5.12	Step 6b: User Defined Template Portal Setup					
5.13	Step 7a: Create Security Profile for Portal					
5.14	Step 7b: Create Security Profile for WPA					
5.15	Step 7c: Create Security Profile for MAC Auth					
5.16	Step 7d: Create Security Profile for WPA-PSK					
5.17	Step 8: Create SSID (WLAN)					
5.18	Step 9: AP Registration					
5.19	Step 9a: Single AP Registration					
5.20	Step 9b: AP Batch Registration					
6	**AP Firmware Update**					
6.1	AP Firmware Compatibility Check					
6.2	Single AP Firmware Update					
6.3	AP Batch Firmware Update					

Training Content

Item	Topic	Duration	Presented By	Participants	Prerequisite	Preparation Required
7	**Verification**	3 hr	TPS, Altai	Engineers	Basic networking and WiFi knowledge required	1 pcs of AP, AltaiCare account, Internet access for demo if needed
7.1	Verification: Custom Template Portal					
7.2	Verification: User Defined Template Portal					
7.3	Verification: WPA – PEAP					
7.4	Verification: MAC Authentication					
7.5	Verification: WPA-PSK					
8	**Advanced Configuration (To be updated in Ver 2.2)**					
8.1	Individual AP Setting					
8.2	Branch Configuration					
8.3	Auto-Fill SSID					
8.4	Access Control List					
8.5	Advertisement Engine					
9	**Statistics Monitoring (To be updated in Ver 2.2)**					
10	**Report Generation (To be updated in Ver 2.2)**					

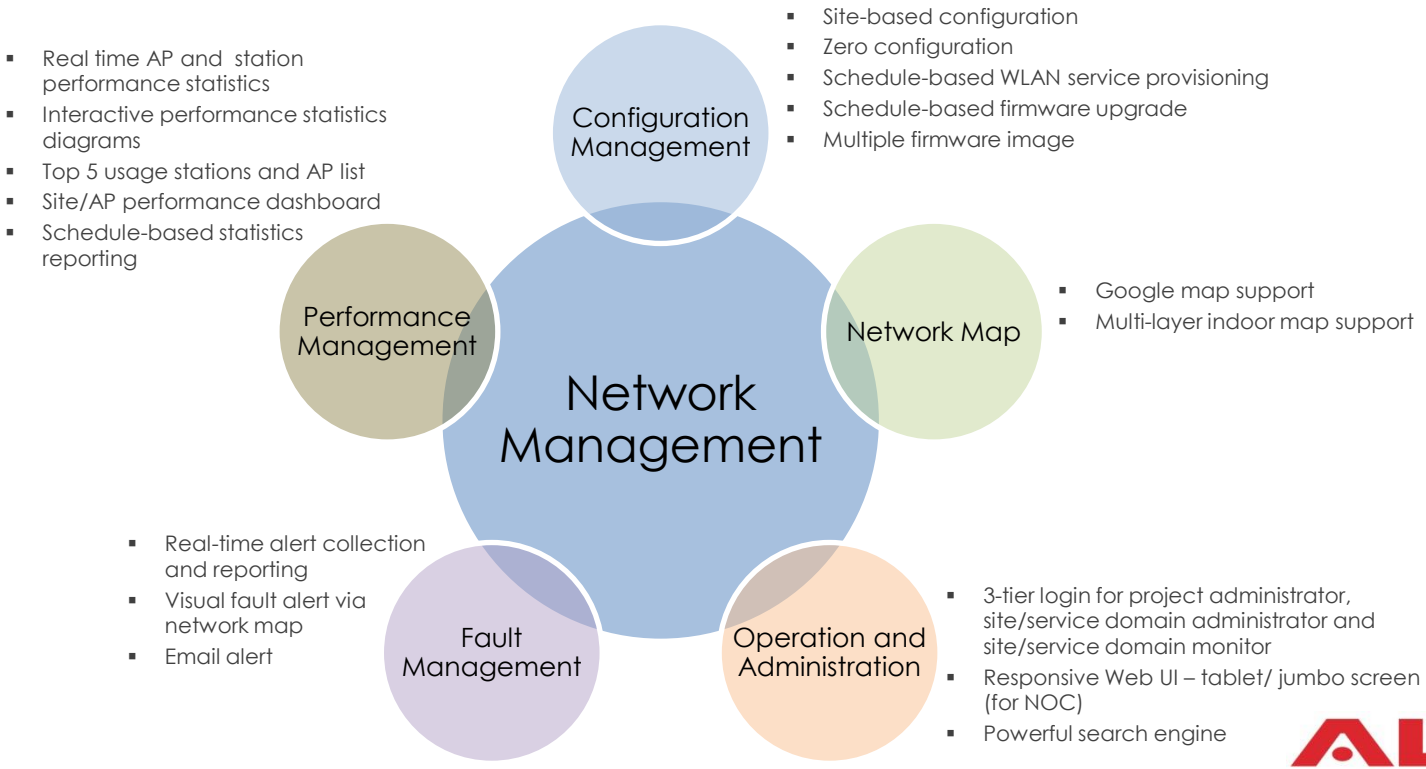
ALTAI Super WiFi

AltaiCare Overview

Wireless Network Management Feature Highlights

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

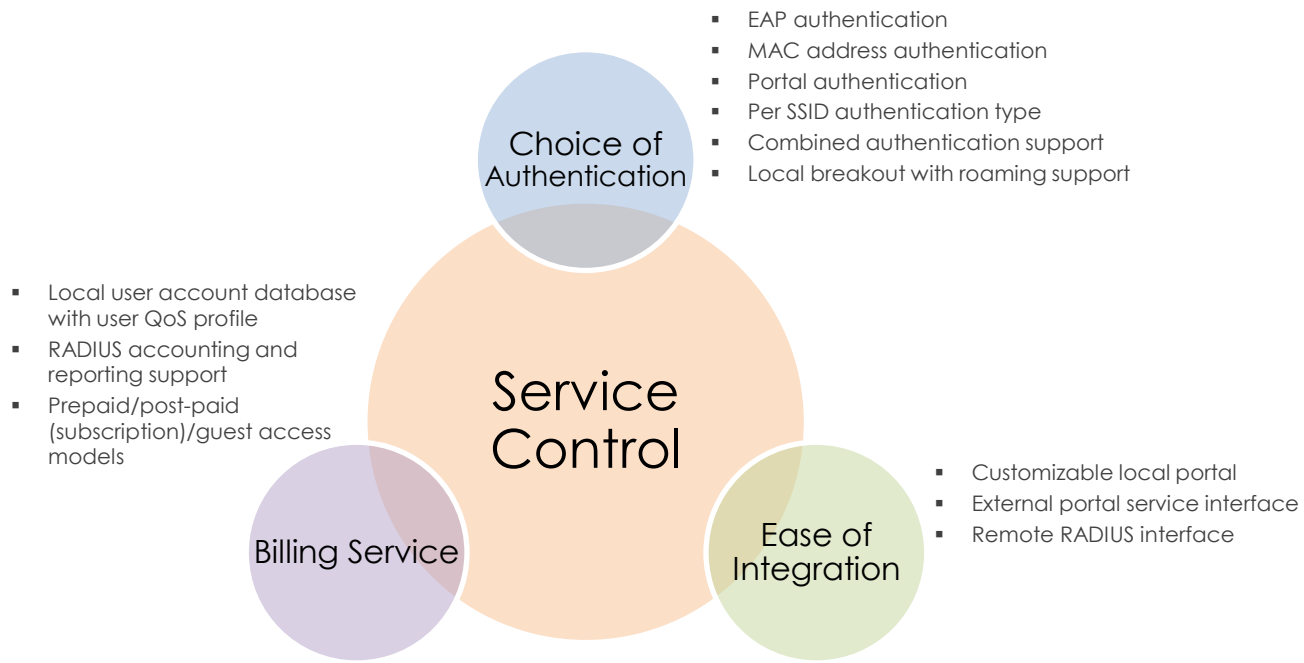
Wireless Network Management Feature Highlights:



ALTAI Super WiFi

Service Control Feature Highlights

Service Control Feature Highlights:

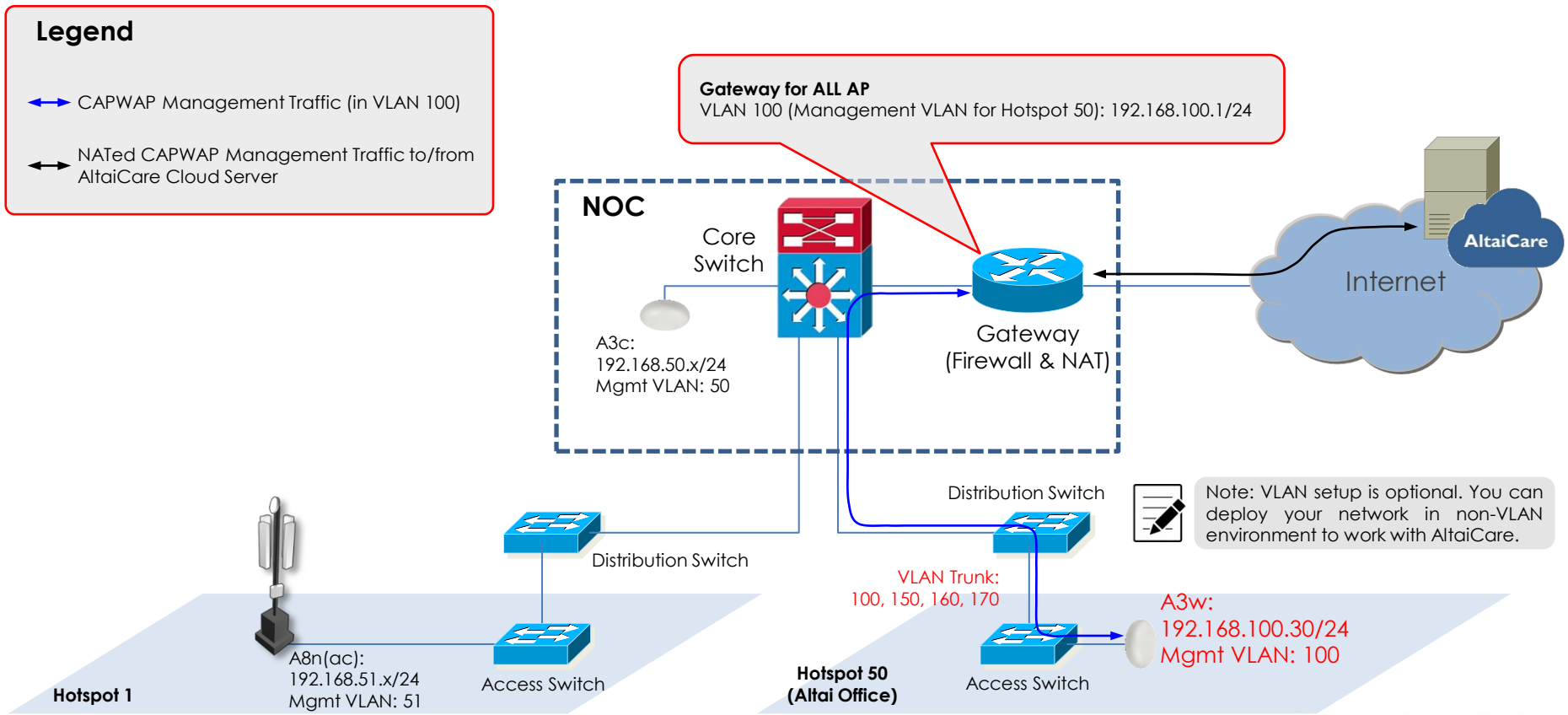


ALTAI Super WiFi

Case Study

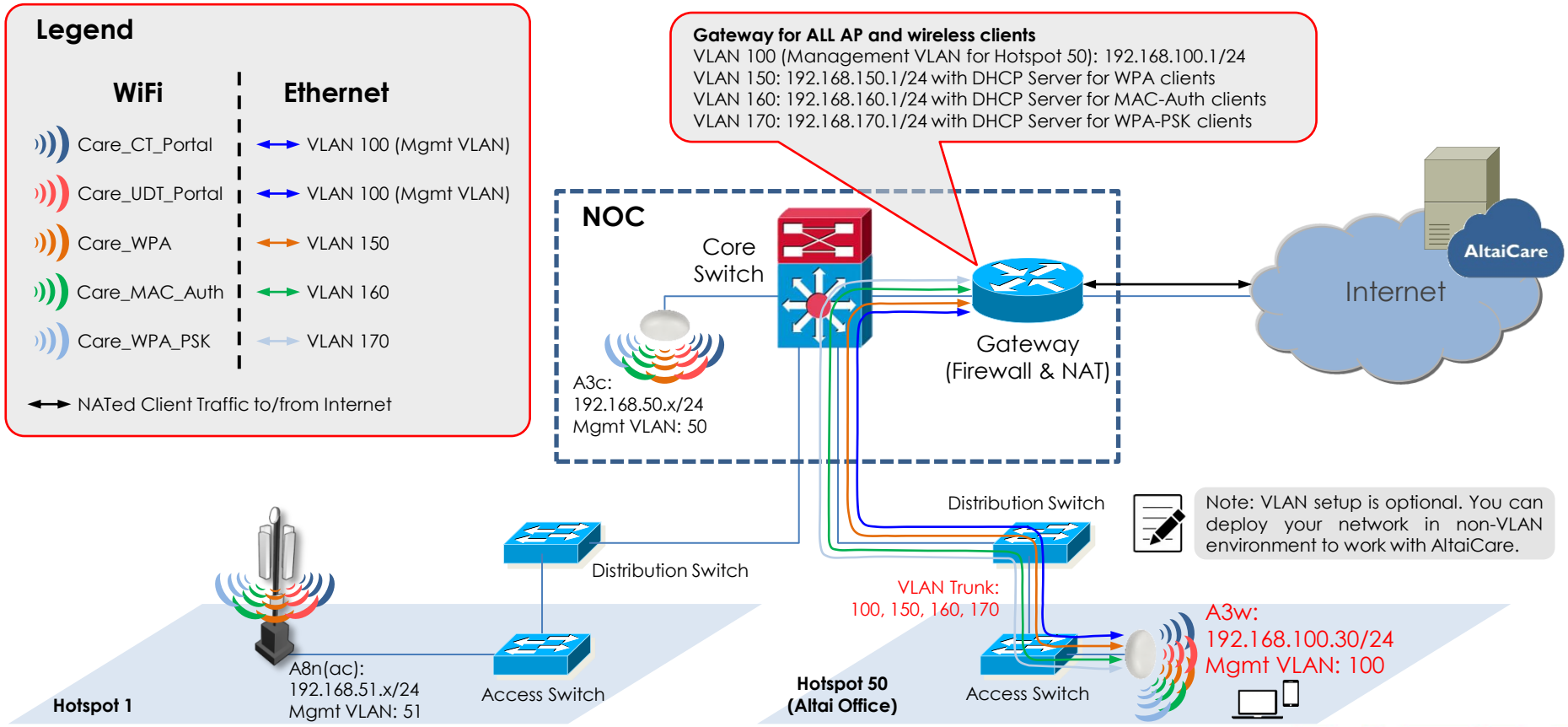
ALTAI Super WiFi

Typical Network Topology and Management Traffic



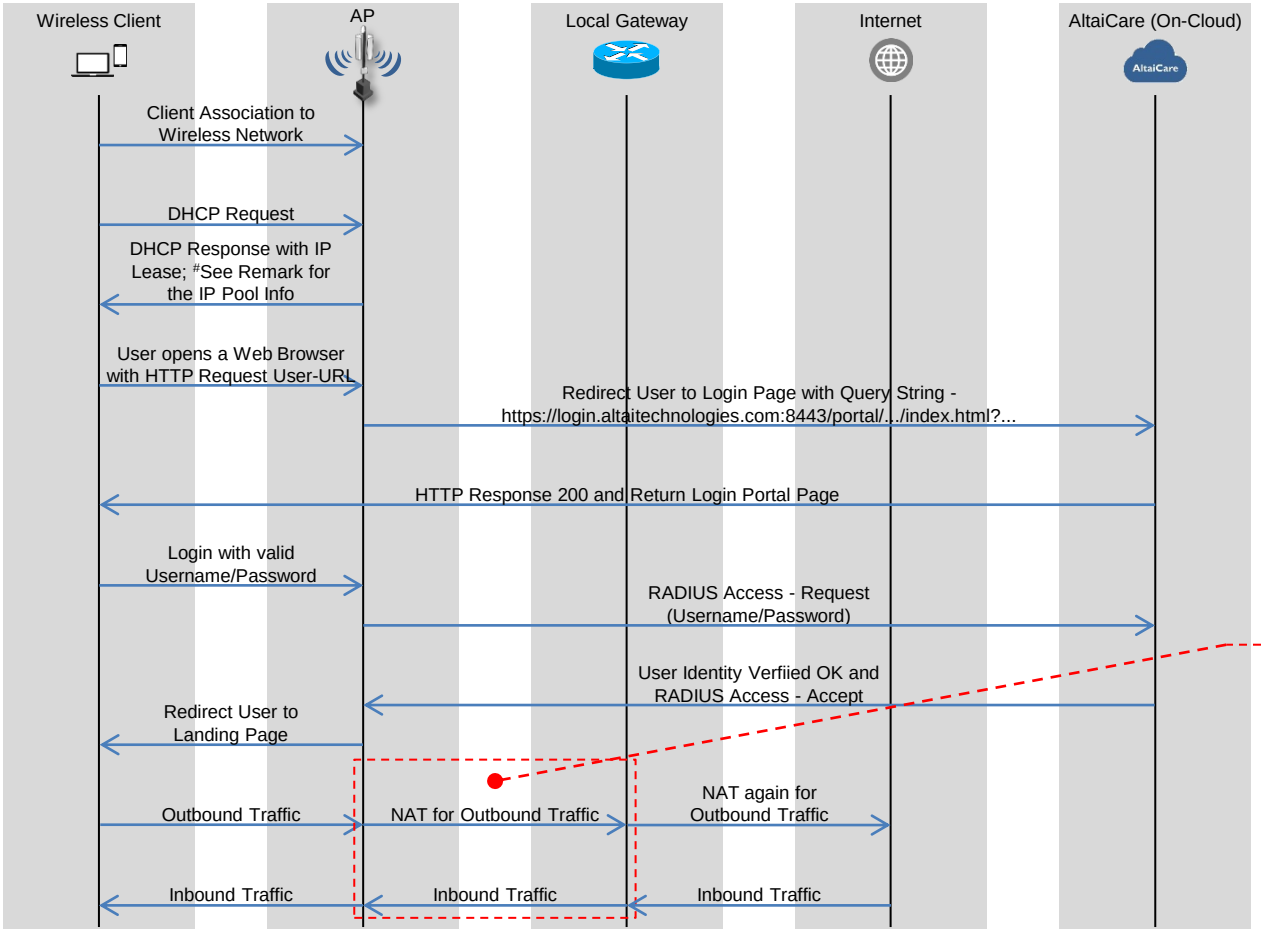
ALTAI Super WiFi

Typical Network Topology and Client Traffic



ALTAI Super WiFi

Call Flow for Built-In Portal Auth



Remark:

AP as #DHCP server, RADIUS client & authenticator, and gateway with NAT for wireless client traffic

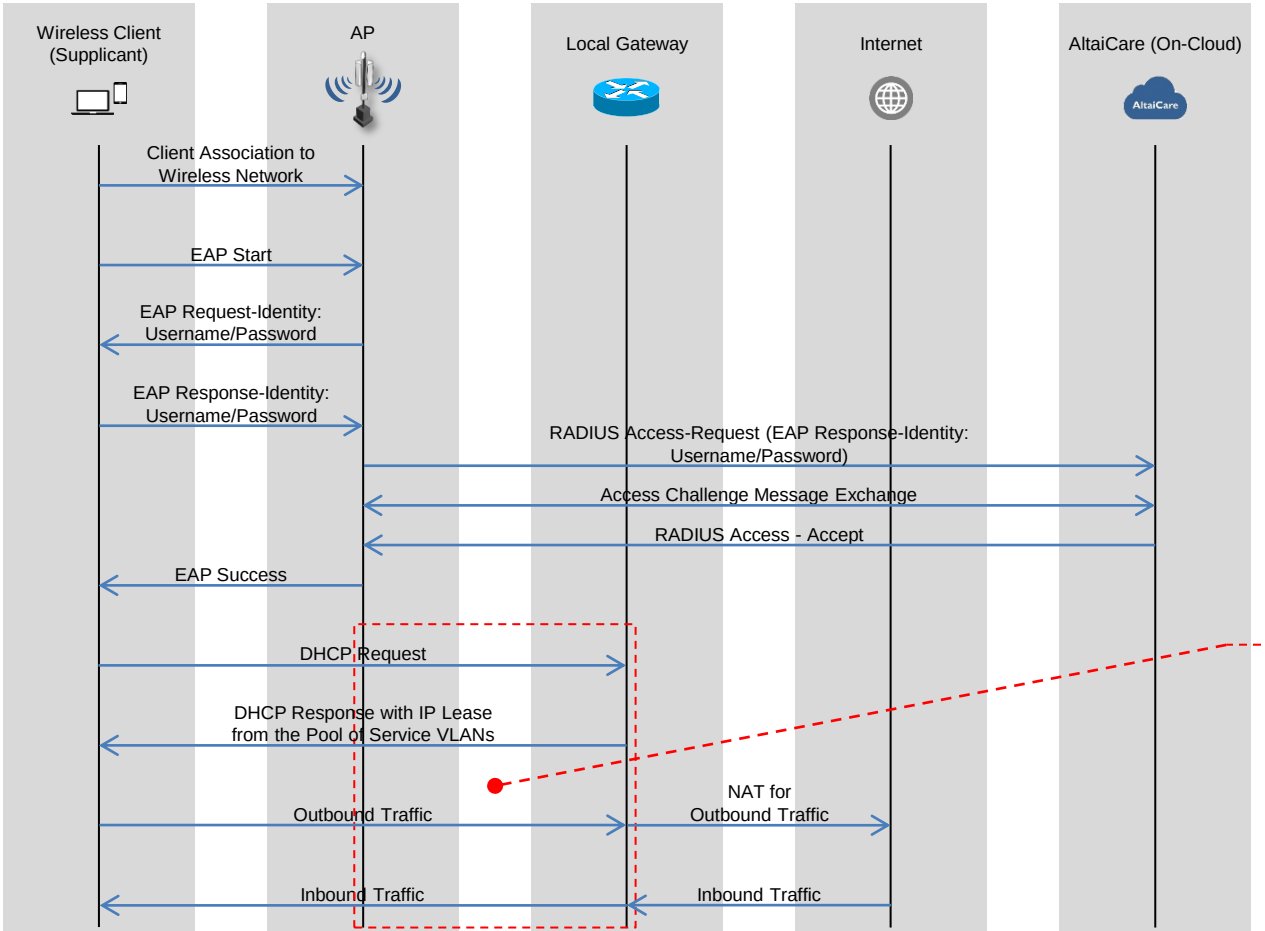
AltaiCare as RADIUS server and web portal hosting server

2.4G and 5G clients will get IP address from the default pools: 192.168.120.0/24 & 192.168.121.0/24 respectively

User Data Traffic running in Management VLAN for VLAN-enabled local network

ALTAI Super WiFi

Call Flow for Built-In RADIUS Auth (WPA)



Remark:

AP as RADIUS client & authenticator

AltaiCare as RADIUS server

Local Gateway as DHCP server for wireless clients and NAT implementation on their traffic

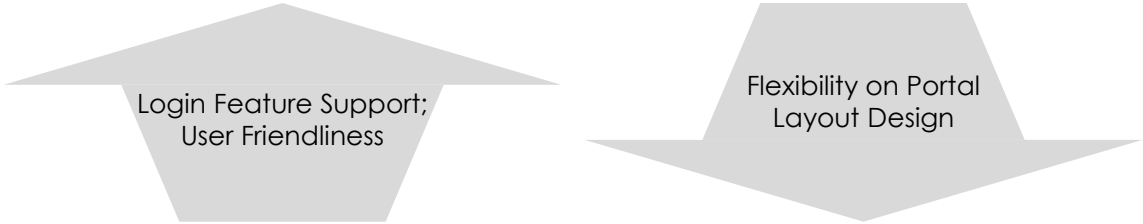
User Data Traffic running in Service VLANs for VLAN-enabled local network

ALTAI Super WiFi

Portal Template Types

- 3 different ways available for portal design. Each one can its own login feature support and advantages.

1. **Custom Template (Built-In)**
2. **User Defined Template (Built-in)**



3. **Package Upload (Built-In/External)**

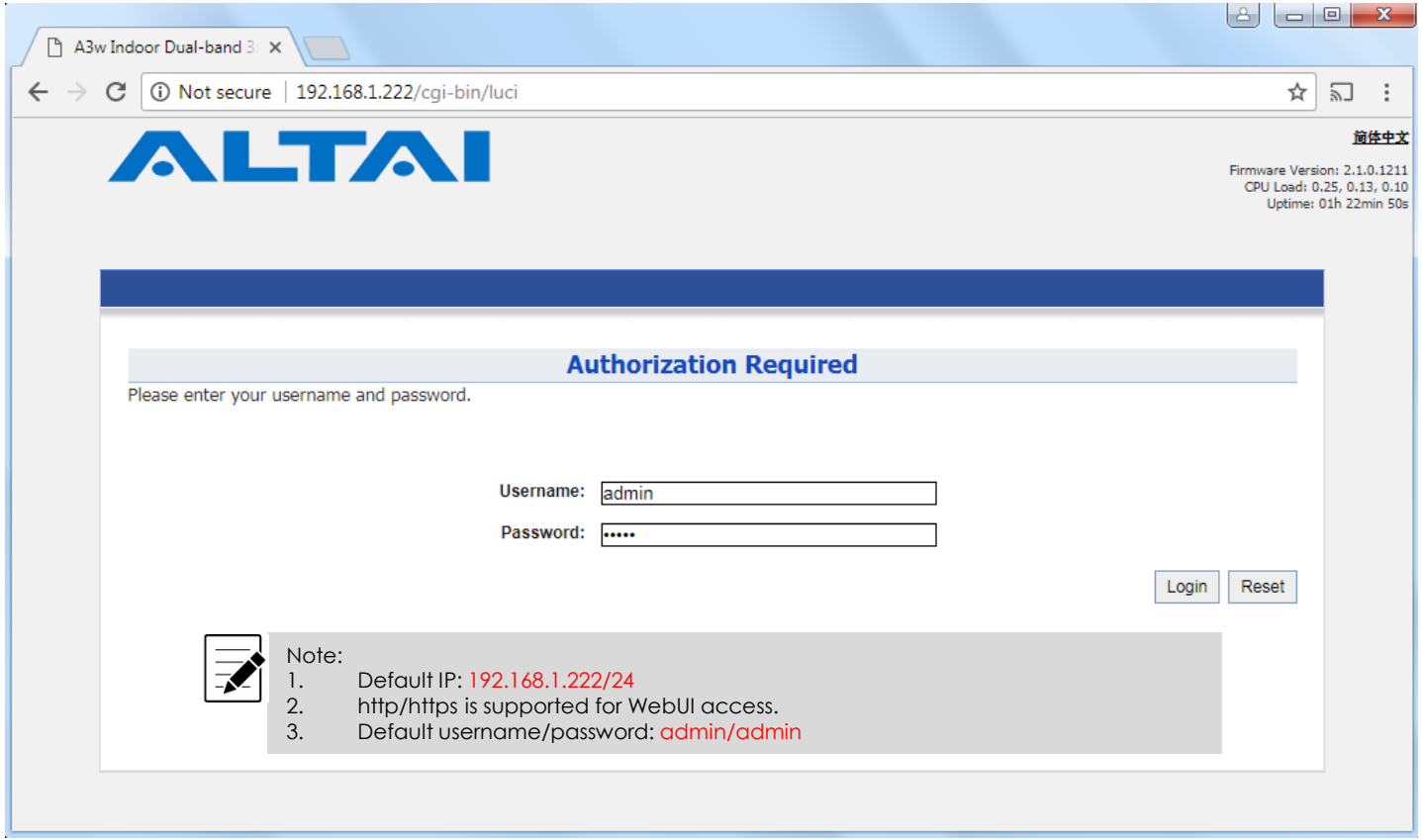
- Below is a table to summarize different login type support for different templates

	Auto-Generated User Account Type					Predefined User Account Type
	Social Account Login		Guest Login (Single Button)	Sign Up Login 1 (with Passcode return for login)	Sign Up Login 2 (no Passcode return required)	User Account Login (Username / Password)
	Facebook	Google		Email		
Custom Template (Built-In)	✓	✓	✓	✓		
User Define Template (Built-In)			✓		✓	✓
Package Upload (Built-In/External)						✓

ALTAI Super WiFi

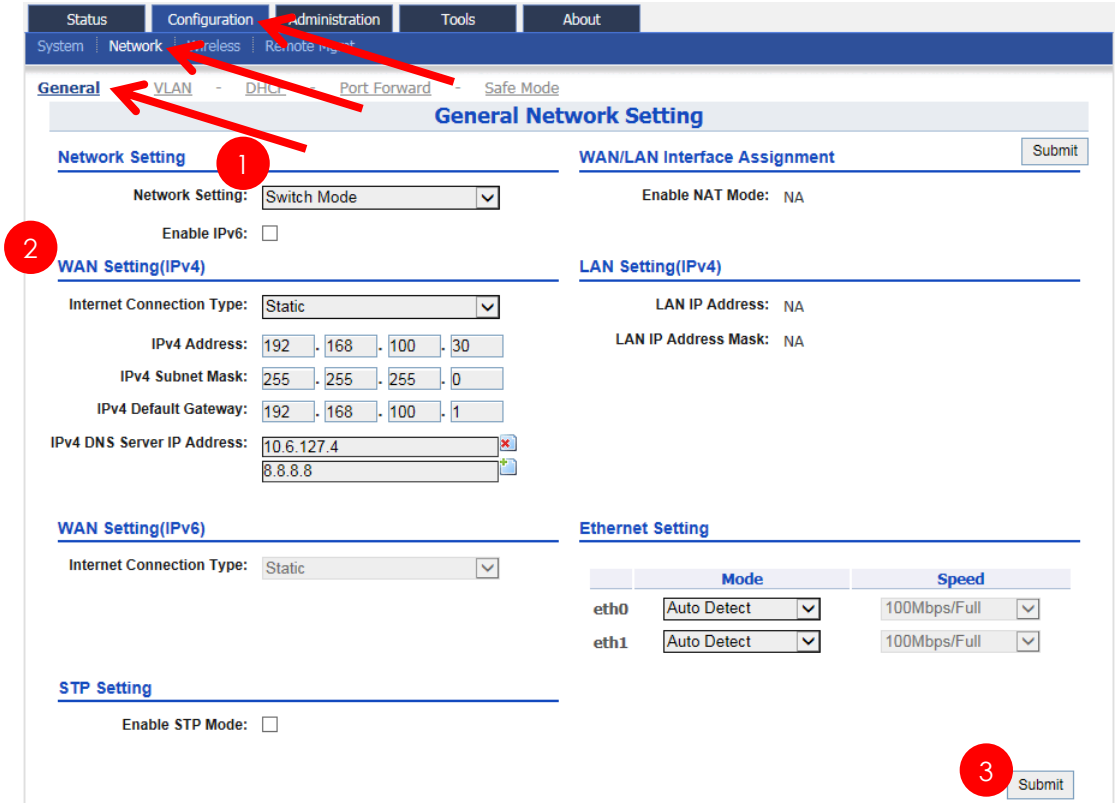
Before You Begin - AP Configuration

Access to AP WebUI



ALTAI Super WiFi

Step 1: Network Setting



Procedures:

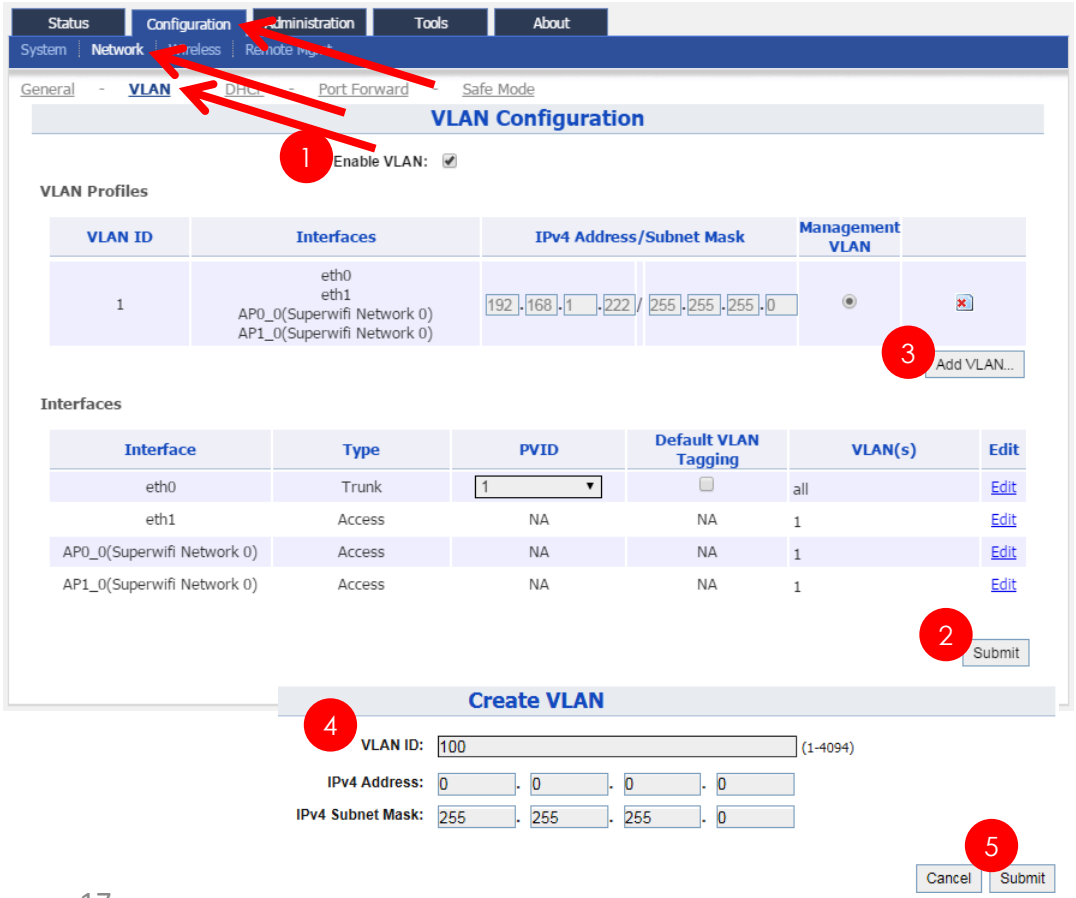
1. Make sure "Switch Mode" is selected as Network Setting
2. Assign **valid** IP settings including **Management IP Address**, **Subnet Mask**, **Default Gateway** and **DNS Server IP Address** either via DHCP or with Static IP configuration so that the AP can get access to the Internet and AltaiCare cloud server
3. Click "Submit" button

Note: AltaiCare service is not supported under **Gateway Mode**

IMPORTANT NOTE: DNS Server IP is required to resolve the domain name of the AltaiCare cloud server: **care.altaitechnologies.com**. If you are not sure about your ISP DNS Server IP, you can use Google Public DNS Server e.g. 8.8.8.8

ALTAI Super WiFi

Step 2 (Optional): Management VLAN Setting
(Applicable to local VLAN environment only)



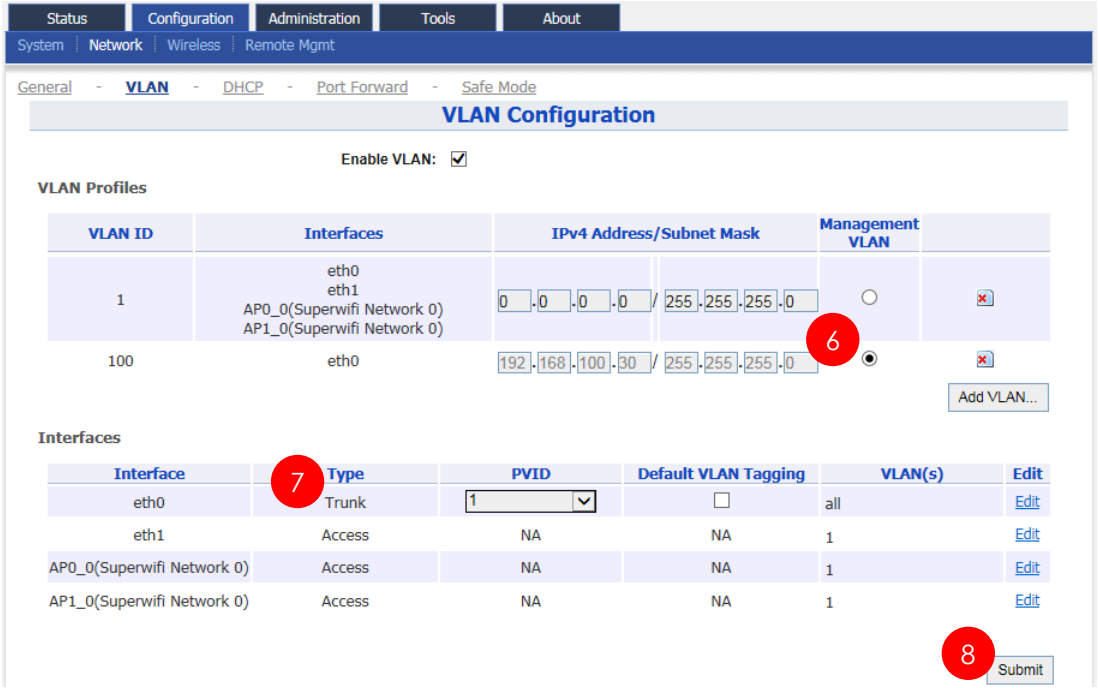
Procedures:

1. Check the box of **Enable VLAN**
2. Click "Submit"button to save the changes
3. Click "Add VLAN..." button to create a new VLAN profile for management VLAN
4. Input the management VLAN in the field of **VLAN ID** and click "Submit" button. In this example, VLAN 100 is the management VLAN for the local network

Note: Make sure the firewall and IP routing settings of the local network allow the AP traffic to reach Internet via local management VLAN for the AP connection with AltaiCare cloud server.

ALTAI Super WiFi

Step 2 (Optional): Management VLAN Setting
(Applicable to local VLAN environment only) (Cont.)

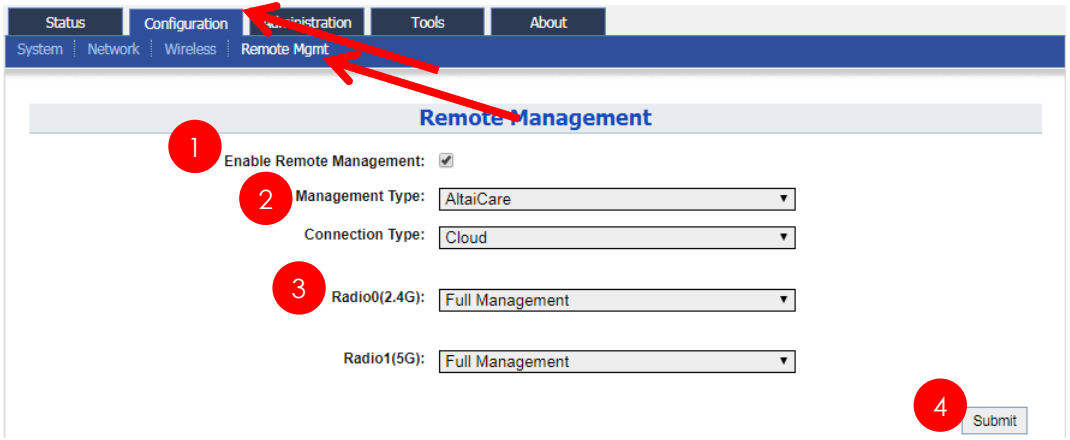


Procedures:

6. Click "Management VLAN" button on the newly created VLAN entry, i.e. VLAN 100, in the VLAN Profile list
7. Make sure the interface to the Internet to be set to "Trunk" type. In this case, eth0 is the interface communicating with AltaiCare, so it is set to "Trunk"
8. Click "Submit" button

Note: All network nodes and links should be configured as trunk to all service VLANs and management VLAN for different kinds of traffic to/from the AP.

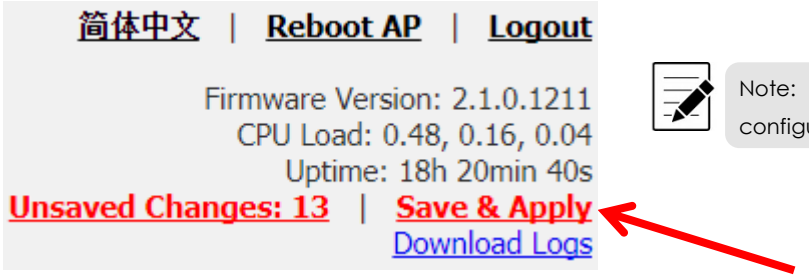
Step 3: Enable Remote Management



Procedures:

1. Check the box of **Enable Remote Management**
2. Select **AltaiCare** as **Management Type** and **Cloud** as **Connection Type**. This option will let AP connect to the AltaiCare cloud server (care.altaitechnologies.com)
3. Select one of the following options for the management type on both radios: (1) Radio0(2.4G); and (2) Radio1(5G)
   - **(1) Not Management**: Under this mode, all the radio configuration and statistics monitoring will be disabled in AltaiCare
   - **(2) Full Management**: Under this mode, the radio will be fully managed by AltaiCare. Any configuration changes made on the AP radio and WLAN profiles in AltaiCare will be provisioned to the AP. In general, this option is selected when the device is operating in AP mode
   - **(3) Monitor Mode**: Under this mode, all the radio settings in AltaiCare will become non-configurable. Also, any configuration changes made on the WLAN profiles in AltaiCare will not be provisioned to the AP. In general, this option is selected when the device is operating in Station Mode, Bridge Mode and Repeater Mode for radio statistics monitoring
4. Click "**Submit**" button

Step 4: Save & Apply AP Configuration Change



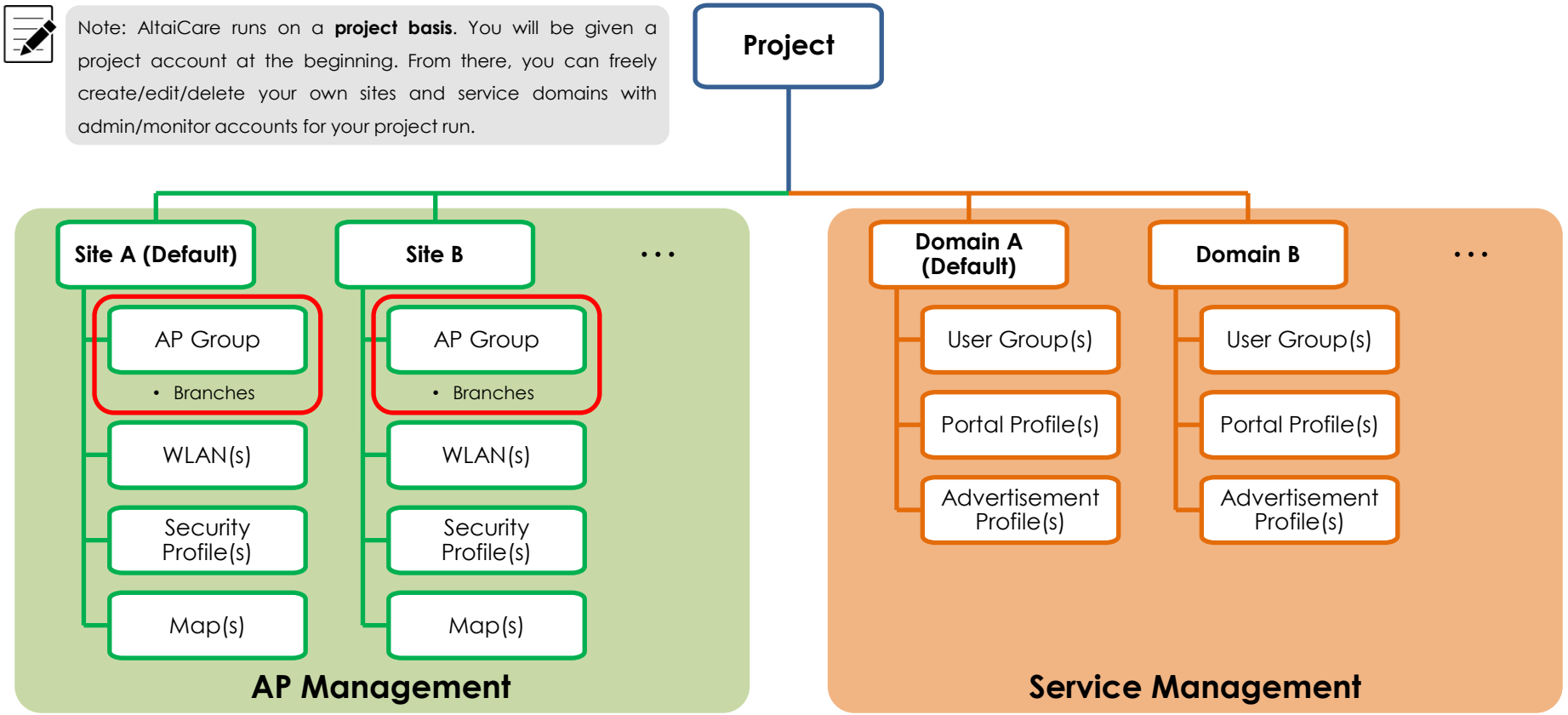
Note: Be reminded to click "**Save & Apply**" at the top right corner of WebUI to make all configuration changes take effect.

ALTAI Super WiFi

Getting Started

AltaiCare Hierarchy Overview

Note: AltaiCare runs on a **project basis**. You will be given a project account at the beginning. From there, you can freely create/edit/delete your own sites and service domains with admin/monitor accounts for your project run.



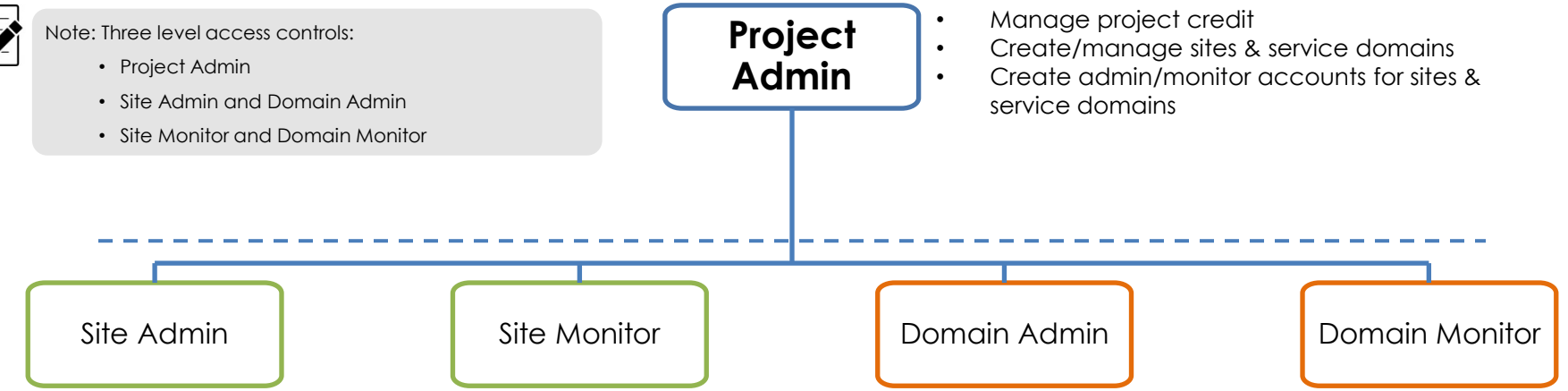
ALTAI Super WiFi

AltaiCare Hierarchy Overview (Cont.)

- **Project** is the root of Site and Service Domain. Under a Project, there must be at least **one** Site and **one** Service Domain.
- **Site** is a basic unit of AP group for centralized management. All common wireless settings in one site such as SSID and security configuration can be applied to all APs belonging to that site for simple operation and management.
- **Domain** is a separate realm for service management which includes user management, captive portal and advertisement service management. You can have user groups and accounts in there for user services such as RADIUS/Portal/MAC authentication, accounting and per user service policy control.

Multiple Level Access Control

Note: Three level access controls:
- Project Admin
- Site Admin and Domain Admin
- Site Monitor and Domain Monitor



- Manage project credit
- Create/manage sites & service domains
- Create admin/monitor accounts for sites & service domains

- Manage the sites to be assigned, including
- Register/deregister APs
- Create/edit/delete WLAN & security profiles

- Monitor site status and site statistics

- Manage the service domains to be assigned, including
- Create/edit/delete user groups and user accounts
- Create/edit/delete portal configuration
- Create/edit/delete advertisement configuration

- Monitor user account profile, login history and session statistics
- Monitor advertisement view/click count statistics

ALTAI Super WiFi

AltaiCare Credit System and Policy

AltaiCare uses a credit system to determine how many and how long the APs can be managed with an AltaiCare account. The credit system deducts credits for the APs being managed by AltaiCare, using the following consumption rates for different AP models:

A8n/A8n(ac) series: 25 credits per day per unit
A3Ei: 8 credits per day per unit
A3c/A3w/A2/A2e: 6 credits per day per unit
A2c/C2s: 2 credits per day per unit
C1n/C1an series: 1 credit per day per unit

Note: Once an AP is successfully connected to AltaiCare, the credit system will start counting and deducting credits for that AP on a daily basis (UTC time from 00:00 to 24:00). If an AP has been offline in AltaiCare for a full day (24 hours), the corresponding credits for that day will then NOT be deducted.

Example:
For an account with 100 credits left, the time that the AP(s) can be managed by AltaiCare is as follows.

Scenario 1: 1 x A8Ein for 4 days
Scenario 2: 4 x A8Ein(ac) for 1 day
Scenario 3: 2 x A3Ei and 2 x C2s for 5 days (100/(2x8+2x2) = 5 days)
Scenario 4: 5 x A2c and 10 x C1n for 5 days (100/(5x2+10x1) = 5 days)
Scenario 5: 1 x A3Ei and 5 x A3c for 2 days (100/(1x8+5x6) = 2 days with 24 credits left).

In Scenario 5, the remaining 24 credits will not be processed for the 3rd day of operation due to insufficient credits. AltaiCare will accordingly cut off its service and AP WLAN operation until further credit refill. **To avert AltaiCare service suspension, we recommend you refill credits one month earlier before credit exhaustion.** AltaiCare will also help send email notification and show alert messages on the GUI to remind project admin of credit refill, in one-month advance. For details about credit request and install, please refer to here.

ALTAI Super WiFi

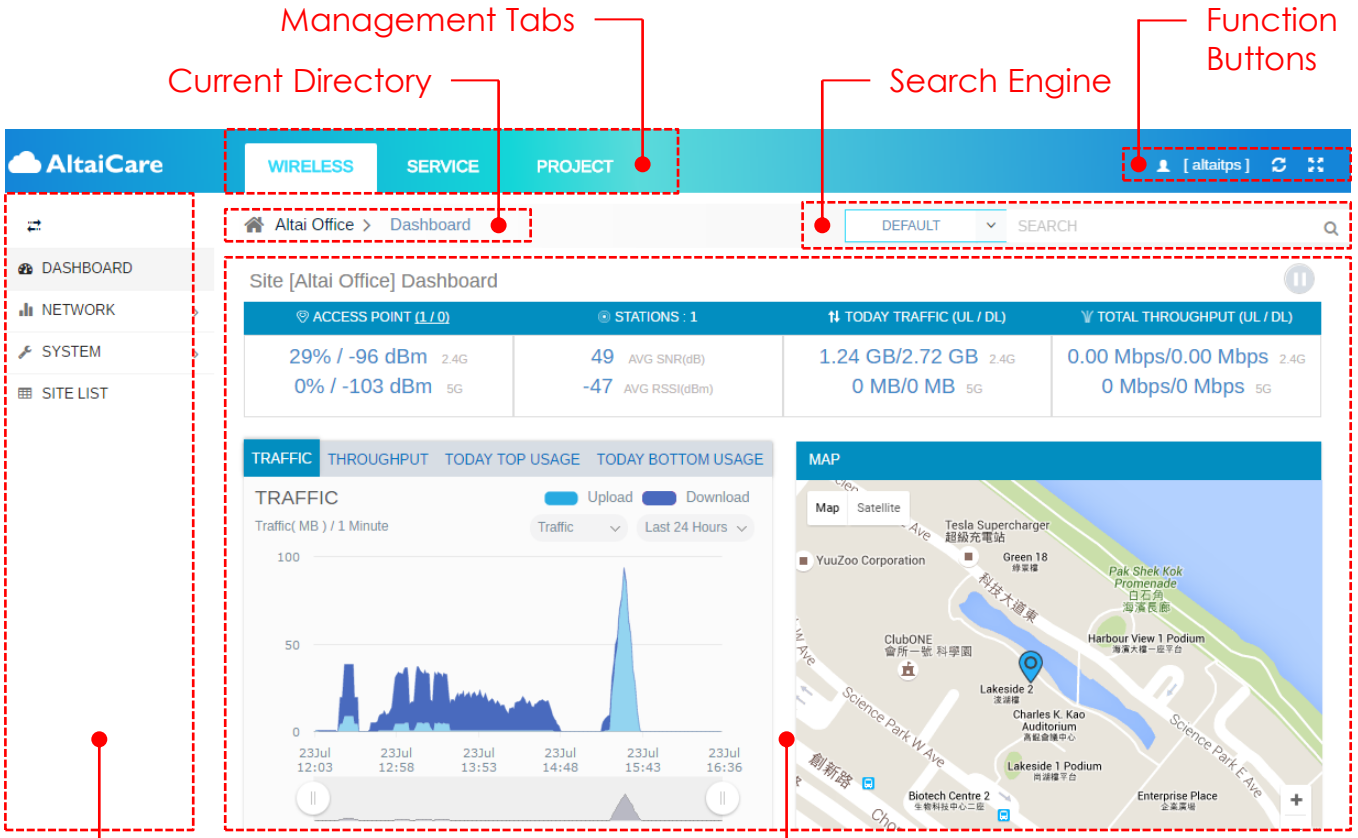
Access to AltaiCare

Note: For the best compatibility, it is strongly recommended the web browser " Google Chrome" be used to access the AltaiCare WebUI.

Note: HTTP and HTTPS are supported for access to AltaiCare platform

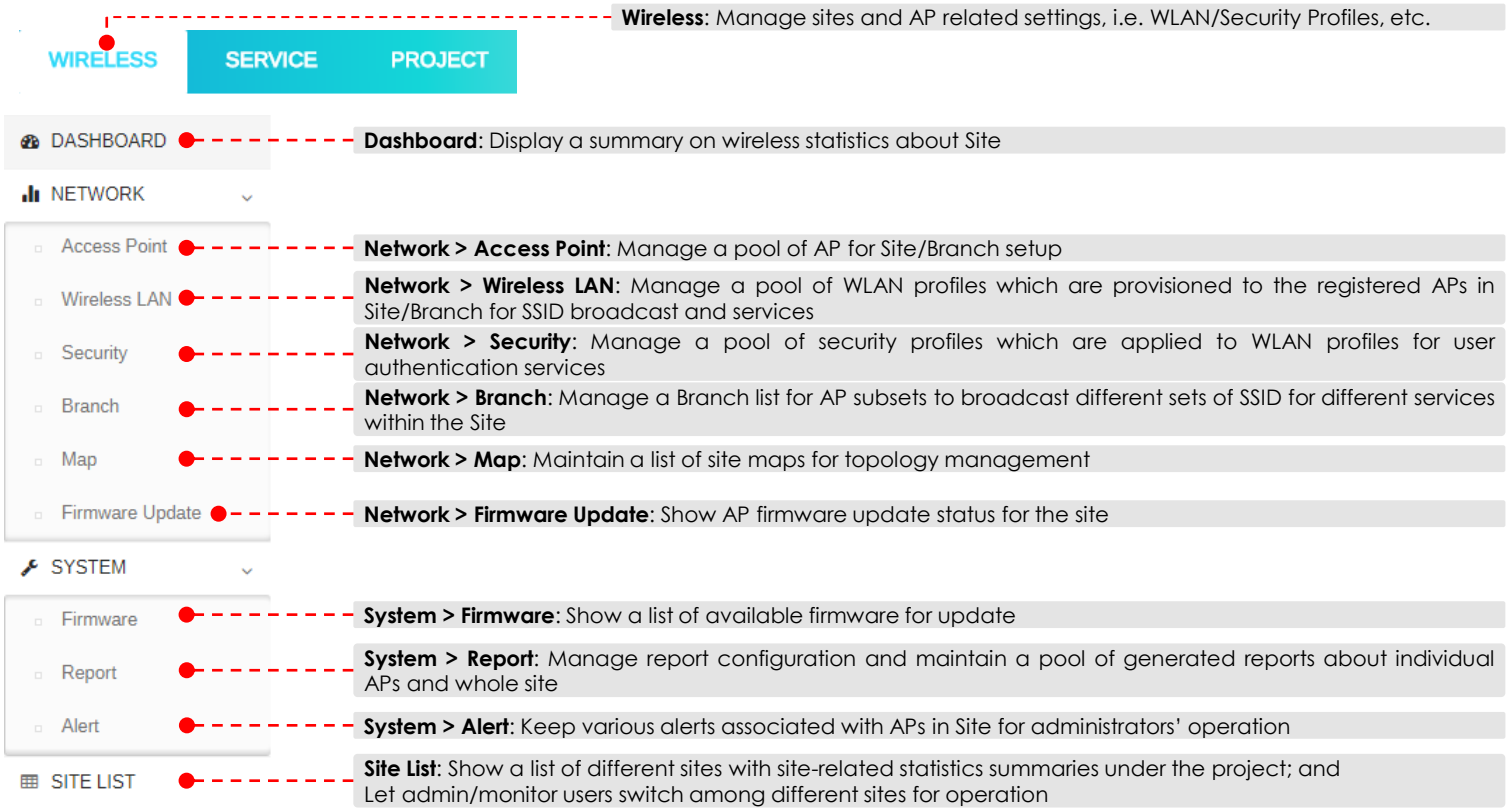
ALTAI Super WiFi

AltaiCare Web Interface



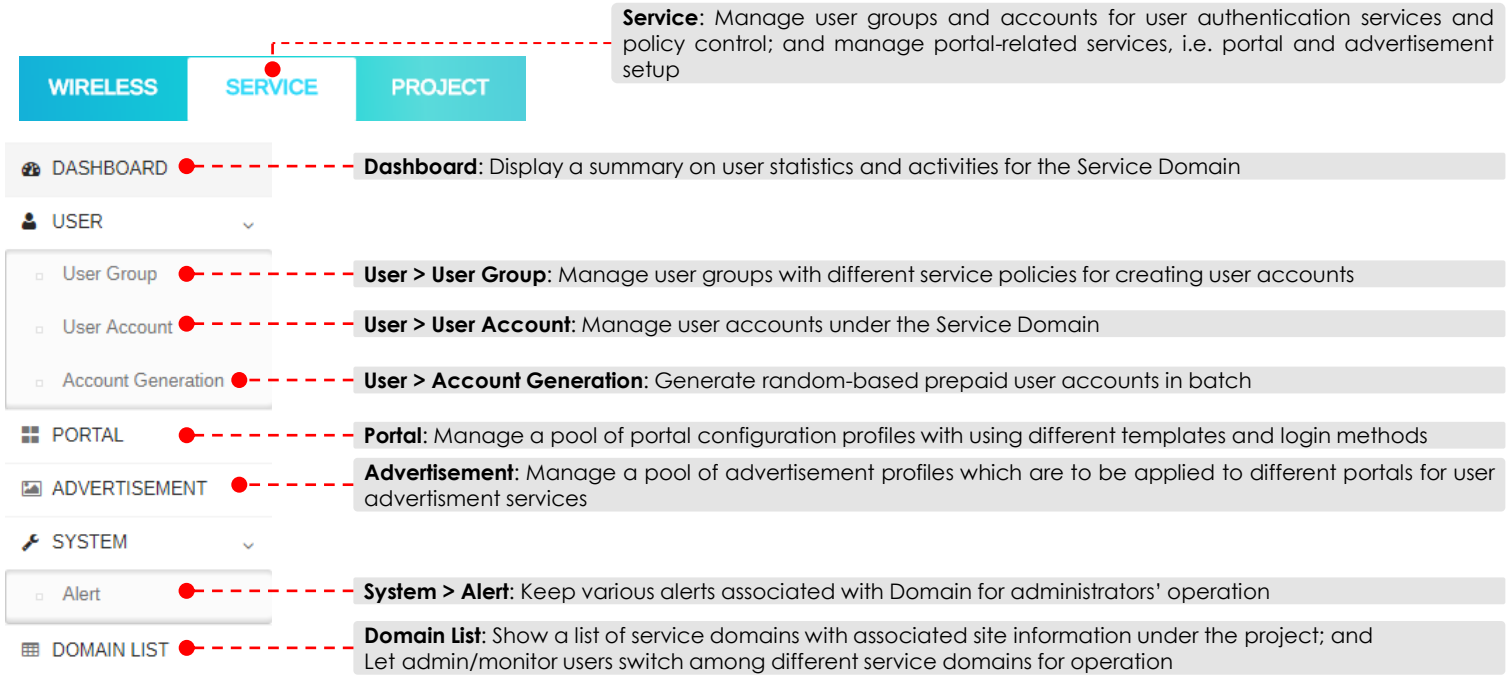
ALTAI Super WiFi

Wireless Management Overview



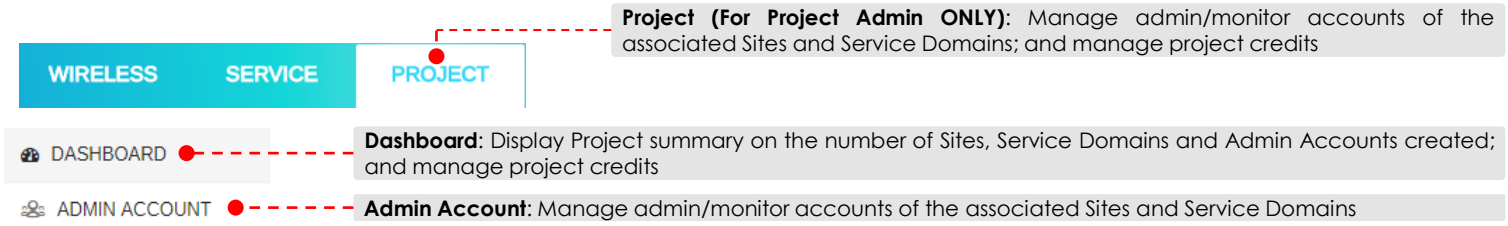
ALTAI Super WiFi

Service Management Overview



ALTAI Super WiFi

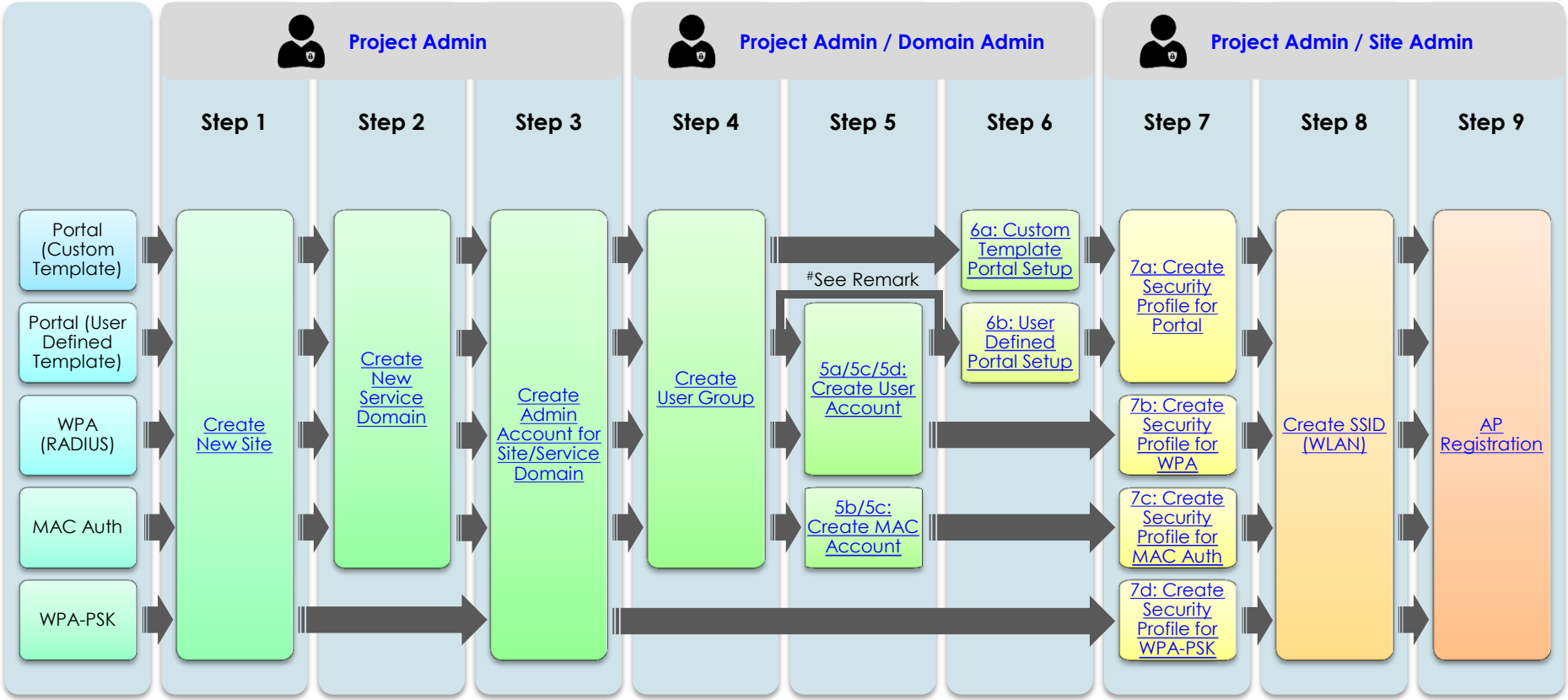
Project Management Overview



ALTAI Super WiFi

Basic Configuration

Configuration Procedures

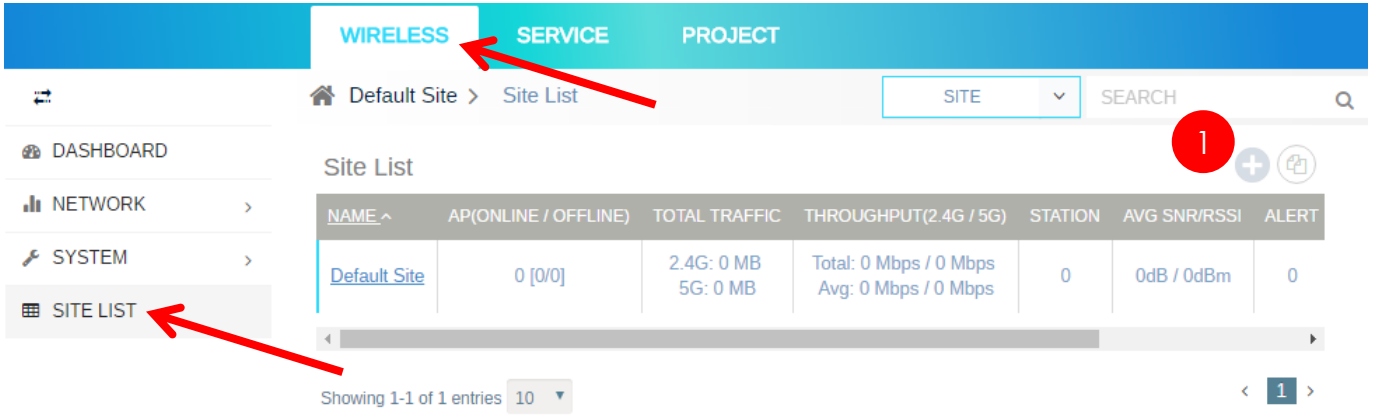


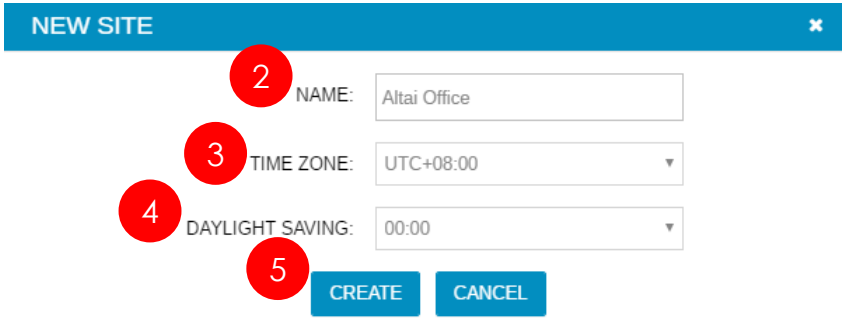
#Remark: Step 5 can be skipped for the portal authentication using Guest Login, Sign Up and Social Account Login.

ALTAI Super WiFi

Step 1: Create New Site

Step 1: Create New Site – Basic Setting





Procedures:

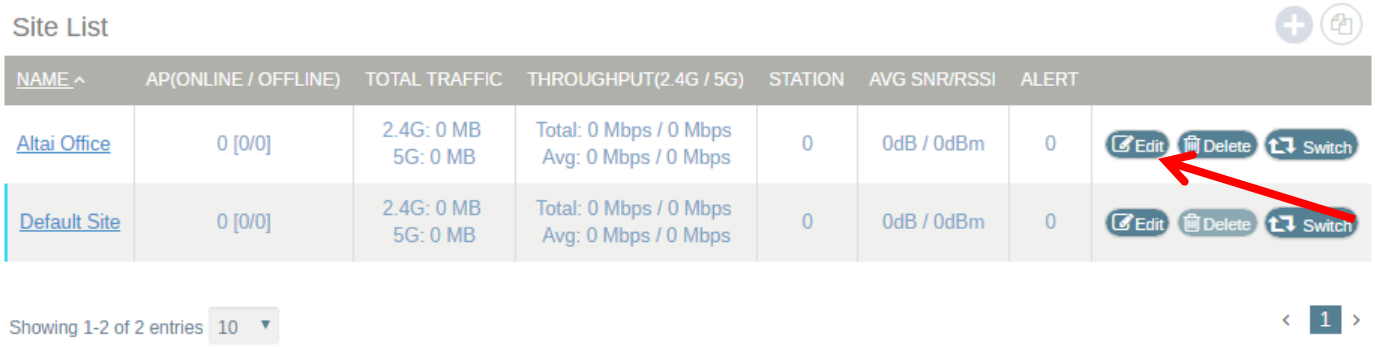
1. Click ⊕ to create a new site.
2. Give a name for the site. In this example, we create a site called "Altai Office" for demo purpose.
3. Specify the time zone in Coordinated Universal Time (UTC) for the site. All the site/AP-related operations such as WLAN service scheduler, firmware update scheduler, and alert /statistics report are all based on this clock setting. By default, it is set to UTC+08:00
4. If necessary, set the clock one hour (01:00) or half an hour (00:30) forward during the summer time. By default, it is set to 00:00
5. Click CREATE button and an entry for the new site will be added to the Site List.

Note: By default, a Default Site is automatically created for every project account. It is not allowed to remove that site. However, Project Admin is free to create/delete his/her own additional sites for project needs.

ALTAI Super WiFi

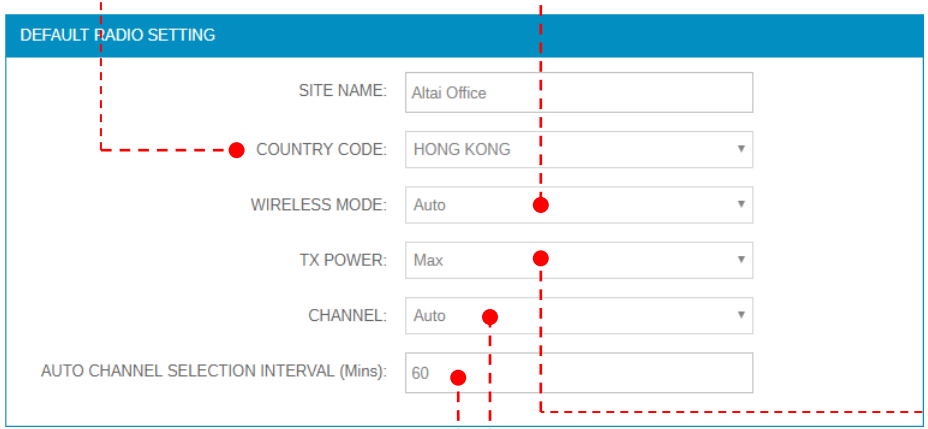
Step 1: Create New Site - Default Radio Setting

A new site entry is created. To make changes on the site details, click Edit button on the entry. You can modify default radio settings in there.



Step 1: Create New Site – Default Radio Setting (Cont.)

Country Code: Select the country where Site/AP is located. Configuring a country code ensures that the radio regulatory domain such as frequency bands, channels and transmit power levels are compliant with country-specific regulations. By default, it is set as Hong Kong.



Tx Power / Auto Channel Selection Interval (Min): See next slide

Wireless Mode: Control what 802.11 standards and how wide of channel bandwidth to be used for AP operation. Each combination of 802.11 standards and channel bandwidth will have different data throughput performance.

Different AP models can have different available Wireless Modes for selection. For simplicity, there are two options available for every newly joining AP: 1) Auto; and 2) Use AP Setting. Once the AP is successfully registered and added to the site, you can specify which Wireless Mode to be run through the AP entry detail setting. For details, refer to Advanced Configuration - Individual AP Setting.

- **Auto**: AltaiCare automatically selects the most generic wireless mode for AP operation under different kinds of environment. By default, 802.11ng HT20 is selected for 2.4G radio and 802.11ac HT20 / 802.11na HT20 for 5G radio.
- **Use AP Setting**: AltaiCare will not alter the AP wireless mode setting and keep it as it is in AP WebUI for its first time to associate to the AltaiCare system. To change the Wireless Mode configuration, you have to go to AP WebUI.

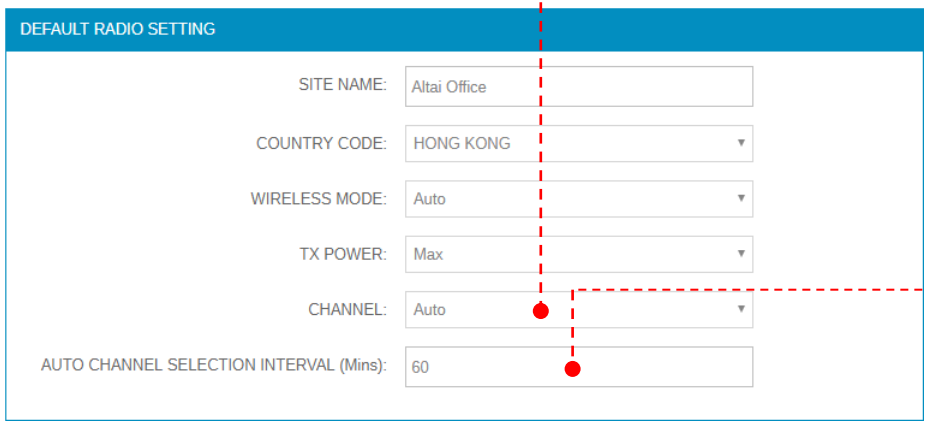
By default, it is set as Auto.

Tx Power: Set the AP transmission power on 2.4G/5G radios. Tx Power can be adjusted in the following different levels.

- **MAX**: Maximum Tx power that AP supports
- **1/2**: 1/2of maximum Tx power
- **1/4**: 1/4 of maximum Tx power
- **1/8**: 1/8 of maximum Tx power
- **1/16**: 1/16 of maximum Tx power
- **1/32**: 1/32 of maximum Tx power
- **Use AP Setting**: AltaiCare will not alter the Tx Power setting and keep it as it is in AP WebUI for its first time to associate to the AltaiCare system

ALTAI Super WiFi

Step 1: Create New Site – Default Radio Setting (Cont.)



Channel: Set operating frequency channel for 2.4G and 5G radios.
Different AP models can have different radios/frequency bands supported. For simplicity, there are two options available for every newly joining AP: 1) Auto; and 2) Use AP Setting. Once the AP is successfully registered and added to the site, you can specify which channel to be run through the AP entry detail setting. For details, refer to Advanced Configuration - Individual AP Setting.

- **Auto**: AltaiCare automatically selects the best channel for the AP, based on the following ACS (Auto Channel Selection) factors:
  - Air busy%;
  - Number of neighboring AP occupying the channel; and
  - Noise floor
- **Use AP Setting**: AltaiCare will not alter the AP channel setting and keep it as it is in AP WebUI for its first time to associate to the AltaiCare system. To change the channel, you have to go to AP WebUI.

By default, it is set as Auto.

Auto Channel Selection interval (Min): Set a schedule (in Minutes) to perform channel scanning periodically for the best channel selection.
This option is available only when the channel is selected as "Auto". "0" means the feature disabled.

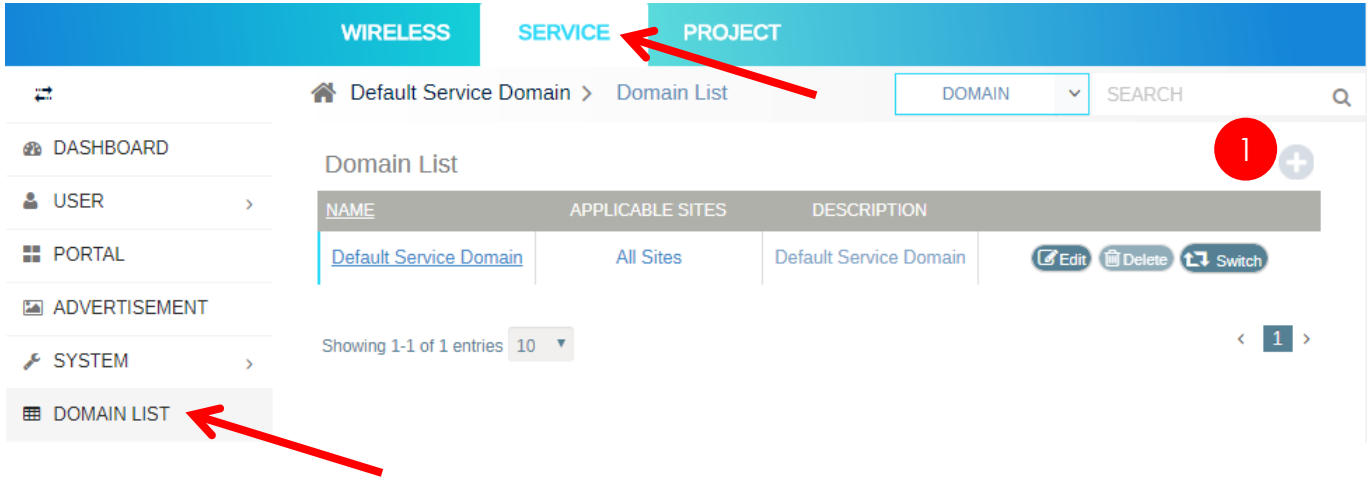
Note: Remember to click SAVE button at the page bottom to make all changes take effect.

Step 2: Create New Service Domain

Step 2: Create New Service Domain – Basic Setup

Procedures:

1. Click to create a new service domain



ALTAI Super WiFi

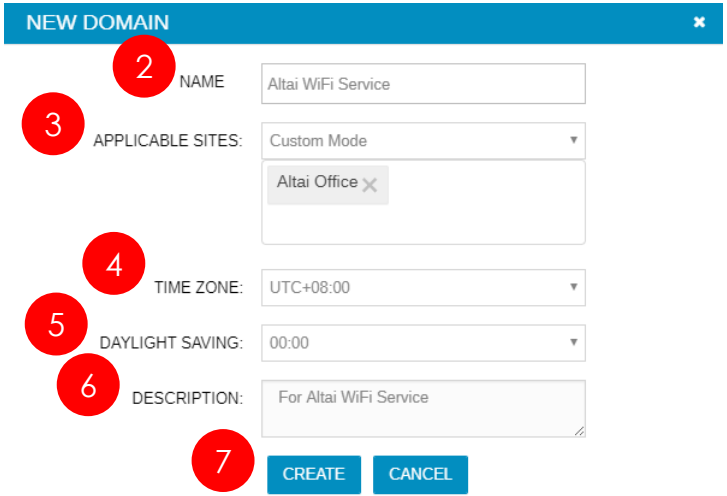
Step 2: Create New Service Domain – Basic Setup

Procedures:

2. Give a name for the domain. In this example, we create a site called "Altai WiFi Service" for demo purpose.
3. Select and map the existing sites to the service domain for user authentication and service control. The mapping allows and makes the ONLY connection between Site Wireless Security and Service Domain. In other words, Site Admin is granted to add the relevant User Groups from the Service Domain for the wireless security profile setting, i.e. portal, RADIUS and MAC authentication. For details of security profile setting, refer to Step 7a/7b/7c.
   You can either choose all or particular sites for the mapping.

   All Sites: With this option selected, all sites will be made connection to the service domain for wireless security profile setting.
   Custom Mode: With this option selected, only a pool of selected sites will be made connection to the service domain for wireless security profile setting.

4. Specify the time zone in Coordinated Universal Time (UTC) for the service domain. All the service-related operations such as User Group/Account expiry control and user login/traffic statistics report are all based on this clock setting. By default, it is set to UTC+08:00
5. Set the clock one hour (01:00) or half an hour (00:30) forward during the summer time. By default, it is set to 00:00
6. Give a brief description of what the service domain is for. It is an optional field.
7. Click CREATE button and an entry for the new domain will be added to the Domain List.



Note: Remember to click SAVE button at the page bottom to make all changes take effect.

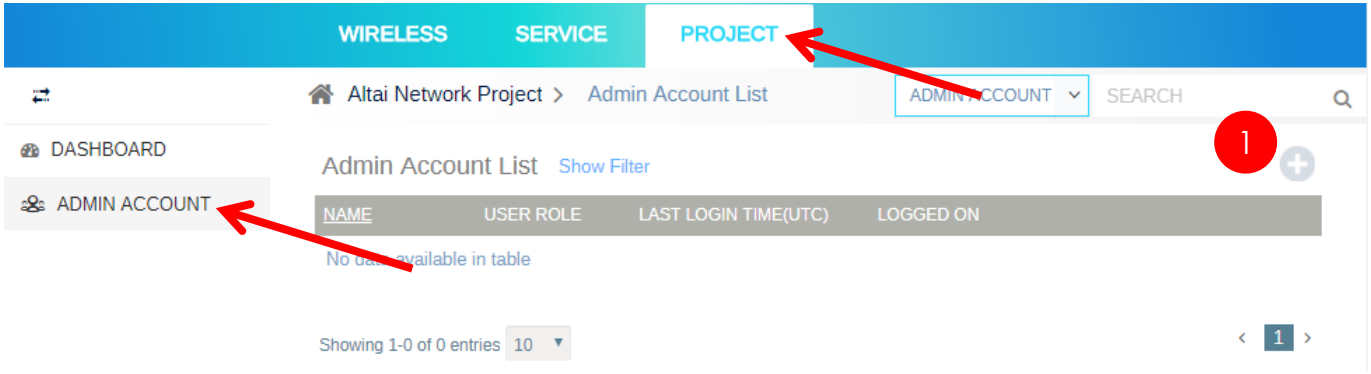
ALTAI Super WiFi

Step 3: Create Admin Account for Site/Service Domain

Step 3: Create Admin Account for Site/Service Domain

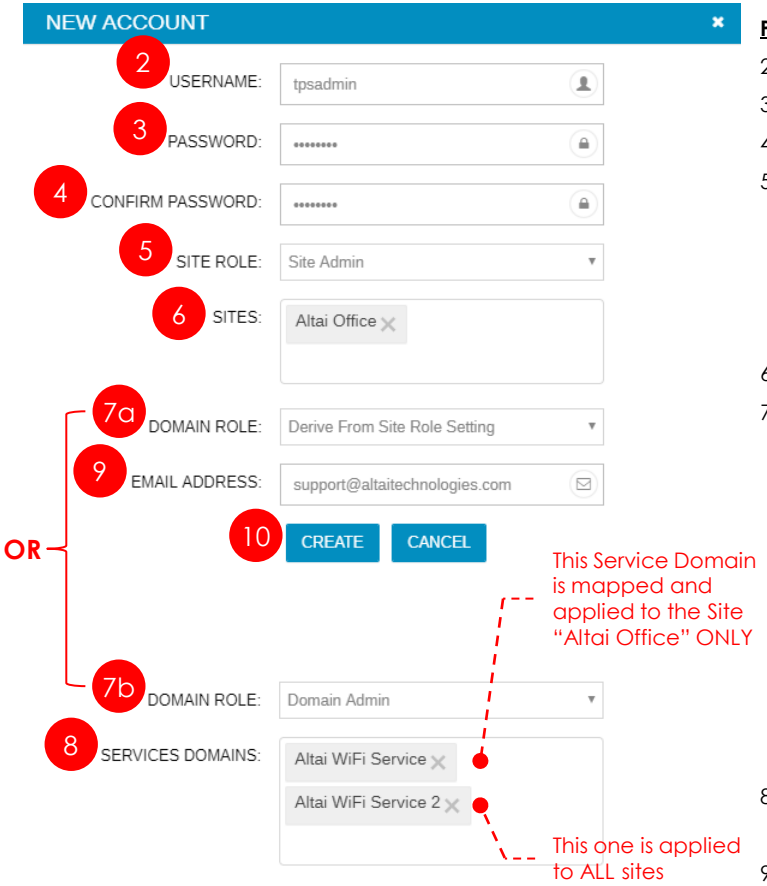
Procedures:

1. Click to create a new admin acount



ALTAI Super WiFi

Step 3: Create Admin Account for Site/Service Domain (Cont.)



Procedures:

2. Input a username for the new account.
3. Input a string not less than 6 characters for the password.
4. Retype the password to confirm it.
5. Define a site role for the account:

   Site Admin: who has all access rights for the assigned sites (which is specified in item #6), i.e. register/deregister APs, create/edit/delete WLAN and security profiles, etc.

   Site Monitor: who can only monitor the site status and statistics. Any operations on site/wireless-related configuration is forbidden.
6. Specify the site(s) to be managed for the account.
7. Define a domain role for the account:

   Domain Admin: who has all access rights for the assigned service domains (which is specified in item #8), i.e. create/edit/delete service-related settings such as user groups, user accounts, portals and advertisement.

   Domain Monitor: who can only monitor the domain status and statistics. Any operations on domain-related configuration is forbidden.

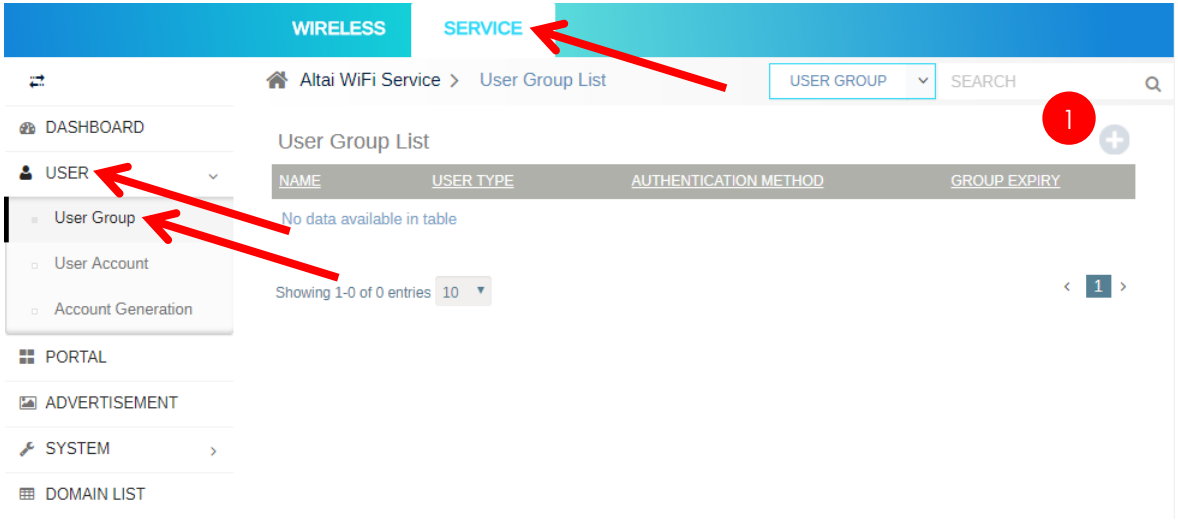
   Derive From Site Role Setting: which will automatically assign domain admin/monitor role for site admin/monitor respectively. The domains to be managed for this setting are ONLY limited to those which are applicable to the sites selected in item #6. In other words, with this setting, you are NOT allowed to manage the service domains which apply to ALL sites.
8. Select the existing service domains to be managed for the account. The pool contains the service domains which are applicable to the sites selected in item #6 and those which apply to ALL sites.
9. Enter the user's email address of account registration.
10. Click CREATE button to open and confirm the account.

Step 4: Create User Group

Step 4: Create User Group

Procedures:

1. Click to create a new User Group



Step 4: Create User Group (Cont.)

Procedures:

2. Give a name for the group.
3. Select one of the following User Type which is to define the user account nature for the user group. Three user types available here:

   (1) Prepaid: As the name suggests, "Prepaid" requires the users pay before the service. This kind of service is always to be valid for a certain period. Once expired, it will stop the service.

   (2) Subscription: On the other hand, "Subscription" means post-paid service. This kind of service is always long-term. Users have to foot the monthly bill to maintain the service. Therefore, their data quota is reset in every month.

   (3) Guest: Not like prepaid and subscription users, this kind of users do not need to possess a valid account and can still enjoy the WiFi service. Common examples are portal guest and sign up for public WiFi. In this case, AltaiCare will automatically generate accounts for this kind of anonymous users for service and policy control.

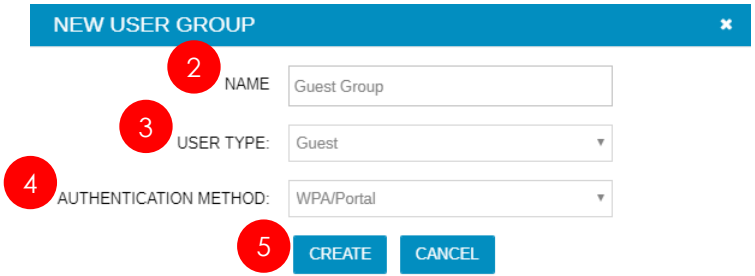
4. Choose one of the following Authentication Method which is to define user account type for different authentication purposes:

   (1) WPA/Portal: Use "username/password" as user account for #portal authentication or WPA authentication (PEAP).

   (2) MAC: Use device MAC address as username of user account for MAC authentication.

   #NOTE: For portal guest/sign up/social account login users, they are automatically assigned with "username/password" type of account by the system.

5. Click CREATE button to confirm the user group creation.



ALTAI Super WiFi

Step 4: Create User Group (Cont.)

Overall, we created the following 5 user groups for the demo:

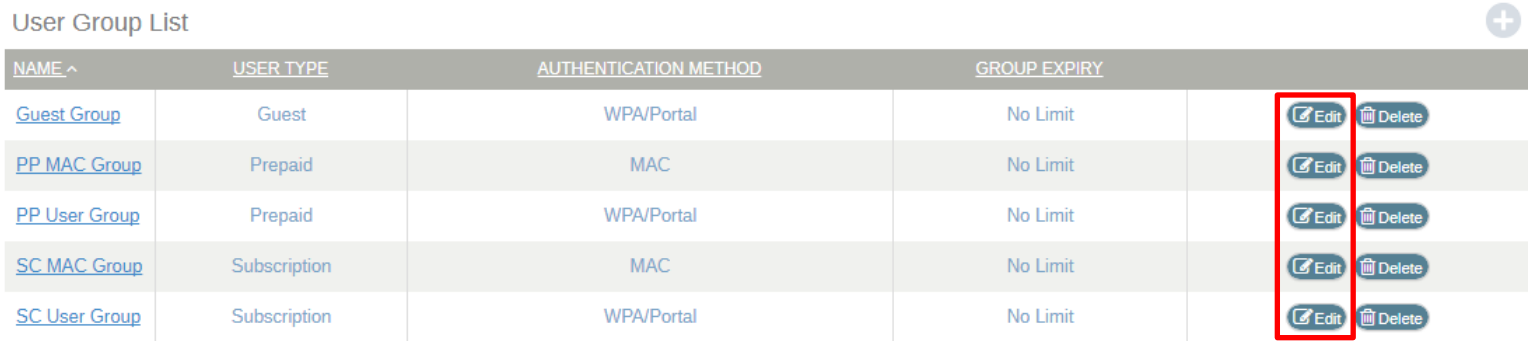
(1) **Guest Group** – Used for **portal guest login and sign up login** via SSIDs: "Care_CT_Portal" and "Care_UDT_Portal"

(2) **PP User Group** – Used for **portal username/password login** via SSID: "Care_UDT_Portal"

(3) **SC User Group** – Used for **WPA authentication** via SSID: Care_WPA

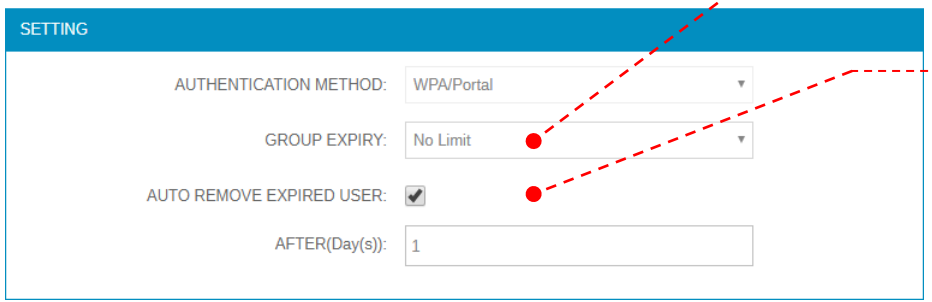
(4) **PP MAC Group** – Used for **MAC authentication** via SSID: Care_MAC_Auth

(5) **SC MAC Group** – Used for **MAC authentication** via SSID: Care_MAC_Auth



Next, click Edit on each of the newly created entries of user group for further configuration.

Step 4: Create User Group – Group Setting



It can be either defined by "Custom Mode" with a specific date and time or set as "No Limit".

Once the user group is expired by the specified time, all the user accounts belonging to that user group will be expired as well at the same time.

The group can be re-activated by setting another time in "Custom Mode" or changing to "No Limit".

With this feature enabled, AltaiCare will automatically remove the expired users belonging to the user group from AltaiCare database in X days later.

Step 4: Create User Group – User Account Default Setting (Guest/Prepaid Type)

Note: All guest, #sign-up and social login users are all automatically assigned with individual accounts using their unique wireless MAC address.

#Except those using the type of Email Sign-Up with verification code return. The user account will be generated using their registered Email as login name.

Applicable to prepaid type of user account ONLY. It defines the period of time the account is valid for. It starts from the time when the users log in the system for the first time. If the account becomes expired before the current session timeout, the user can still access the network until session timeout or idle timeout.

It can be either defined by "custom mode" in unit of Minute(s), Hour(s) or Day(s) or set as "No Limit".

Applicable to prepaid type of user account ONLY. It is to set the data quota (sum of uplink and downlink traffic) for each user account of this User Group.

It can be either defined by "custom mode" in a range from 1 to 100000MB or set as "No Limit".

Set upper limit to the UL and DL throughput for each user under the User Group. The unit is in kbps. In other words, setting of 10000 means 10Mbps of throughput limit for each user.

It can be either defined by "custom mode" in a range from 1 to 1000000kbps or set as "No Limit".

Define how long (in minute) one session will last for upon users' successful login. Once the current session is expired, users have to log in the system again for network access.

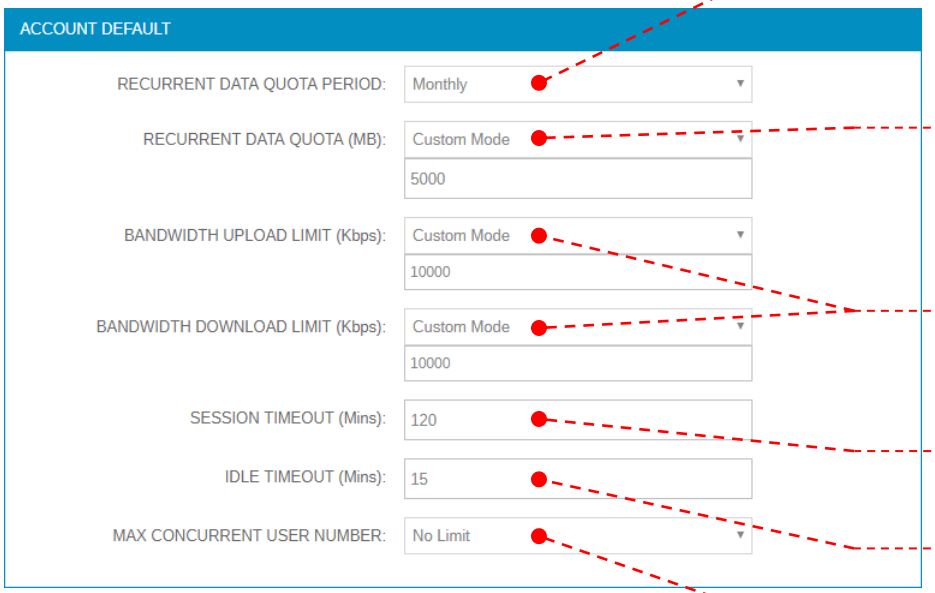
Define how long (in minute) the session is idle for. When there is no wireless traffic running for a period defined here, the user will be kick out of the session. Users have to log in the system again for network access.

Not applicable to portal guest, sign up and social login users. It is used for pre-defined user account type and defines how many concurrent users using the same account (username/password) to log in the WiFi network.

Note: The only difference between Guest and Prepaid types lies on the default account setting of Validity. By default, guest type accounts are set to 2 hours of validity while prepaid type accounts are set to "No Limit".

ALTAI Super WiFi

Step 4: Create User Group – User Account Default Setting (Subscription Type)



Applicable to subscription type of user account ONLY. It defines the period of time to reset the data quota to the value as specified in the next item. It starts counting from the time as specified when user account is created (refer to Step 5 Account Start Time Setting). If the data quota is used up before the current session timeout, the user can still access the network until session timeout or idle timeout.

The reset period can be on a Daily, Weekly or Monthly basis.

Applicable to subscription type of user account ONLY. It defines the data quota (sum of uplink and downlink traffic) to be reset for each user account of this User Group.

It can be either defined by "custom mode" in a range from 1 to 144000MB or set as "No Limit".

Set upper limit to the UL and DL throughput for each user under the User Group. The unit is in kbps. In other words, setting of 10000 means 10Mbps of throughput limit for each user.

It can be either defined by "custom mode" in a range from 1 to 1000000kbps or set as "No Limit".

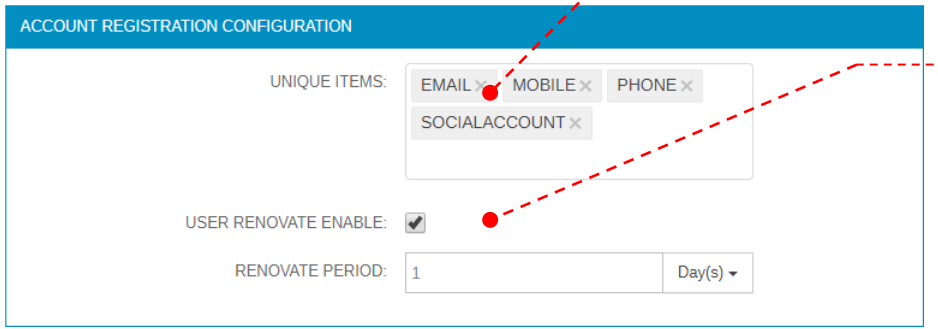
Define how long (in minute) one session will last for upon users' successful login. Once the current session is expired, users have to log in the system again for network access.

Define how long (in minute) the session is idle for. When there is no wireless traffic running for a period defined here, the user will be kick out of the session. Users have to log in the system again for network access.

Not applicable to portal guest, sign up and social login users. It is used for pre-defined user account type and defines how many concurrent users using the same account (username/password) to log in the WiFi network.

ALTAI Super WiFi

Step 4: Create User Group – Account Registration Configuration



For portal sign up users only. By defining unique items (Email/Mobile/Phone/Social Account) here, it prevents users from submitting the same information over multiple devices for portal sign up.

Assume "E-mail" as unique item. That means users cannot use the same E-mail to sign up over two devices. To sign up 2 accounts, users have to use 2 different E-mail addresses.

Applicable for auto-generated user accounts such as portal guest, sign up and social login. When it is enabled, it will renew the account and reset the data quota in an interval defined here.

It is in unit of Minute(s), Hour(s) and Day(s). It starts counting from the time the account is activated (at the moment the users log in the portal).

For example, set the guest user account (portal guest / sign up / social login) to be valid for 2 hours. And then enable "User Renovate" feature and set "Renovate Period" as 1 day.

That means the user can log in to get a session for 2 hours. To regain the session, the user has to wait for next day and then log in the portal again.

Therefore, the portal guest / sign up / social login users can get 2 hour session every day.

Step 5: Create User Account

ALTAI Super WiFi

Step 5: Create User Account

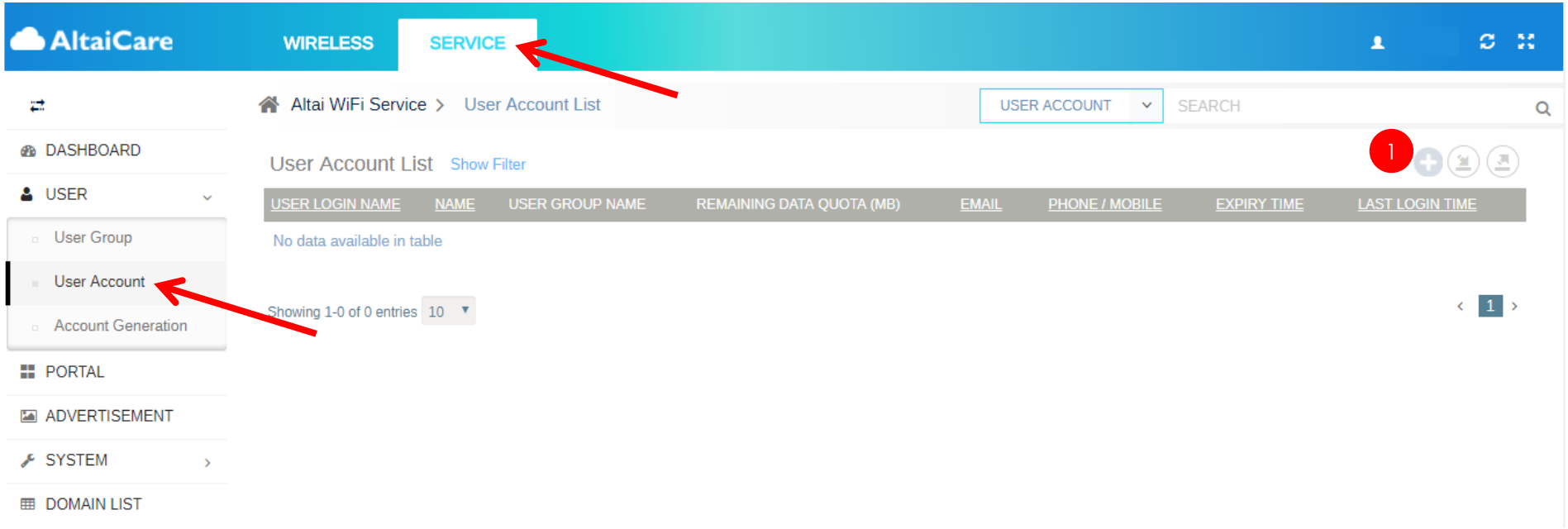
We provide the following three ways of user account generation.

User Account Generation Method	Supported User Account Type				Remarks
	WPA/Portal		MAC Auth		
	Prepaid	Subscription	Prepaid	Subscription	
(1) Single User Account Generation	✓	✓	✓	✓	For WPA/Portal user account setup procedures, go to Step 5a For MAC account setup procedures, go to Step 5b
(2) User Account Batch Import (in .CSV file)	✓	✓	✓	✓	For user account setup procedures, go to Step 5c
(3) Voucher-based User Account Batch Generation	✓	N/A	N/A	N/A	For user account setup procedures, go to Step 5d

Step 5a/5b: Create Single User Account

Procedures:

1. Click ⊕ to create a new user account. For WPA/Portal type of user account generation, go to Step 5a. For MAC Auth type of user account generation, go to Step 5b.

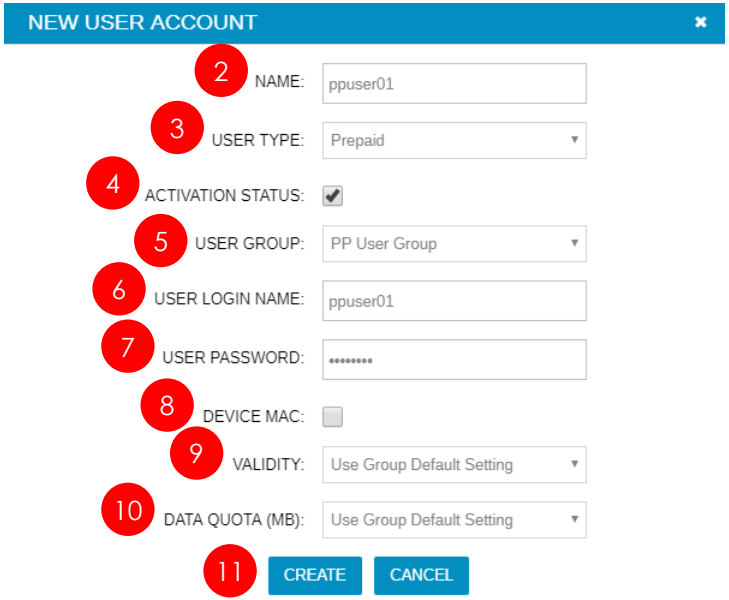


ALTAI Super WiFi

Step 5a: Create Single User Account (Prepaid)

Procedures:

2. Give a name for the account. This name is not used for login.
3. Choose Prepaid as User Type for the user account.
4. Check the box of Activation Status; otherwise, the account will become disabled.
5. Assign the user account to the User Group which have been created in Step 4. It should give you a pool of prepaid type of user groups for selection, e.g. PP User Group and PP MAC Group.
6. Enter Username for user login.
7. Enter Password for user login.
8. If necessary, you can check the box of "Device MAC" which will bind the account to a particular device by the MAC address specified here. In other words, the account cannot be shared with other devices. The MAC can be in **colon-separated** or **hyphen-separated** format with either **uppercase** or **lowercase** alphabets, e.g. **XX:XX:XX:XX:XX:XX** or **xx-xx-xx-xx-xx-xx**
9. Set Validity of the user account. For the term definition, see Step 4: Create User Group – User Account Default Setting. There are three options available: **(1) Custom Mode**; **(2) No Limit**; and **(3) Use Group Default Setting** of the selected user group in item 5.
10. Set Data Quota (MB) of the user account. For the term definition, see Step 4: Create User Group – User Account Default Setting. There are three options available: **(1) Custom Mode**; **(2) No Limit**; and **(3) Use Group Default Setting** of the selected user group in item 5.
11. Click CREATE button and a new user account entry will be created in the list. See the list here.

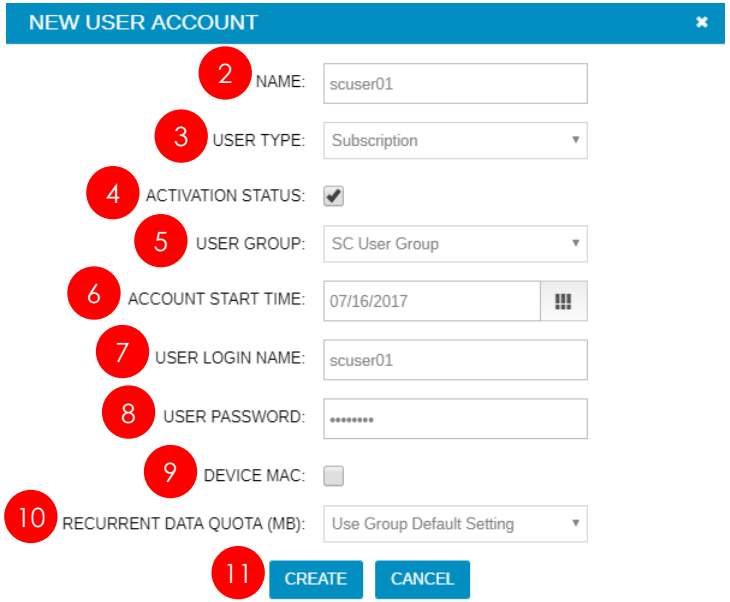


ALTAI Super WiFi

Step 5a: Create Single User Account (Subscription)

Procedures:

2. Give a name for the account. This name is not used for login.
3. Choose Subscription as User Type for the user account.
4. Check the box of Activation Status; otherwise, the account will become disabled.
5. Assign the user account to the User Group which have been created in Step 4. It should give you a pool of subscription type of user groups for selection, e.g. SC User Group and SC MAC Group.
6. Select a date to control when the users can start using the account.
7. Enter Username for user login.
8. Enter Password for user login.
9. If necessary, you can check the box of "Device MAC" which will bind the account to a particular device by the MAC address specified here. In other words, the account cannot be shared with other devices. The MAC can be in **colon-separated** or **hyphen-separated** format with either **uppercase** or **lowercase** alphabets, e.g. **XX:XX:XX:XX:XX:XX** or **xx-xx-xx-xx-xx-xx**
10. Set Recurrent Data Quota (MB) of the user account. For the term definition, see Step 4: Create User Group – User Account Default Setting. There are three options available: **(1) Custom Mode**; **(2) No Limit**; and **(3) Use Group Default Setting** of the selected user group in item 5.
11. Click CREATE button and a new user account entry will be created in the list. See the list here.

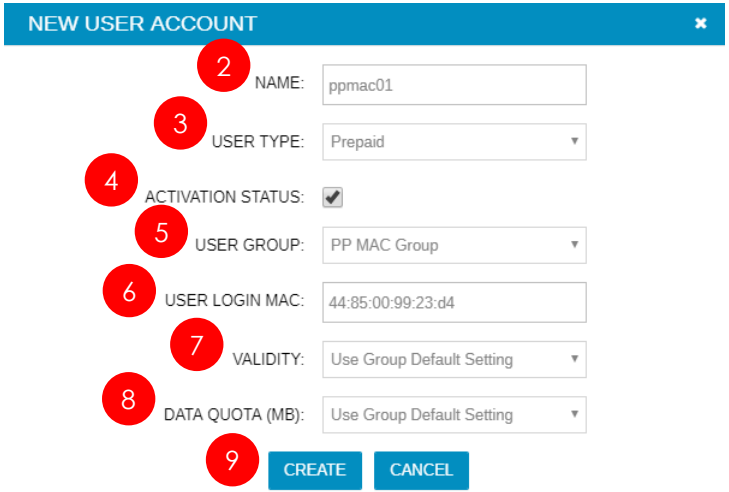


ALTAI Super WiFi

Step 5b: Create Single MAC Account (Prepaid)

Procedures:

2. Give a name for the account.
3. Choose Prepaid as User Type for the user account.
4. Check the box of Activation Status; otherwise, the account will become disabled.
5. Assign the user account to the User Group which have been created in Step 4. It should give you a pool of prepaid type of user groups for selection, e.g. PP User Group and PP MAC Group. In this case, we select "PP MAC Group" which should contain a number of MAC entries for MAC authentication.
6. Enter the device MAC for user login. The MAC to be specified here can be in **colon-separated** or **hyphen-separated** format with either **uppercase** or **lowercase** alphabets, e.g. **XX:XX:XX:XX:XX:XX** or **xx-xx-xx-xx-xx-xx**
7. Set Validity of the user account. For the term definition, see Step 4: Create User Group – User Account Default Setting. There are three options available: **(1) Custom Mode**; **(2) No Limit**; and **(3) Use Group Default Setting** of the selected user group in item 5.
8. Set Data Quota (MB) of the user account. For the term definition, see Step 4: Create User Group – User Account Default Setting. There are three options available: **(1) Custom Mode**; **(2) No Limit**; and **(3) Use Group Default Setting** of the selected user group in item 5.
9. Click CREATE button and a new user account entry will be created in the list. See the list here.

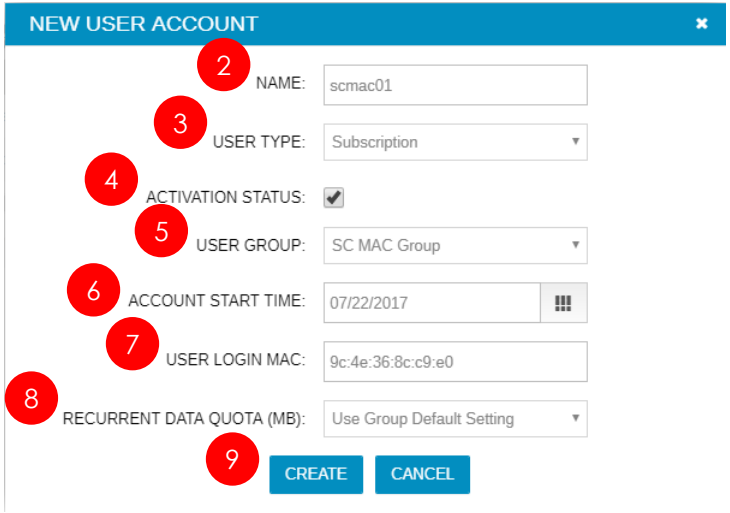


ALTAI Super WiFi

Step 5b: Create Single MAC Account (Subscription)

Procedures:

2. Give a name for the account.
3. Choose Subscription as User Type for the user account.
4. Check the box of Activation Status; otherwise, the account will become disabled.
5. Assign the user account to the User Group which have been created in Step 4. It should give you a pool of subscription type of user groups for selection, e.g. SC User Group and SC MAC Group. In this case, we select "SC MAC Group" which should contain a number of MAC entries for MAC authentication.
6. Select a date to control when the user can start using the account.
7. Enter the device MAC for user login. The MAC to be specified here can be in **colon-separated** or **hyphen-separated** format with either **uppercase** or **lowercase** alphabets, e.g. **XX:XX:XX:XX:XX:XX** or **xx-xx-xx-xx-xx-xx**
8. Set Recurrent Data Quota (MB) of the MAC account. For the term definition, see Step 4: Create User Group – User Account Default Setting. There are three options available: **(1) Custom Mode**; **(2) No Limit**; and **(3) Use Group Default Setting** of the selected user group in item 5.
9. Click CREATE button and a new user account entry will be created in the list. See the list here.



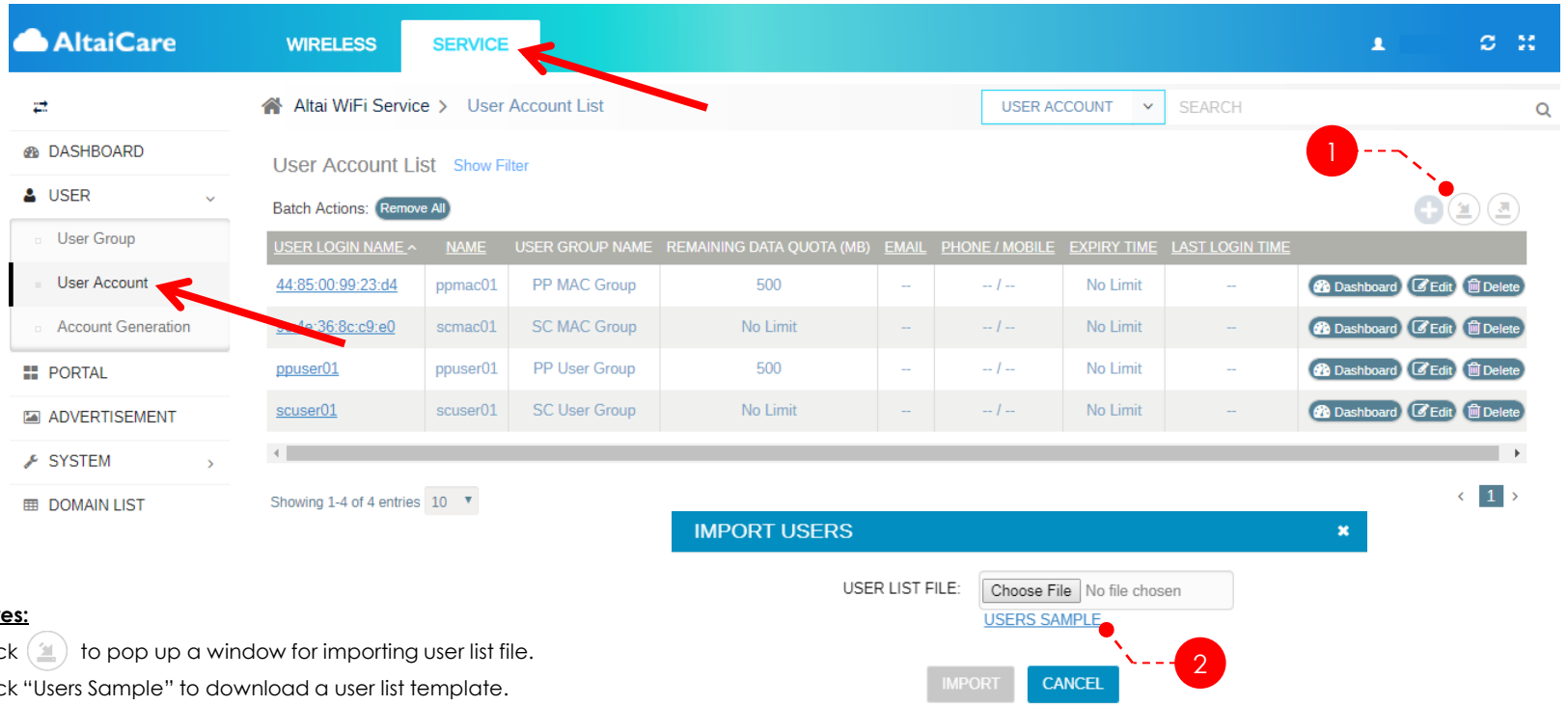
ALTAI Super WiFi

Step 5a/5b: Create Single User Account / MAC Account

Overall, we created the following 4 user accounts for the demo:

Account Name	Username	Password	User Group	Purpose
ppuser01	ppuser01	ppuser01	PP User Group	Used for portal username/password login via SSID: "Care_UDT_Portal"
scuser01	scuser01	scuser01	SC User Group	Used for WPA authentication via SSID: "Care_WPA"
ppmac01	44:85:00:99:23:d4	N/A	PP MAC Group	Used for MAC authentication via SSID: "Care_MAC_Auth"
scmac01	9c:4e:36:8c:c9:e0	N/A	SC MAC Group	Used for MAC authentication via SSID: "Care_MAC_Auth"

Step 5c: Batch import of user accounts

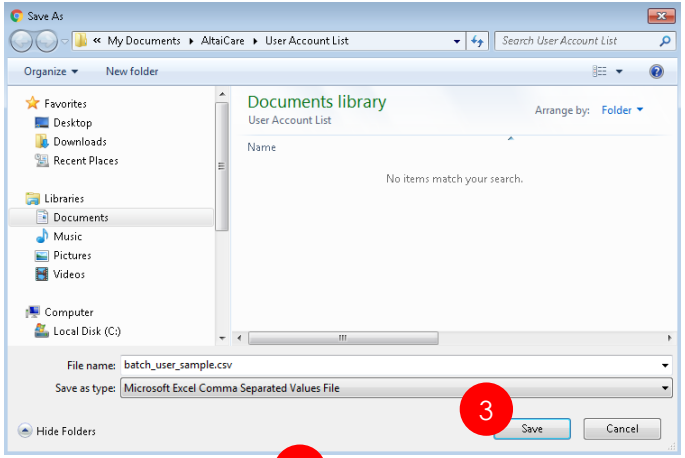


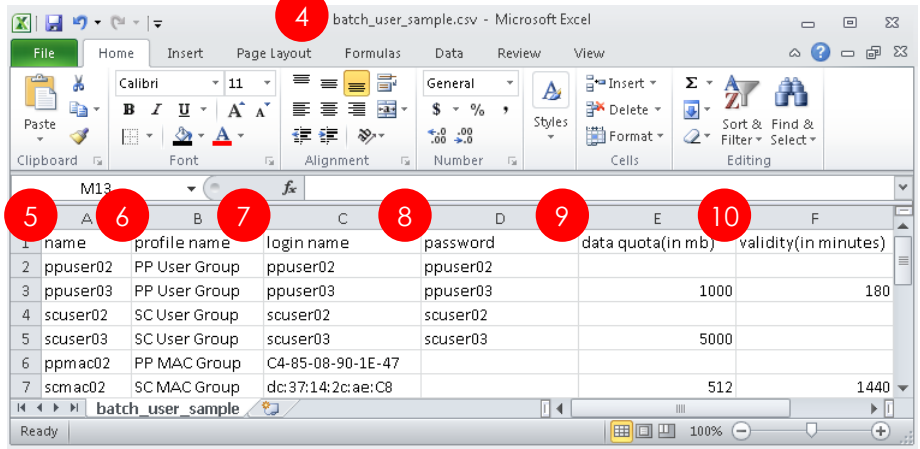
Procedures:

1. Click to pop up a window for importing user list file.
2. Click "Users Sample" to download a user list template.

ALTAI Super WiFi

Step 5c: Batch import of user accounts (Cont.)



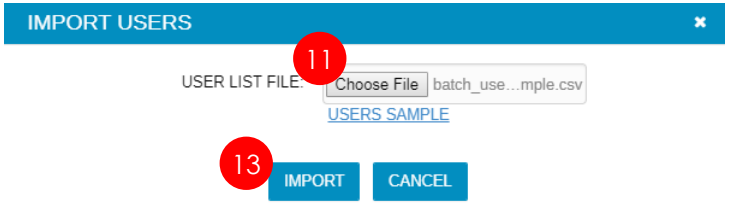


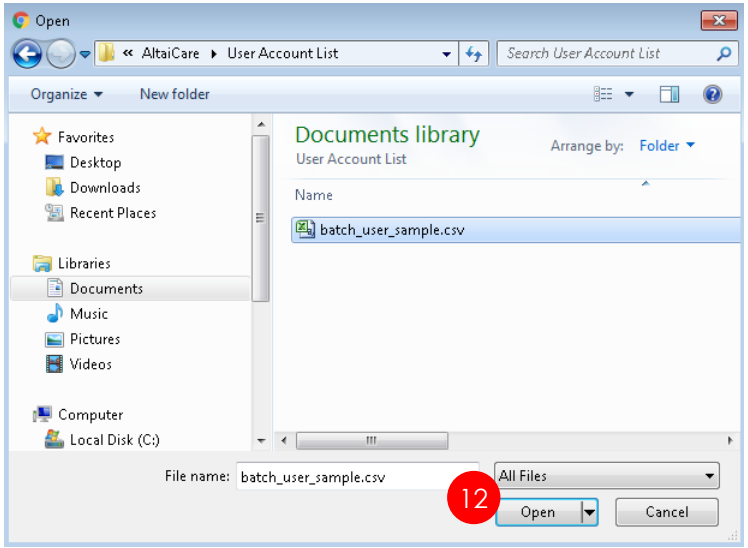
Procedures:

3. Click "Save" button.
4. Open the file "batch_user_sample.csv".
5. Give a name for the account. This name is not used for login.
6. Assign the user account to one of the User Groups which have been created in Step 4, e.g. PP User Group and SC User Group for WPA/Portal Authentication; and PP MAC Group and SC MAC Group for MAC Authentication in our example.
7. Enter Username for user login. For MAC Authentication, the username is the client MAC address can be in **colon-separated** or **hyphen-separated** format with either **uppercase** or **lowercase** alphabets,
   e.g. **XX:XX:XX:XX:XX:XX** or **xx-xx-xx-xx-xx-xx**
8. Enter Password for user login. For MAC Authentication, this item is not applicable and you can keep it blank.
9. Set Data Quota for Prepaid User Account (MB) / Recurrent Data Quota for Subscription User Account (MB). For the term definition, see Step 4: Create User Group – User Account Default Setting. You can specify a custom value for the accounts or leave it blank to use User Group Default Setting of the selected user group in item 5.
10. Set Validity (Min) for the Prepaid User Account. For the term definition, see Step 4: Create User Group – User Account Default Setting. You can specify a custom value for the accounts or leave it blank to use User Group Default Setting of the selected user group in item 5. This item is not applicable to Subscription User Account and you can leave it blank as well.

ALTAI Super WiFi

Step 5c: Batch import of user accounts (Cont.)





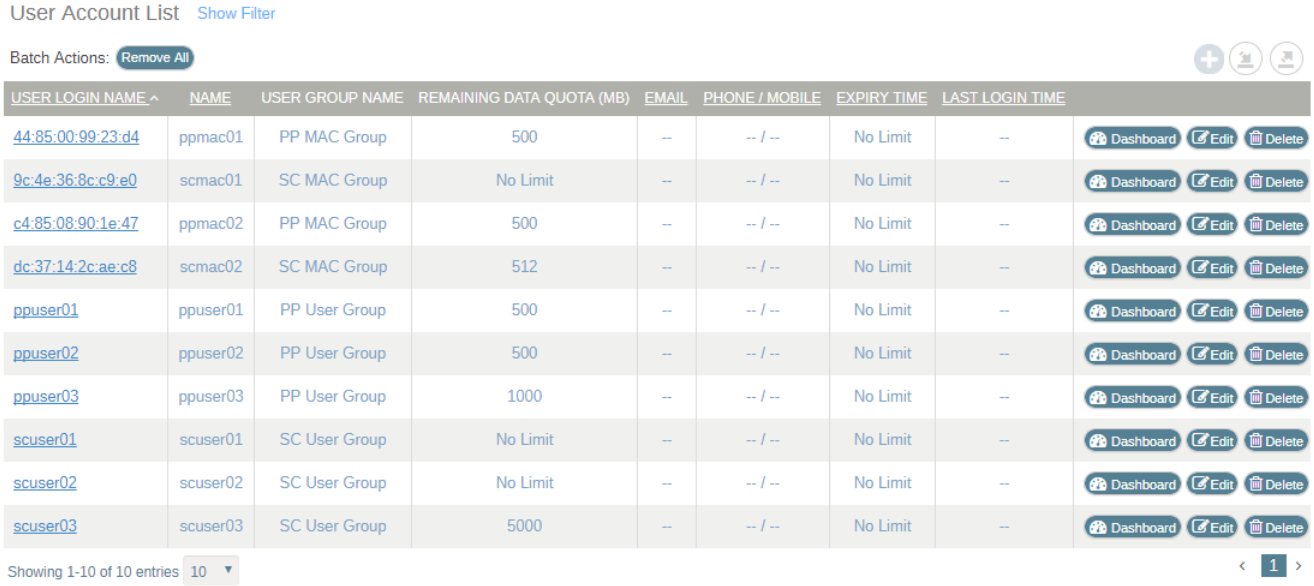
Procedures:

11. Go back to the "Import Users" window and click "Choose File" button to upload the user batch file.
12. A window pops up. Select the modified batch_user_sample.csv file and click "Open" button
13. Click IMPORT button.

Note: You are allowed to import up to 5,000 user account entries for each time of batch import.

ALTAI Super WiFi

Step 5c: Batch import of user accounts (Cont.)



Overall, we created the following 6 user accounts via user batch import:

Account Name	Username	Password	User Group	Purpose
ppuser02	ppuser02	ppuser02	PP User Group	Used for portal username/password login via SSID: "Care_UDT_Portal"
ppuser03	ppuser03	ppuser03	PP User Group	Used for portal username/password login via SSID: "Care_UDT_Portal"
scuser02	scuser02	scuser02	SC User Group	Used for WPA authentication via SSID: "Care_WPA"
scuser03	scuser03	scuser03	SC User Group	Used for WPA authentication via SSID: "Care_WPA"
ppmac02	c4:85:08:90:1e:47	N/A	PP MAC Group	Used for MAC authentication via SSID: "Care_MAC_Auth"
scmac02	dc:37:14:2c:ae:C8	N/A	SC MAC Group	Used for MAC authentication via SSID: "Care_MAC_Auth"

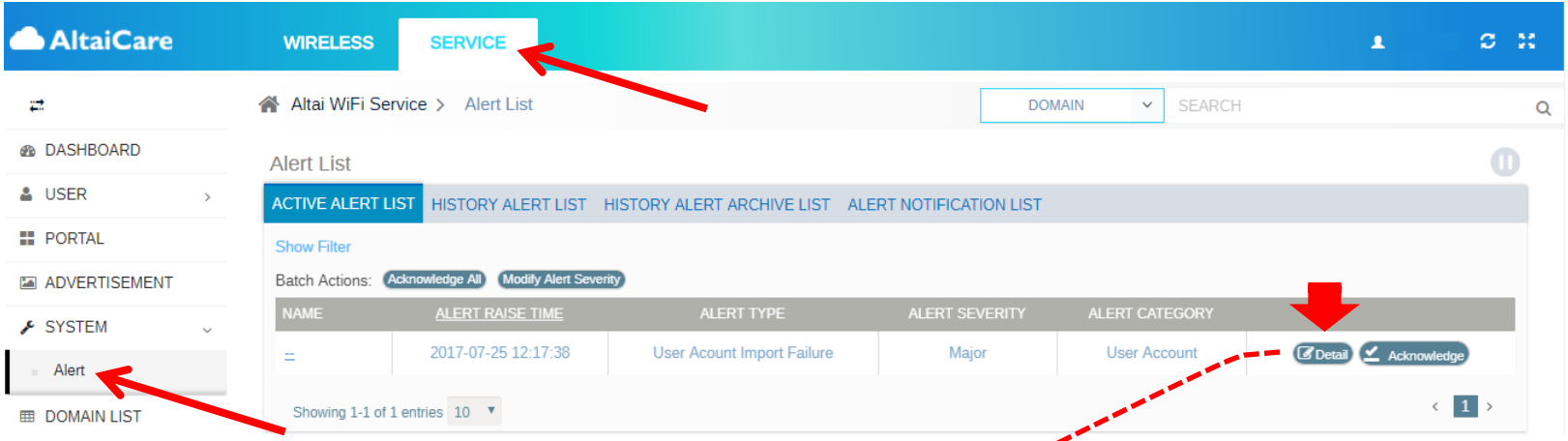
Step 5c: Batch import of user accounts (Cont.)

Note: In case of error during user batch import, it will give you warning  . It might be caused by

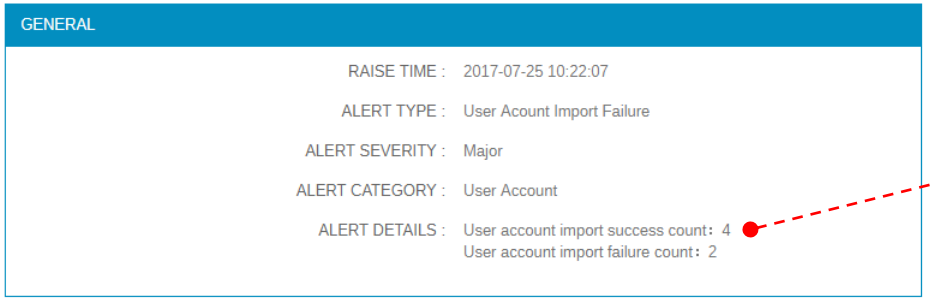
- same account name or username of multiple entries; or
- Inputting a non-existing User Group name

For alarm details, go to the next slide.

Step 5c: Batch import of user accounts (Cont.)



Alert [353488] Detail Info



Tells you how many accounts are successfully created and how many are failed for the event of user account batch import

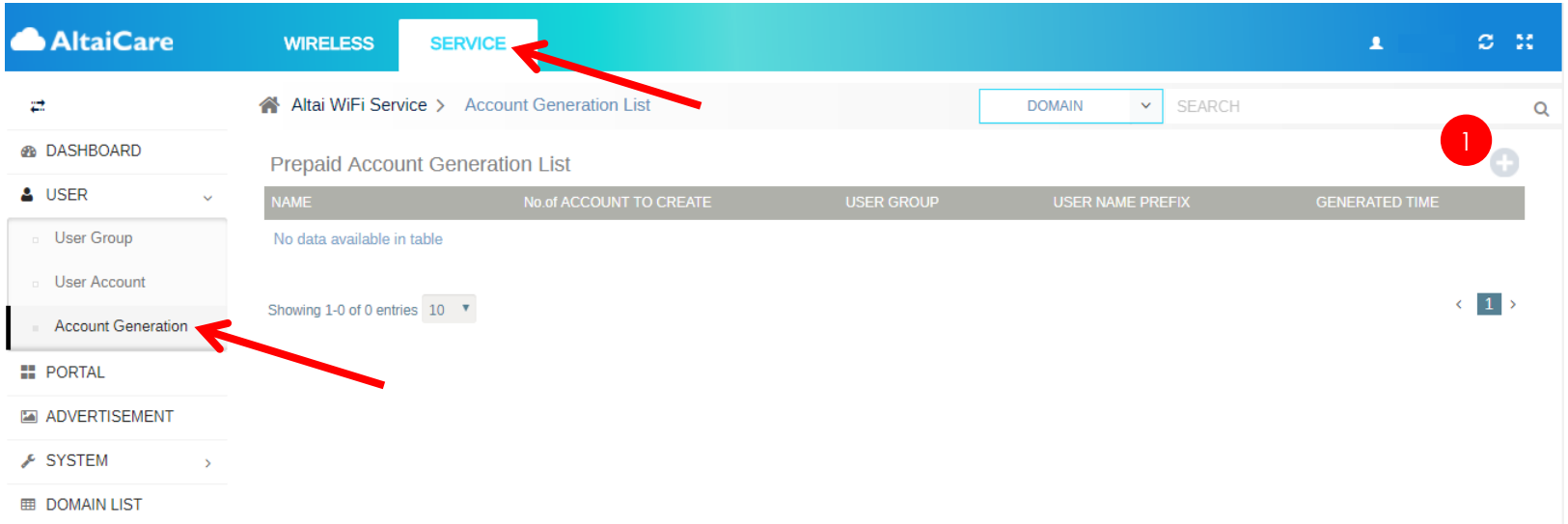
ALTAI Super WiFi

Step 5d: Voucher-based user account batch generation
(For WPA/Portal Prepaid Account ONLY)

Note: For demo purpose, we created a new **WPA/Portal prepaid type** of User Group called "PP Voucher User Group" for user account batch generation in this Section

Procedures:

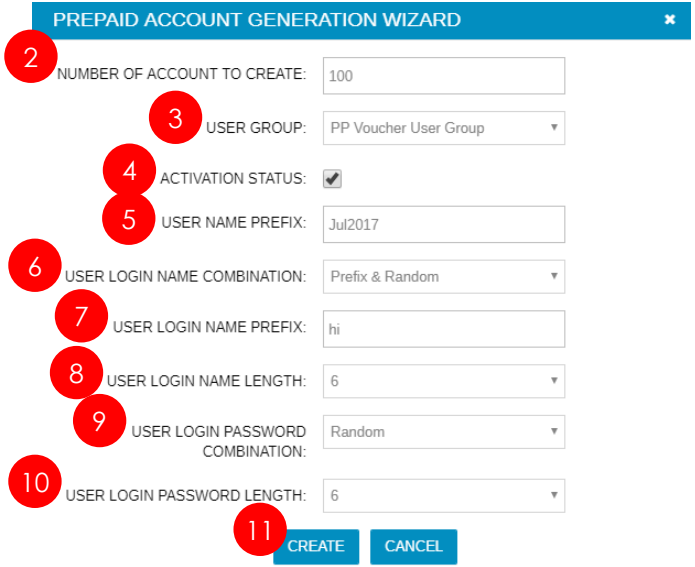
1. Click to pop up a window for prepaid user account batch generation.



Step 5d: Voucher-based user account batch generation (Cont.)
(For WPA/Portal Prepaid Account ONLY)

Procedures:

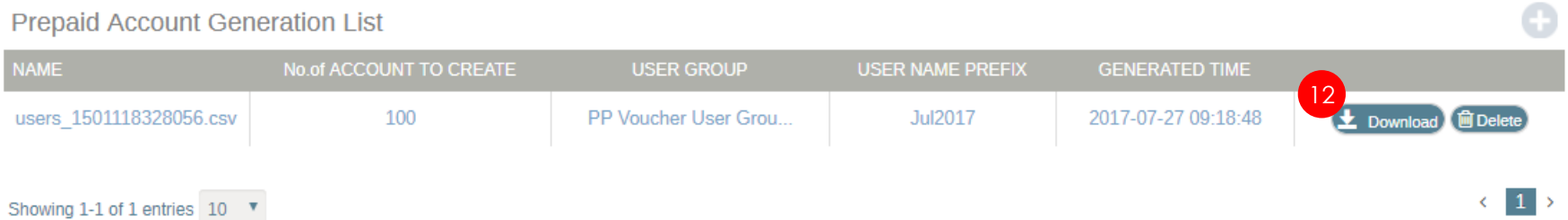
2. Enter the number of user accounts (max 5,000) for one batch generation.
3. Assign the whole batch of accounts to one of the prepaid User Groups that have been created in Step 4. In this example, we assign all 10 accounts to "PP Voucher User Group".
4. Check the box of Activation Status; otherwise, the accounts will become disabled.
5. Give a user name prefix of 1-8 characters long for the batch identification. The account name which is in form of "<Prefix>_<Index starting from 1>" is not used for user login. In this example, we give it as "Jul2017".
6. Select one of the following options for User Login Name Combination:
   - **Prefix & Index**: With this option selected, user names will be in form of "<Prefix which is defined in item #7><Index starting from 0>"
   - **Prefix & Random**: With this option selected, user names will be in form of "<Prefix which is defined in item #7><Random generated string of length defined in item #8>"
   - **Random**: With this option selected, user names will be in form of "<Randomly generated string of length defined in item #8>"
7. Input a string of 1-64 characters long as User Login Name Prefix. It is not applicable to the option "Random" of User Login Name combination.
8. Set the random string length to be (i) 6, or (ii) 8, or (iii) 10, or (iv) 12 characters long. The string is a part of the User Login Name and not applicable to the option "Prefix & Index" of User Login Name Combination.

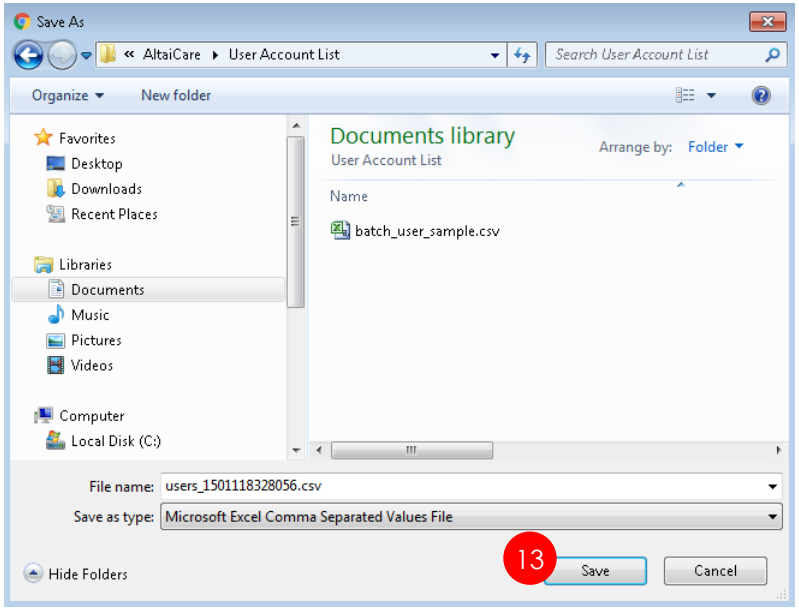


9. Select one of the following options for User Login Password Combination:
   - **Same As Login Name**: With this option selected, the password will be set identical to the User Login Name
   - **Random**: With this option selected, the password will be in form of "<Randomly generated string of length defined in item #10>"
10. Set the random string length to be (i) 6, or (ii) 8, or (iii) 10, or (iv) 12 characters long. It is not applicable to the option "Same As Login Name" of User Login Password Combination.
11. Click CREATE

ALTAI Super WiFi

Step 5d: Voucher-based user account batch generation (Cont.)
(For WPA/Portal Prepaid Account ONLY)





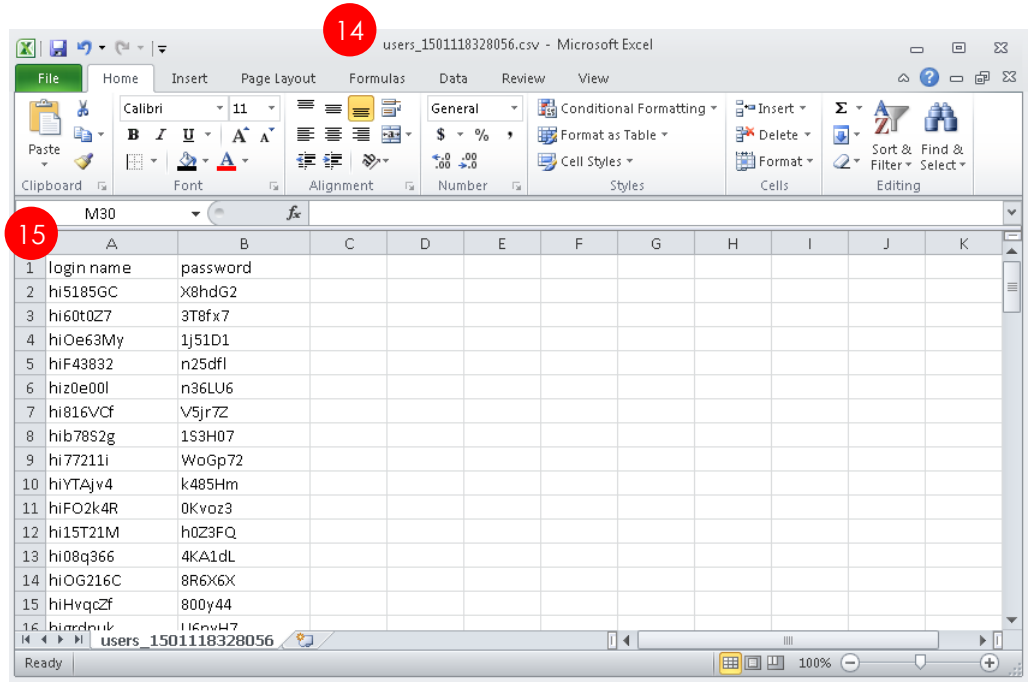
Note: It will take a moment for user account importing and generation. The length of duration depends on the amount of user accounts.

Procedures:

12. A new entry with a user account list (.CSV file) is created. Click Download
13. A window pops up. Select the destination path for file download and then click "Save" button.

ALTAI Super WiFi

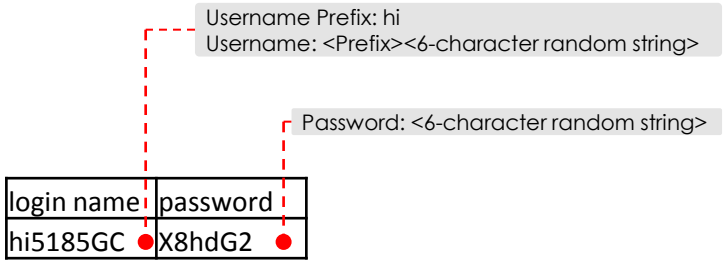
Step 5d: Voucher-based user account batch generation (Cont.)
(For WPA/Portal Prepaid Account ONLY)



	A	B
1	login name	password
2	hi5185GC	X8hdG2
3	hi60t0Z7	3T8fx7
4	hiOe63My	1j51D1
5	hiF43832	n25dfl
6	hiz0e00l	n36LU6
7	hi816VCf	V5jr7Z
8	hib78S2g	1S3H07
9	hi77211i	WoGp72
10	hiYTAjv4	k485Hm
11	hiFO2k4R	0Kvoz3
12	hi15T21M	h0Z3FQ
13	hi08q366	4KA1dL
14	hiOG216C	8R6X6X
15	hiHvqcZf	800y44

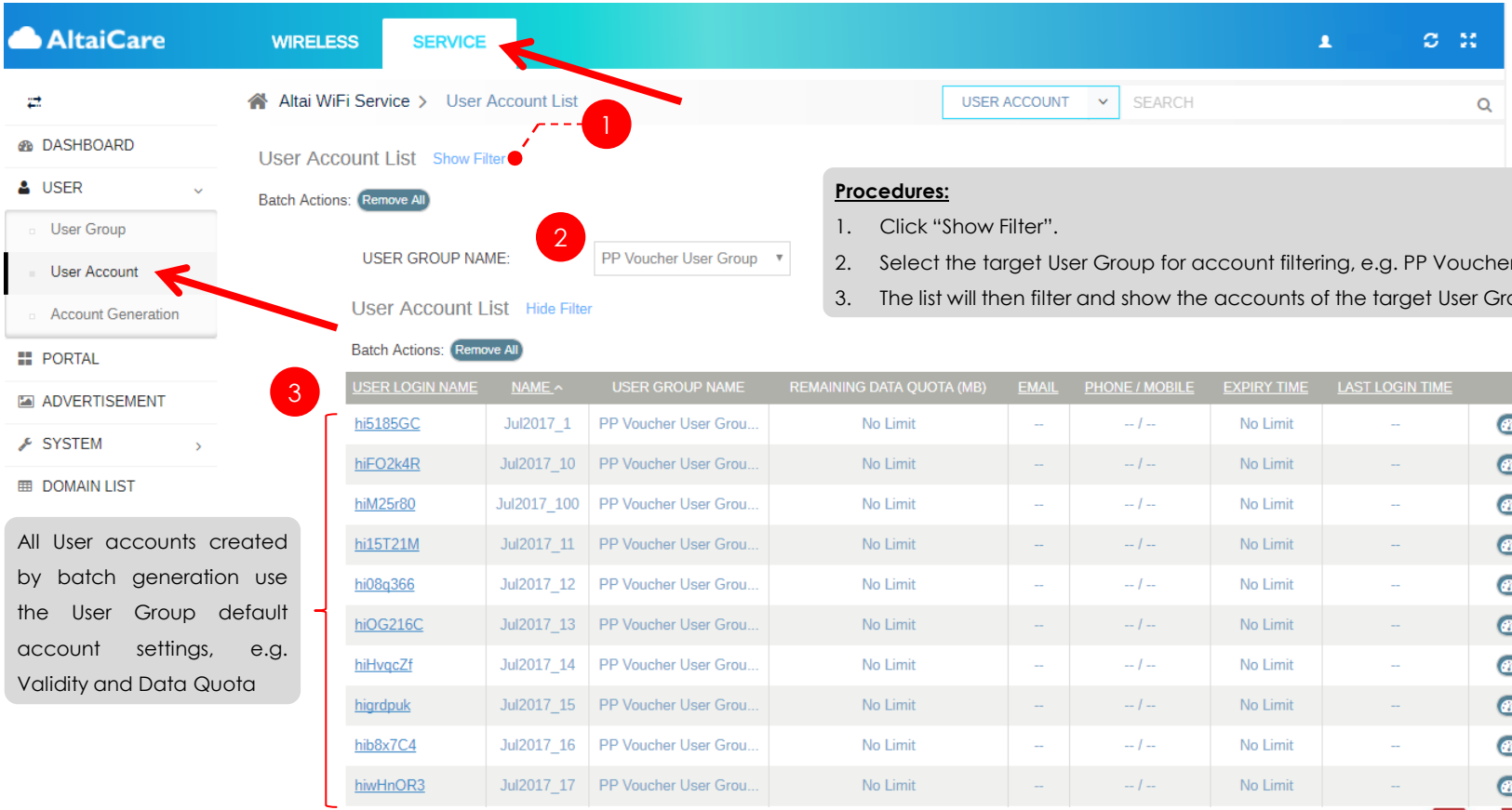
Procedures:

14. Open the .CSV file and you will have a list of prepaid user accounts that are just created by the system. You can make use of the list to prepare your own vouchers.
15. In our example, we have 100 pairs of different username/password combination for demo purpose.



ALTAI Super WiFi

Step 5d: Voucher-based user account batch generation (Cont.)
(For WPA/Portal Prepaid Account ONLY)



Procedures:

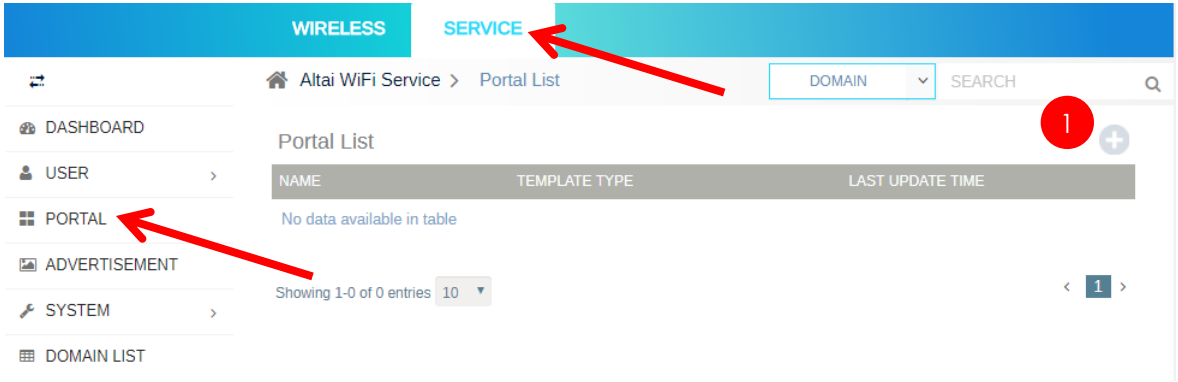
1. Click "Show Filter".
2. Select the target User Group for account filtering, e.g. PP Voucher User Group.
3. The list will then filter and show the accounts of the target User Group.

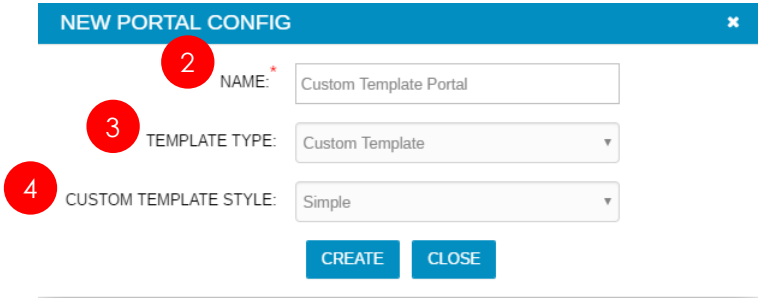
All User accounts created by batch generation use the User Group default account settings, e.g. Validity and Data Quota

ALTAI Super WiFi

Step 6a: Custom Template Portal Setup

Step 6a: Custom Template Portal Setup – Create Portal



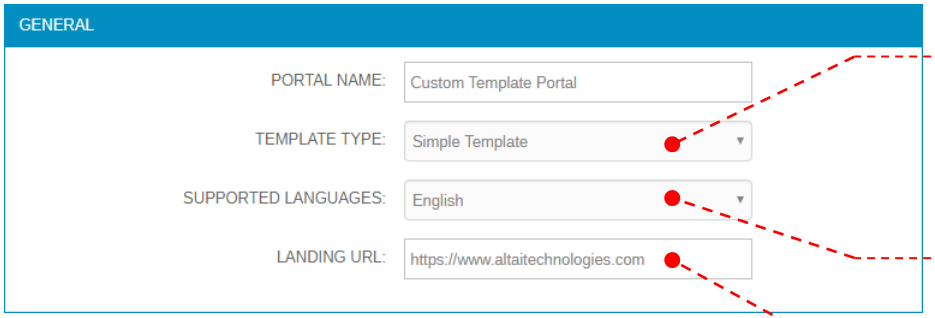


Procedures:

1. Click to create and enable new portal service.
2. Give a name for the new portal.
3. Select "Custom Template" for template type.
4. Pick one of the Custom Template Styles. You can change it later.

ALTAI Super WiFi

Step 6a: Custom Template Portal Setup – General & Login/Sign-Up Methods



Provide 6 different options of layout for the portal page background and body

- Simple
- Clear
- Blur
- Grid
- Curvy
- Stylish

Provide 3 options of portal page language

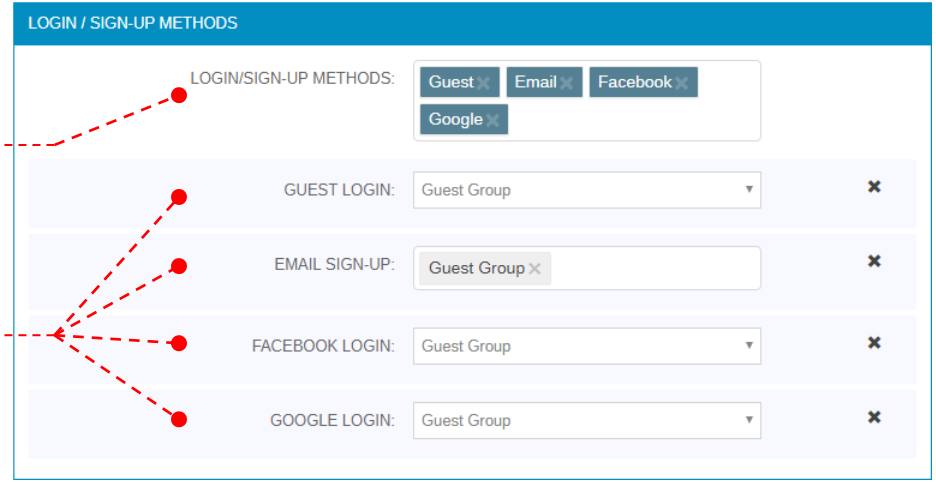
- English
- Simplified Chinese
- Both of them

Specify the URL to which the users will be redirected upon successful authentication

Select your desired login methods for your portal. There are four login types you can choose from Custom Template Portal Mode:

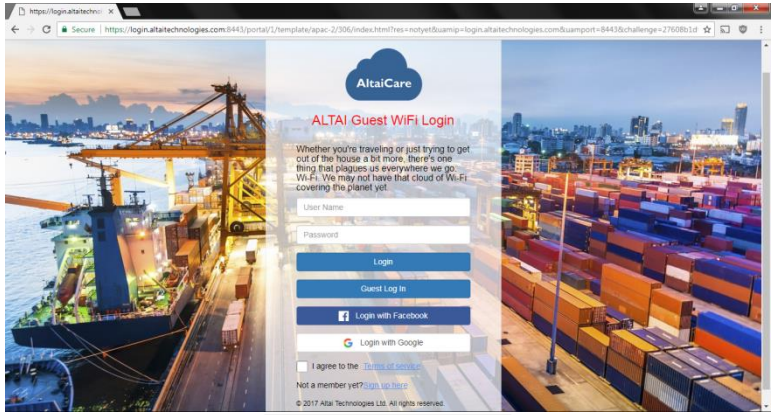
- Guest Login (Single button login without providing personal information)
- Email Sign Up with verification code return for login
- Social Account Login with Facebook and Google+ accounts support

Assign User Groups for those auto-generated accounts for different login methods

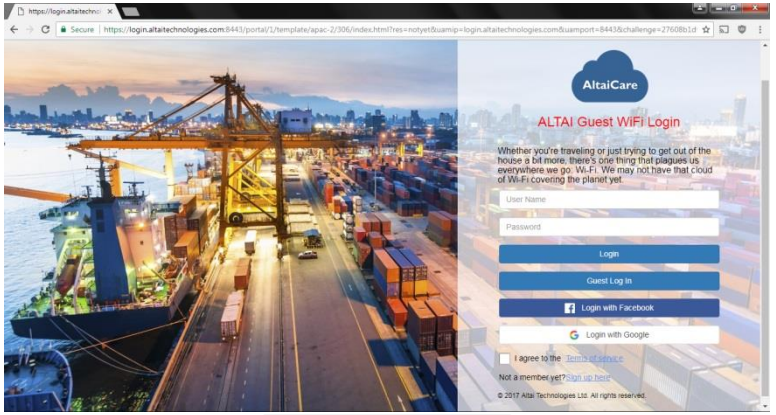


ALTAI Super WiFi

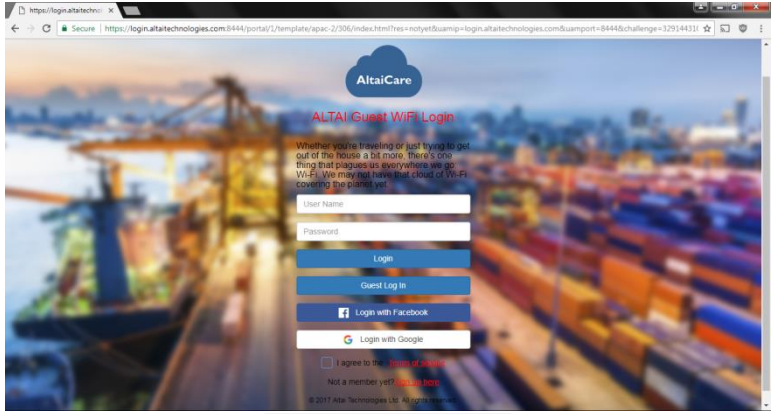
Step 6a: Custom Template Portal Setup – General & Login/Sign-Up Methods (Cont.)



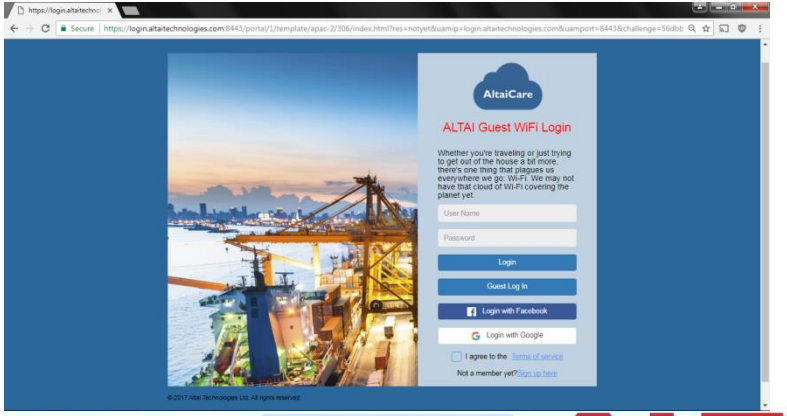
Simple Type Template



Clear Type Template



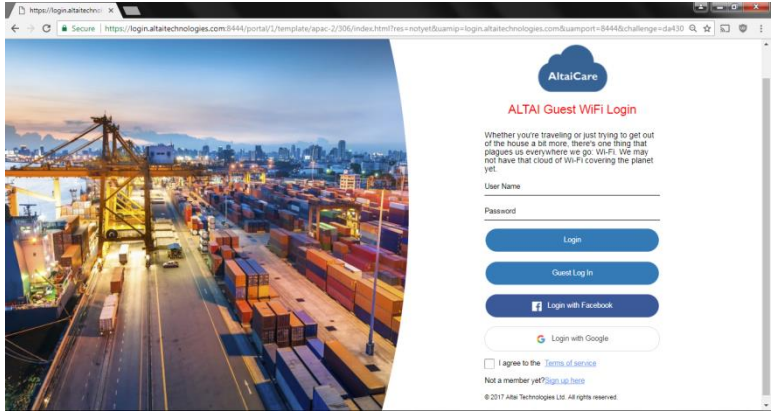
Blur Type Template



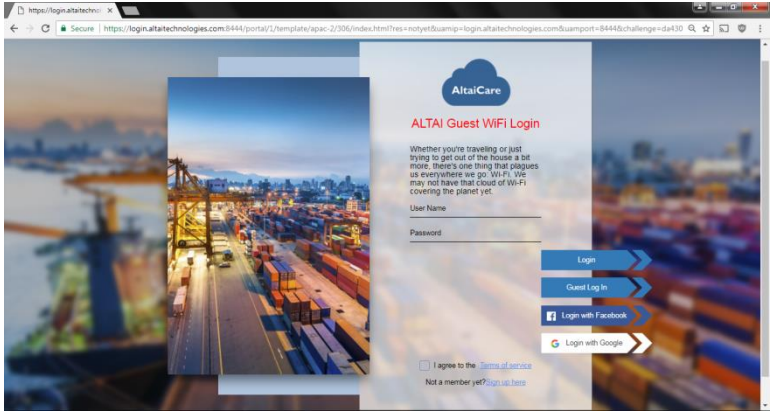
Grid Type Template

ALTAI Super WiFi

Step 6a: Custom Template Portal Setup – General & Login/Sign-Up Methods (Cont.)



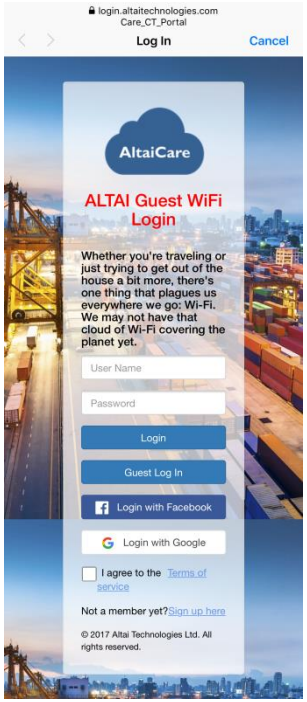
Curvy Type Template



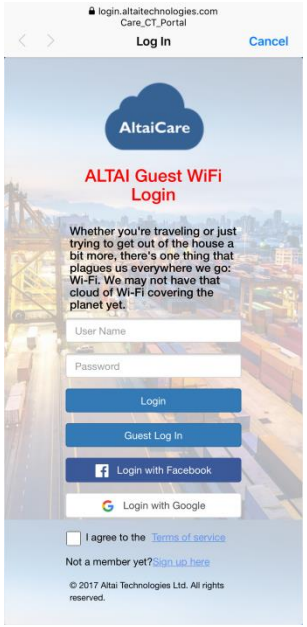
Stylish Type Template

ALTAI Super WiFi

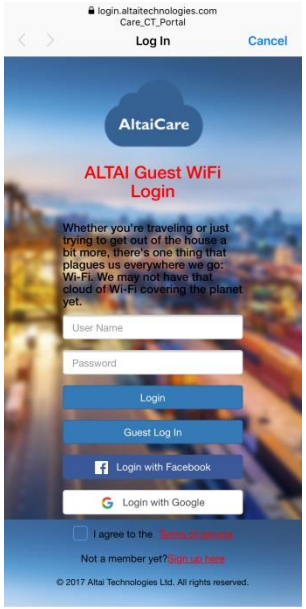
Step 6a: Custom Template Portal Setup – General & Login/Sign-Up Methods (Cont.)



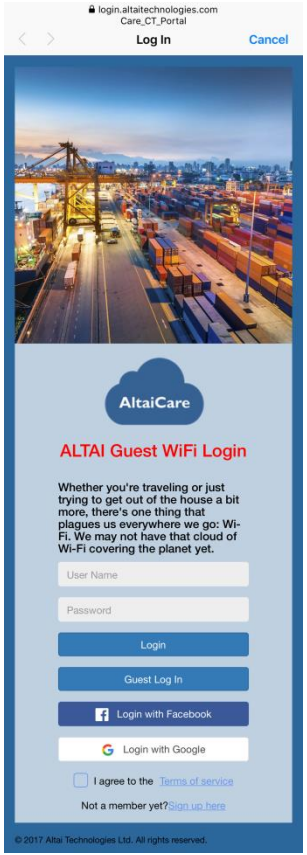
Simple Type Template



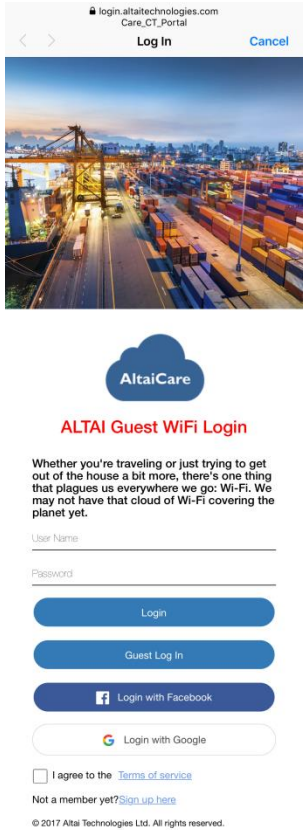
Clear Type Template



Blur Type Template



Grid Type Template



Curvy Type Template

Stylish Type Template

Note: Screenshots from iOS

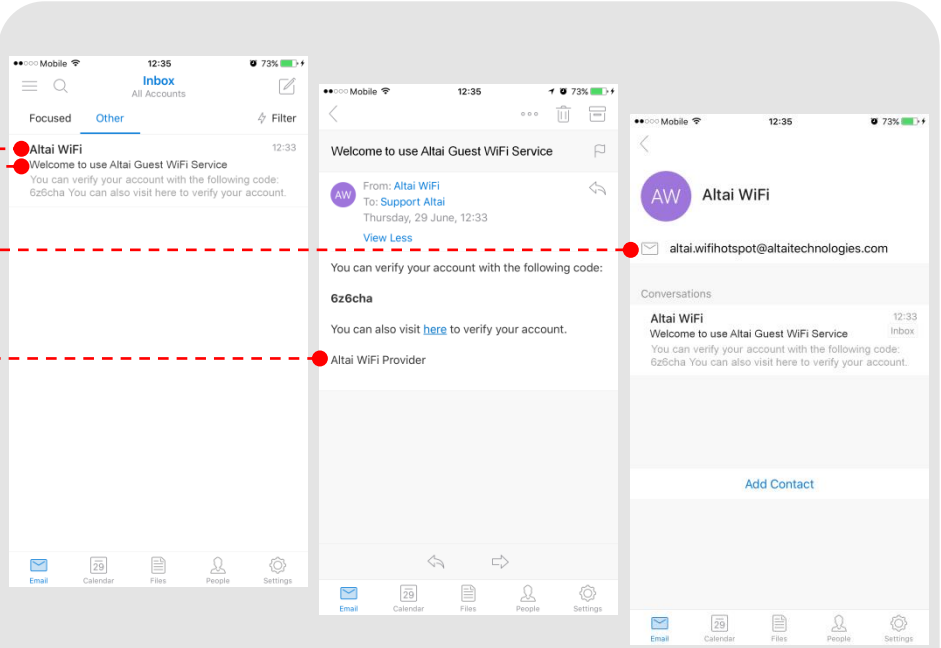
ALTAI Super WiFi

Step 6a: Custom Template Portal Setup – Email Configuration (For Email Sign-Up Only)

Note: This part of configuration is for Email sign up only. AltaiCare System will masquerade as the sender name and Email to send the verification code to end users for their login.

EMAIL CONFIGURATION

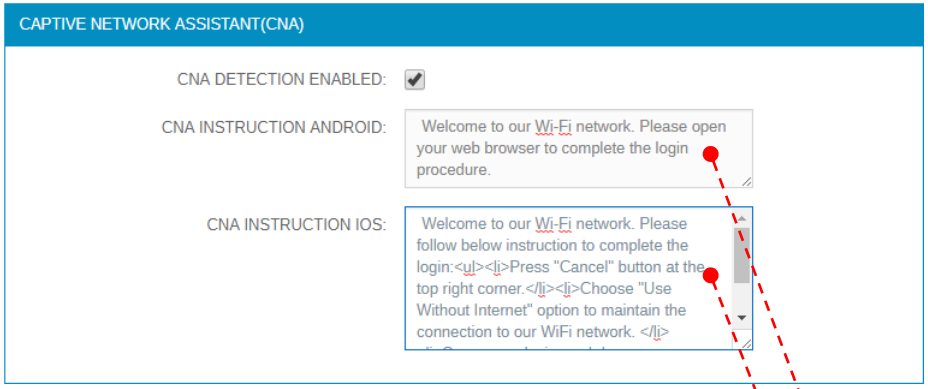
SENDER EMAIL:*	altai.wifihotspot@altaitechnologies.com
SENDER NAME:*	Altai WiFi
EMAIL HEADER:*	Welcome to use Altai Guest WiFi Service
SIGNATURE:*	Altai WiFi Provider



Note: Screenshots from outlook app (iOS version)

ALTAI Super WiFi

Step 6a: Custom Template Portal Setup – Captive Network Assistant



CNA pop-up instruction for iOS

Note: CNA (Captive Network Assistant) is an app which is commonly pre-installed in most of IOS and Android devices. The purpose of it is to assist users to go through portal authentication process without user intervention of opening web browser when accessing open network with the requirement of captive portal authentication.

It automatically pops up a window for user login when the mobile devices detect the network with the presence of captive portal enabled. From user perspectives, it greatly improves user experience and get rid of the awkwardness when people are not aware of the requirement of opening web browser to log in the open WiFi network.

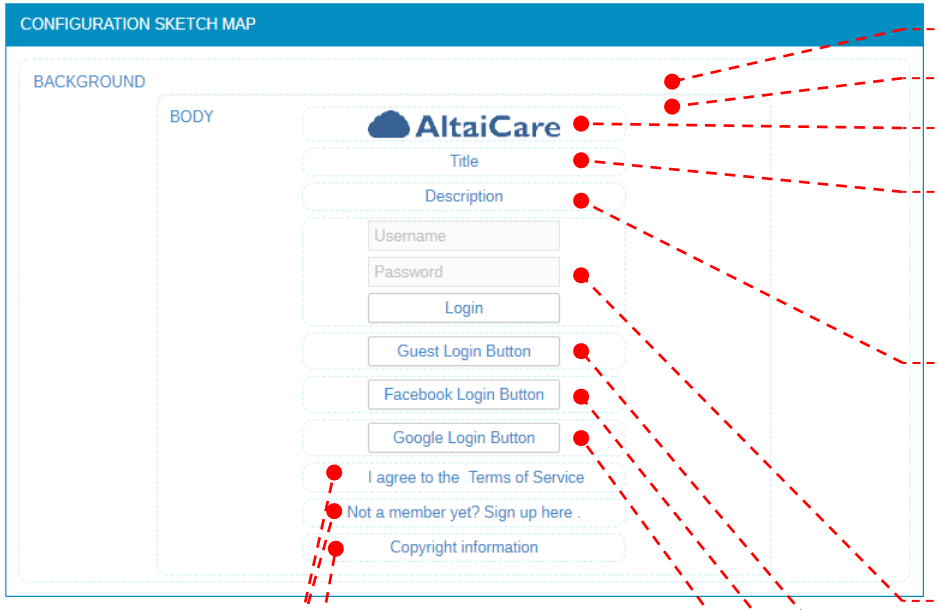
However, the app is not like other web browsers such as Safari, Chrome, … It supports very limited functions and may even not be desirable when it comes to particular login methods. For this case, we may need a way to guide the users how to bypass the CNA and use the standard web browsers to proceed the web portal authentication.

Here, we will make use of the CNA feature but not to provide an interface for user login. Instead, we **give instructions on the pop up window to guide the users through the process to bypass CNA appropriately and log in the portal with standard web browsers**.

Input instructions here for Android devices. This instruction page will be popped up without showing up login page once the users click on the open network SSID with captive portal detected.

Input instructions here for iOS devices. And this pop up instruction is supported for **Google social account login ONLY**. For the rest of login methods, it will pop up portal login page.

Step 6a: Custom Template Portal Setup – Configuration Sketch Map



Background: Either pick color in RGBA from palette or choose a desired image for the portal page background.

Body: Pick color in RGBA from palette for the portal page body.

Logo (Optional): Upload an image of company logo and put it at the top of the body.

Title: Add title for the portal page. You can align the text position, change the text color and font size

Description Content: Add text for the page content. You can have the following operations on the text:

- Font Size
- Font Color
- Bold
- Align Text Left, Center, Right
- Insert/Remove Hyperlink; which is usually used with ACL (Access Control List) to let Portal users click on the hyperlink in the login page and they will then be redirected to the desired URL which is specified in this item without going through the portal authentication.

Username/Password Login Box (for Email Sign Up ONLY): It is used by exiting users who already got an account through their first time sign up login for the network access. Here, Username refers to the user's email address that is used for sign up and Password refers to the user-defined code during sign up process.

You can modify the text of the Username and Password placeholders and the text and color of the Submit Button.

Guest Login Button (for Single Button Login ONLY): You can modify the text and color of the button.

Facebook Login Button (for Facebook Social Account Login ONLY): You can modify the text of the button.

Google Login Button (for Google Social Account Login ONLY): You can modify the text of the button.

Refer to the next few slides

Copyright Information: Edit the text and color for the copyright notice which is to be put at the bottom of the portal page.

ALTAI Super WiFi

Step 6a: Custom Template Portal Setup – Setting & Operation of Terms of Service

TERMS OF SERVICE(TOS) SETTING

MAIN PAGE

TOS LABEL: Terms of Service

TOS REMINDER TEXT: You have to agree the terms of service in order to

POP UP PAGE

TOS DETAIL: large

Terms of Service ("this TOS")

1. Access to this Service

TOS DETAIL COLOR: rgba(0,0,0,1)

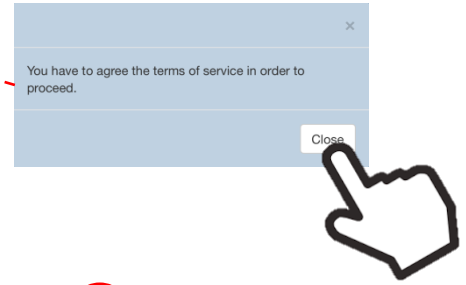
1

Attempt to sign in without checking the box of the "Terms of Service"

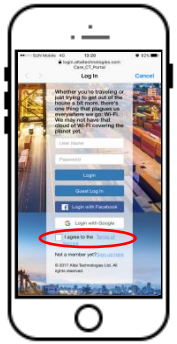
2

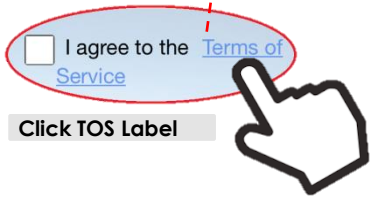
A TOS reminder window pops up immediately to remind the users to check the box to agree the TOS first before getting WiFi service.

Then click "Close" button and return to portal main page



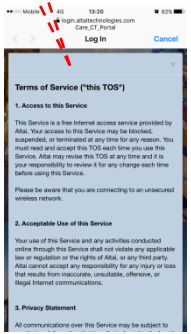
3





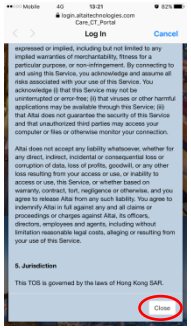
Click TOS Label

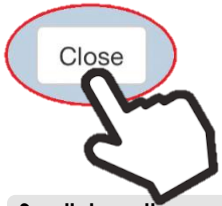
4



A TOS page pops up

5





Scroll down the page to the bottom, and click "Close" button to return to portal main page

6

Check the TOS box and sign in again. The system will then further proceed the sign up process.

ALTAI Super WiFi

Step 6a: Custom Template Portal Setup – Sign-Up Setting (For Email Sign Up Only)

SIGNUP SETTING

MAIN PAGE

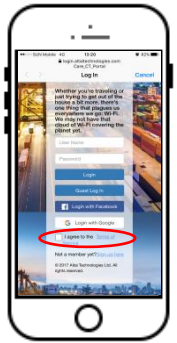
SIGN UP LINK PREFIX:	Not a member yet?
SIGN UP LINK:	Sign up here

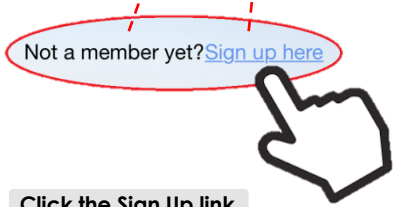
POP UP PAGE

SIGN UP EMAIL PLACEHOLDER:	Email Account
SIGN UP PASSWORD PLACEHOLDER:	Password
SUBMIT BUTTON TEXT:	Sign up Submit

Note: This setting is for Email sign up ONLY

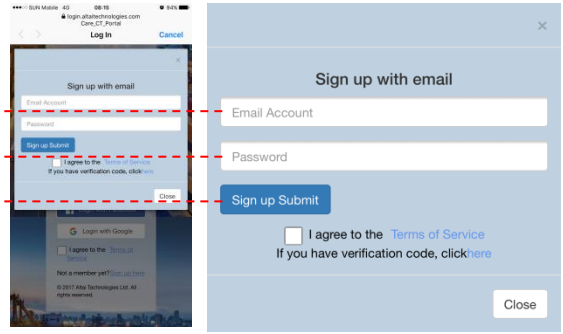
1





Click the Sign Up link for Email sign up

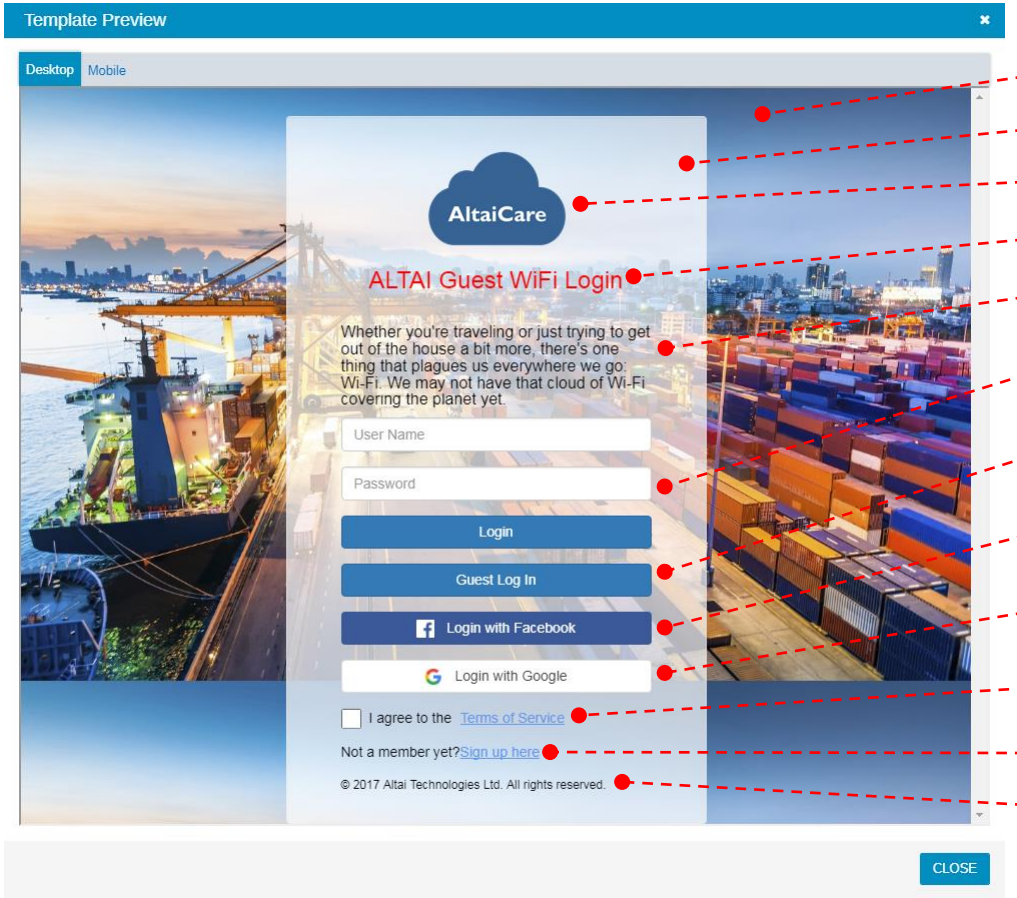
2



Window pops up for users to sign up with Email and user-defined password which are to be used for login in the future

ALTAI Super WiFi

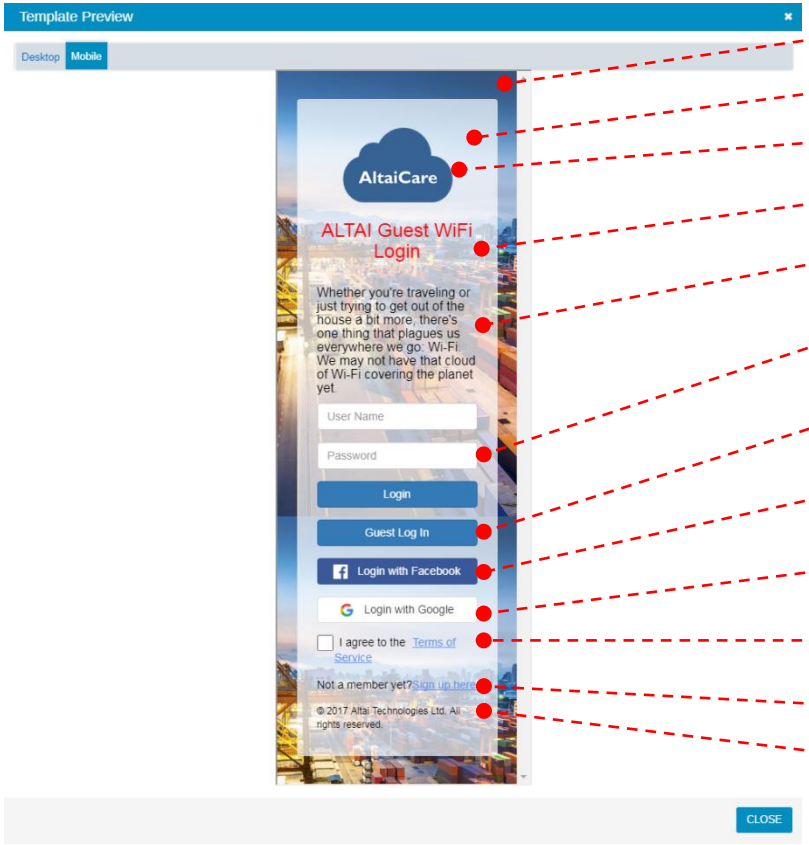
Step 6a: Custom Template Portal Setup – Template Preview (Desktop)



- Background
- Body
- Logo (Optional)
- Title
- Description Content
- Username/Password Login Box (for Email Sign Up ONLY)
- Guest Login Button (for Single Button Login ONLY)
- Facebook Login Button (for Facebook Account Login ONLY):
- Google Login Button (for Google Account Login ONLY):
- Term of Service Statement and Link with Checkbox
- Email Sign Up (For first time login)
- Copyright Information

ALTAI Super WiFi

Step 6a: Custom Template Portal Setup – Template Preview (Mobile)



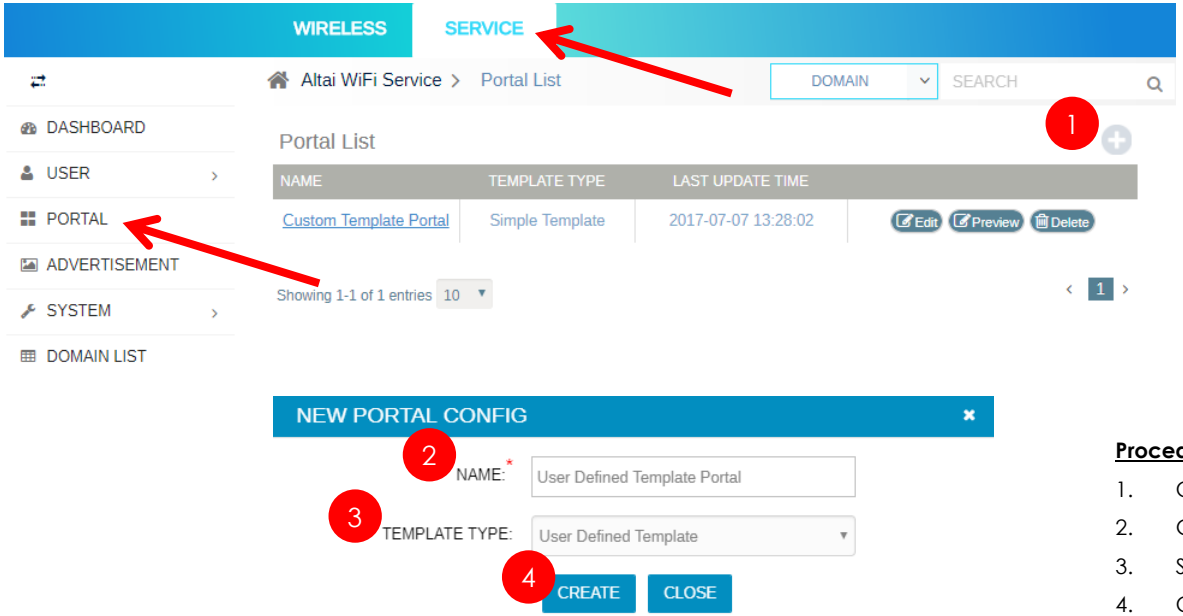
- Background
- Body
- Logo (Optional)
- Title
- Description Content
- Username/Password Login Box (for Email Sign Up ONLY)
- Guest Login Button (for Single Button Login ONLY)
- Facebook Login Button (for Facebook Account Login ONLY):
- Google Login Button (for Google Account Login ONLY):
- Term of Service Statement and Link with Checkbox
- Email Sign Up (For first time login)
- Copyright Information

ALTAI Super WiFi

Step 6b: User Defined Template Portal Setup

ALTAI Super WiFi

Step 6b: User Defined Template Portal Setup – Create Portal



Procedures:

1. Click ⊕ to create and enable new portal service.
2. Give a name for the new portal.
3. Select "User Defined Template" for template type.
4. Click CREATE to confirm the portal setup.

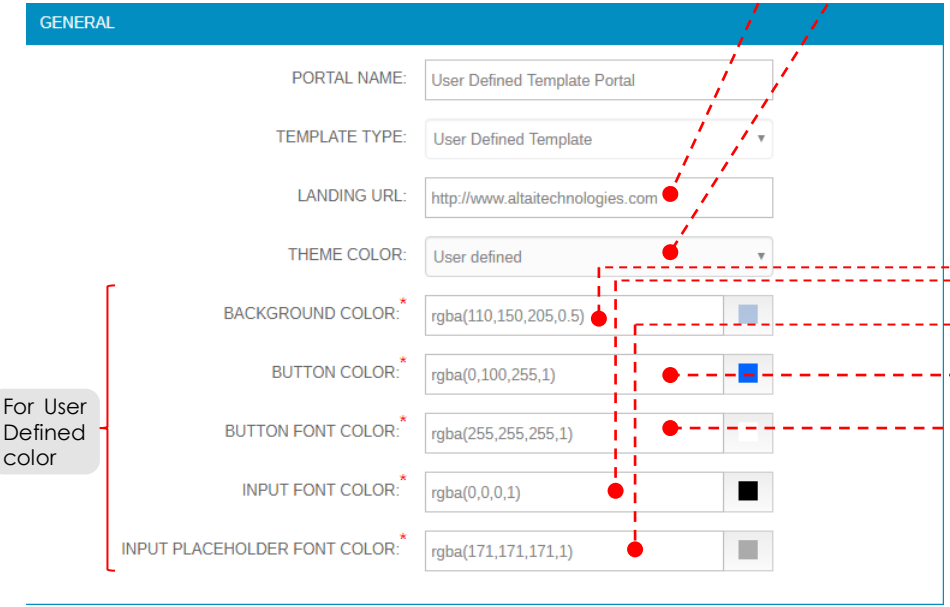
ALTAI Super WiFi

Step 6b: User Defined Template Portal Setup – General

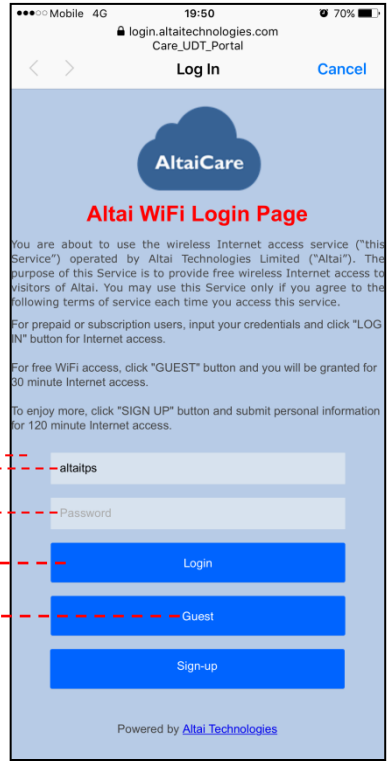
Specify the URL to which the users will be redirected upon successful authentication

Provide 6 different options of theme color for the portal page background:

- Deep Blue
- Green
- Red
- Orange
- No Color
- User Defined



For User Defined color



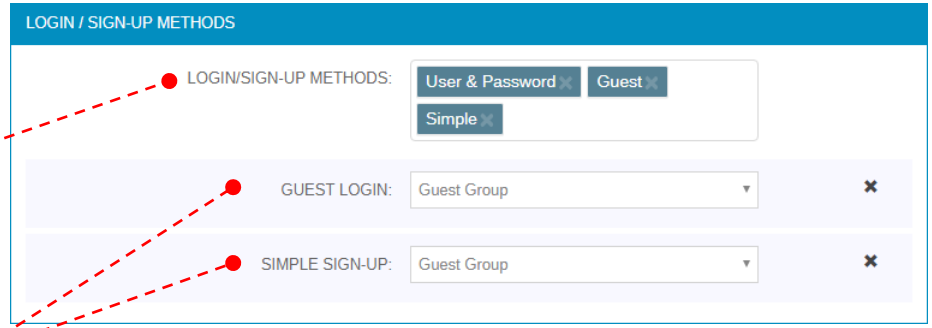
ALTAI Super WiFi

Step 6b: User Defined Template Portal Setup – Login Methods

Select your desired login methods for your portal. There are three login types you can choose from User Defined Template Portal Mode:

- User/Password Login
- Guest Login (Single button login without providing personal information)
- Simple Sign Up (without verification code return for login)

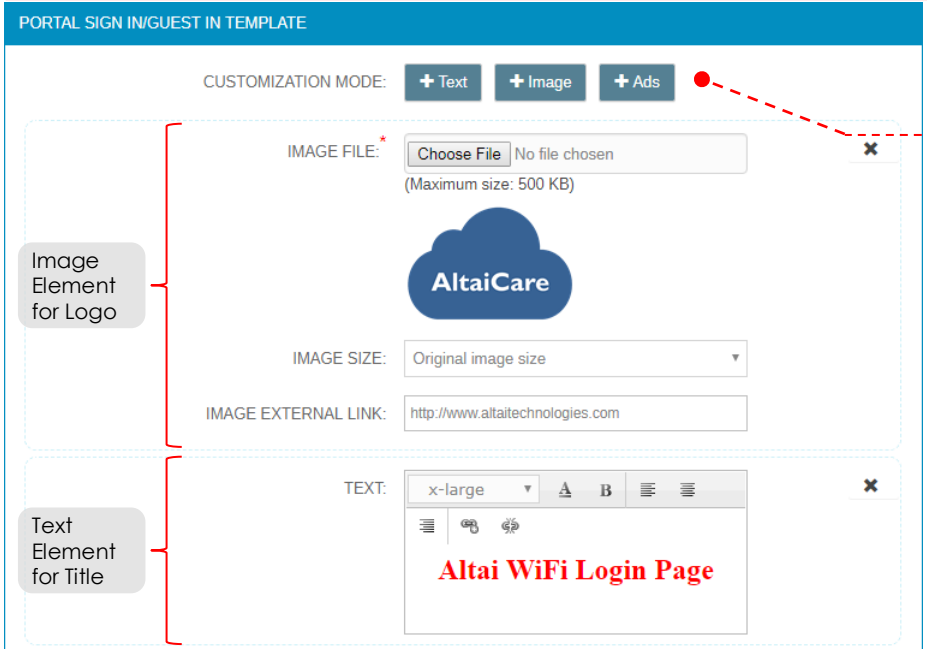
Assign User Groups for those auto-generated accounts for Guest Login and Simple Sign Up methods



Note: For those users using Username/Password type of login, their accounts are all pre-registered and assigned to prepaid or subscription model in the system (Step 5). As to which user groups to be allowed for authentication via the portal, we will define it in RADIUS setting of security profile later (Step 7 item 10).

ALTAI Super WiFi

Step 6b: User Defined Template Portal Setup – Portal Layout (Sign In/Login Page)



Customization Mode: Three types of customization elements can be added to the login page:

- Text
- Image
- Ads (which will be discussed in Advanced Setting later)

You can click "+ Add" button to add multiple text elements and image elements to the login page if needed.

Image Element:

- **Image File**: Click "Choose File" button to upload an image from the local computer to AltaiCare. Maximum size of the image should not exceed 500KB
- **Image Size**: Two options available:
  (1) Adaptive Size; which sets the image size adaptive to the login window
  (2) Original Image Size
- **Image External Link**: It's for embedding hyperlink in the image. Upon a click on the image on the login page, users will then be redirected to the desired URL which is specified in this item without going through the portal authentication.

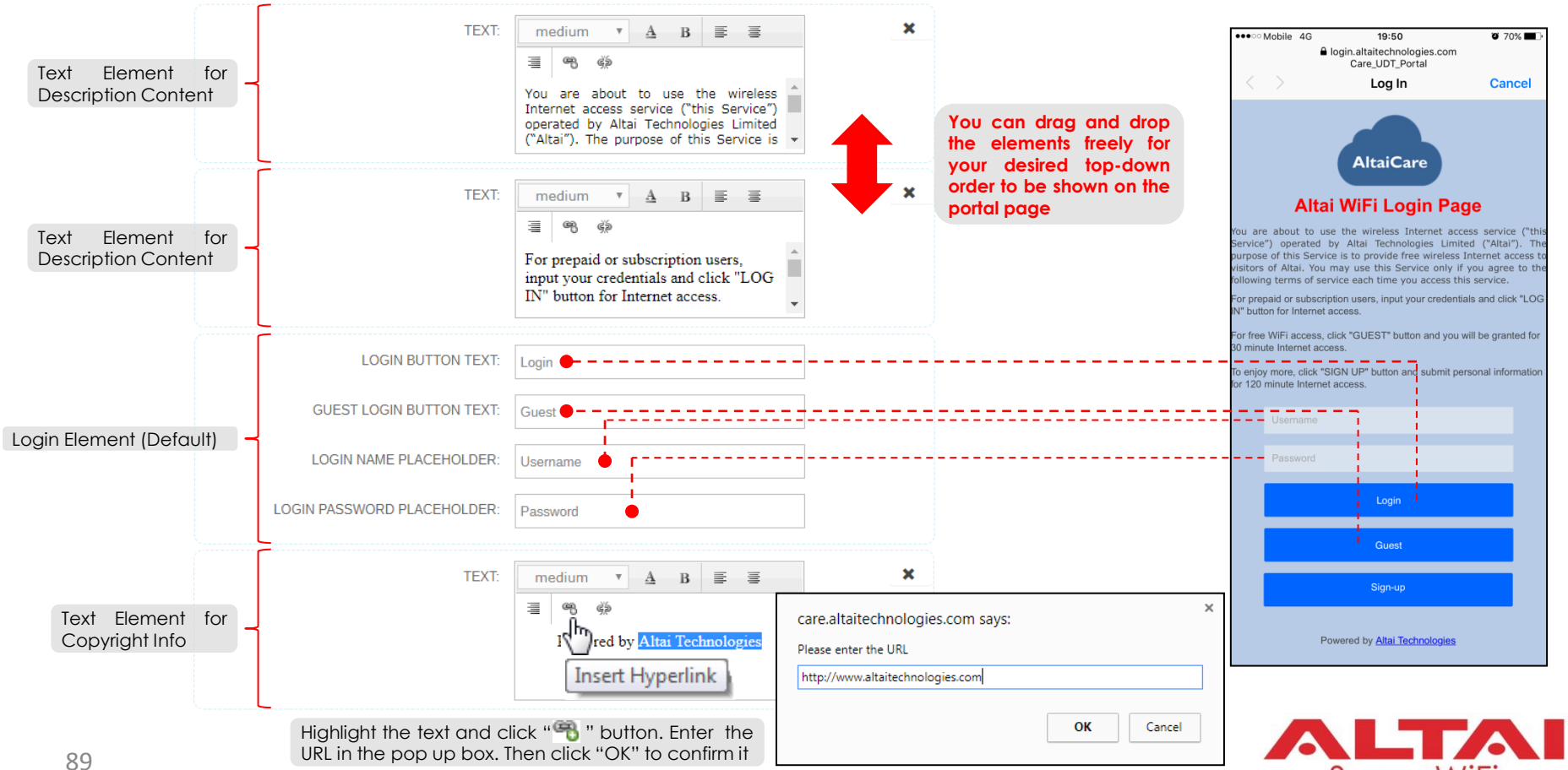
You can drag and drop the elements freely for your desired top-down order to be shown on the portal page

Text Element: You can have the following operations on the text:

- Font Size
- Font Color
- Bold
- Align Text Left, Center, Right
- Insert/Remove Hyperlink; which is usually used with ACL (Access Control List) to let users click on the hyperlink on the login page and they will then be redirected to the desired URL which is specified in this item without going through the portal authentication. For detailed ACL setting, see the following section.

ALTAI Super WiFi

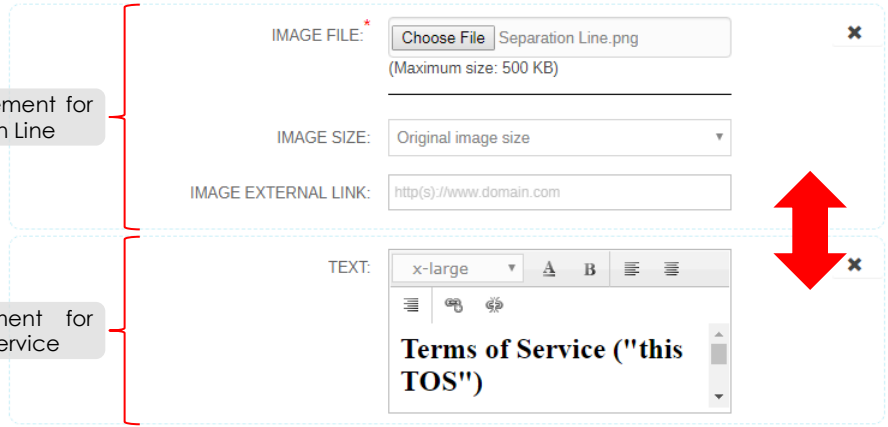
Step 6b: User Defined Template Portal Setup – Portal Layout (Sign In/Login Page) (Cont.)



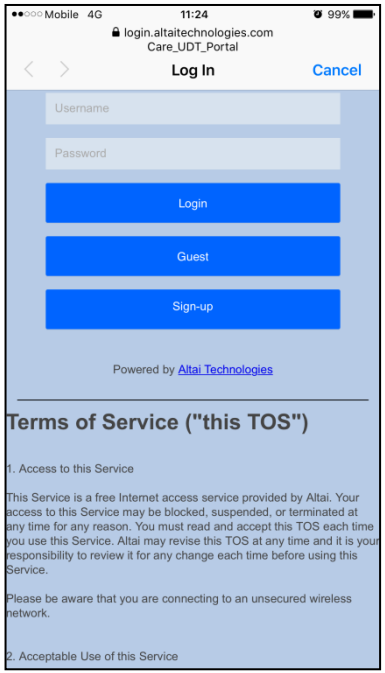
Step 6b: User Defined Template Portal Setup – Portal Layout (Sign In/Login Page) (Cont.)

Image Element for Separation Line

Text Element for Terms of Service



You can drag and drop the elements freely for your desired top-down order to be shown on the portal page



ALTAI Super WiFi

Step 6b: User Defined Template Portal Setup – Portal Layout (Sign Up Page)

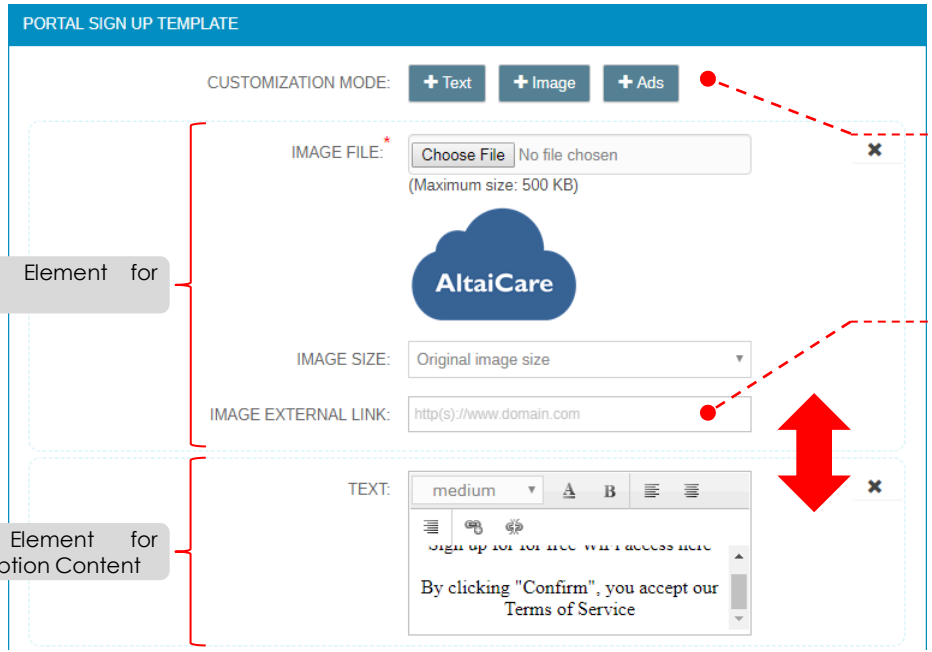


Image Element for Logo

Text Element for Description Content

Customization Mode: Three types of customization elements can be added to the login page:

- Text
- Image
- Ads (which will be discussed in Advanced Setting later)

You can click "+ Add" button to add multiple text elements and image elements to the login page if needed.

Image External Link is an optional item. This time we do not embed any URL in the logo in the sign up page.

You can drag and drop the elements freely for your desired top-down order to be shown on the portal page

ALTAI Super WiFi

Step 6b: User Defined Template Portal Setup – Portal Layout (Sign Up Page) (Cont.)

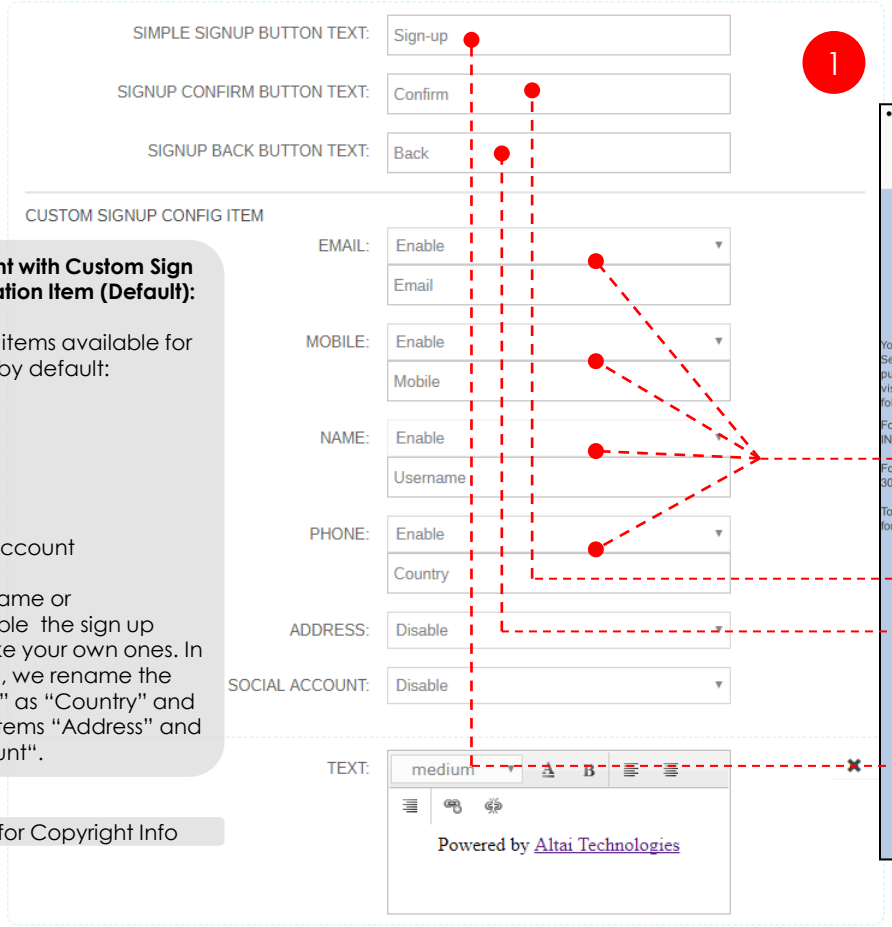
Login Element with Custom Sign Up Configuration Item (Default):

There are six items available for user sign up by default:

(1) Email
(2) Mobile
(3) Name
(4) Phone
(5) Address
(6) Social Account

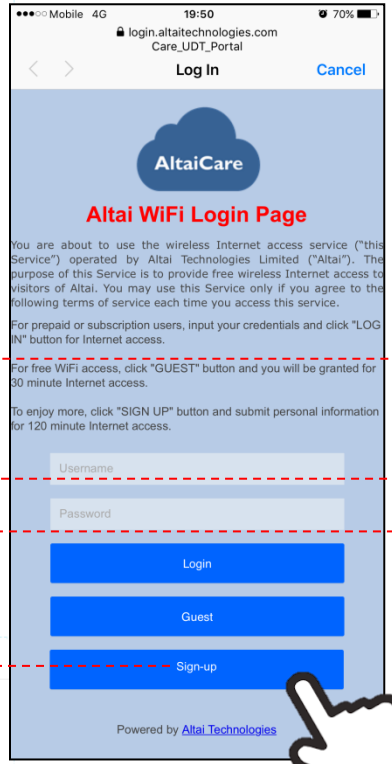
You can rename or enable/disable the sign up items to make your own ones. In this example, we rename the item "Phone" as "Country" and disable the items "Address" and Social Account".

Text Element for Copyright Info



1

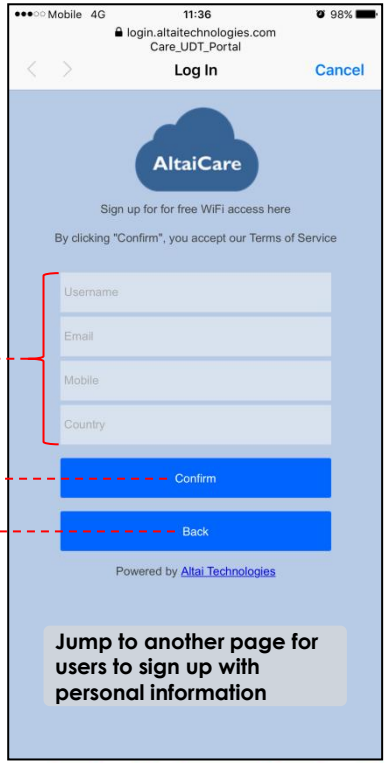
Sign In/Guest Login Page



Click "Sign Up" button

2

Sign Up Page

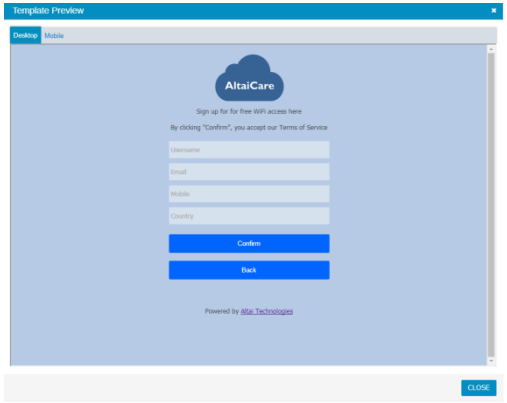


Jump to another page for users to sign up with personal information

Step 6b: User Defined Template Portal Setup – Template Preview (Desktop)

Note: Remember to click SAVE button at the page bottom to make all changes take effect before checking on the preview.

Sign In/Guest Login Page

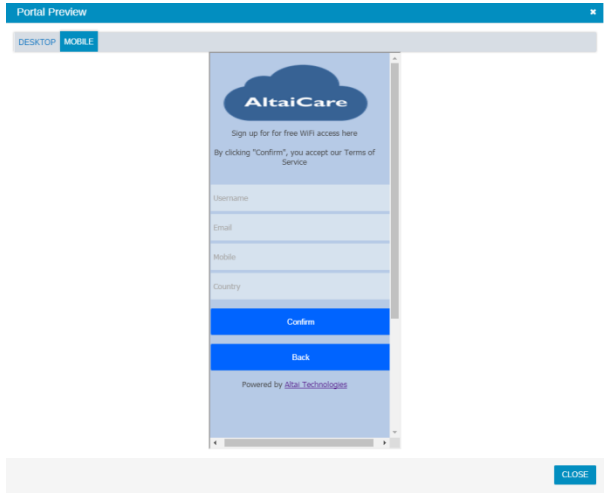


Sign Up Page

Step 6b: User Defined Template Portal Setup – Template Preview (Mobile)

Note: Remember to click SAVE button at the page bottom to make all changes take effect before checking on the preview.

Sign In/Guest Login Page

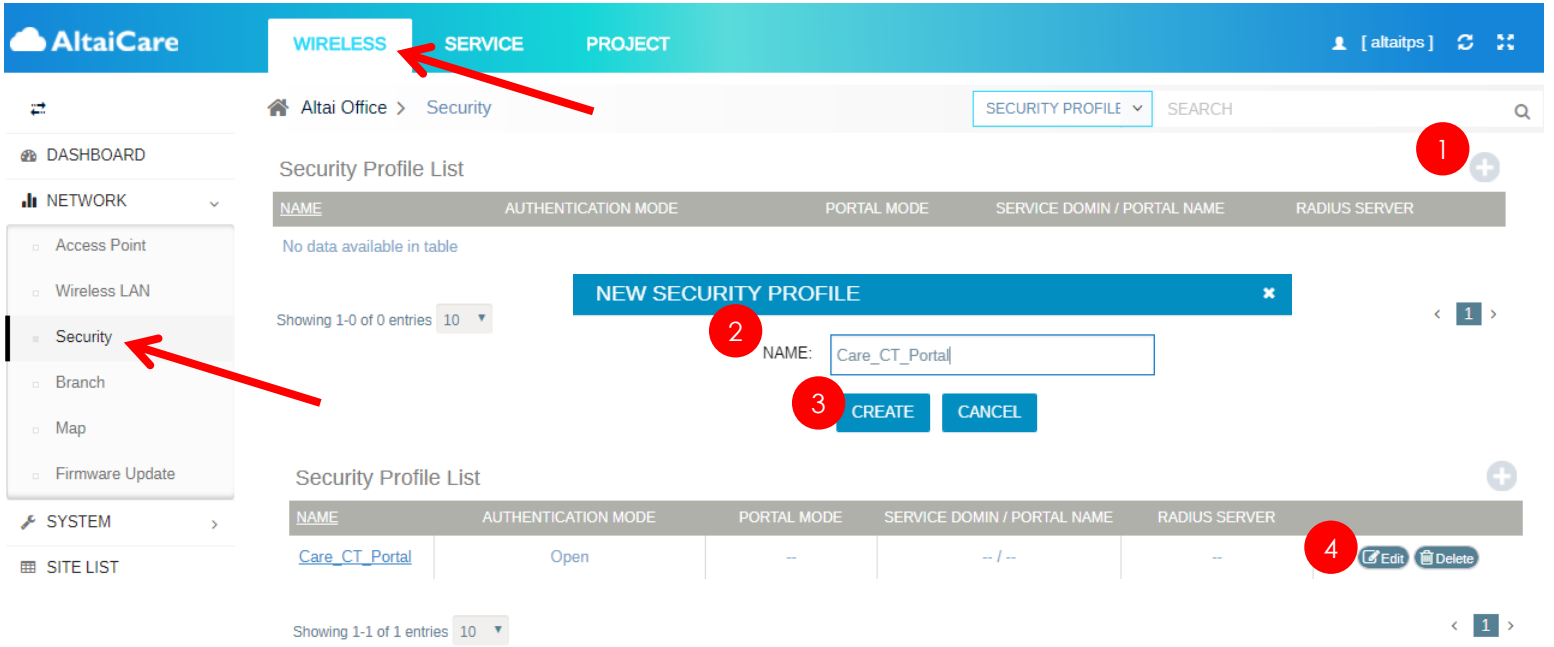


Sign Up Page

ALTAI Super WiFi

Step 7a: Create Portal Security Profile

Step 7a: Create Portal Security Profile

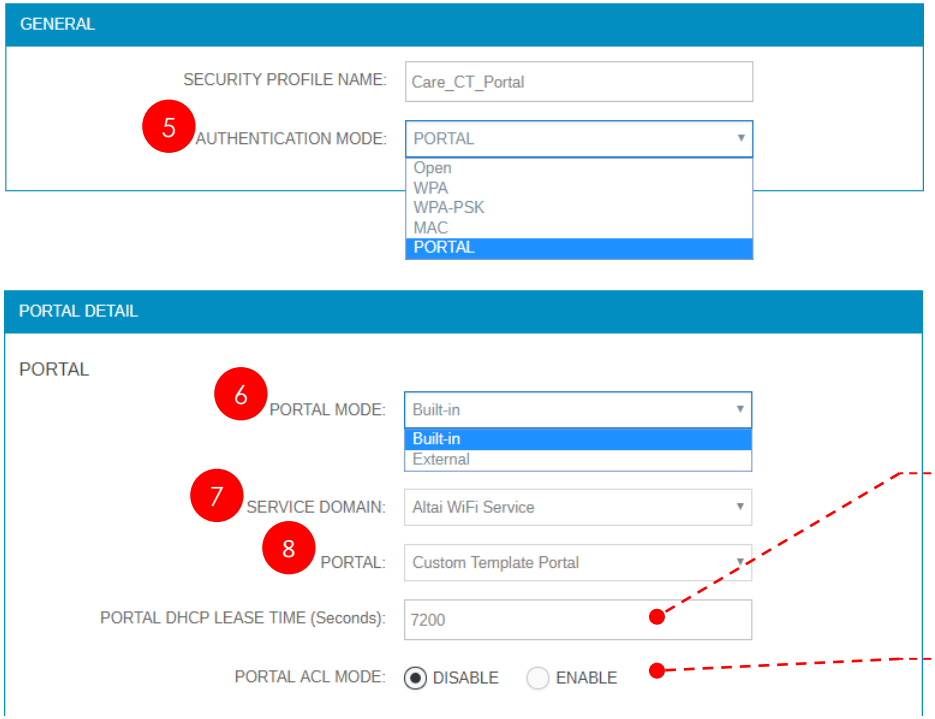


Procedures:

1. Click ⊕ to create a new Security Profile.
2. Give a name for the profile. In our example, we create two profiles called "Care_CT_Portal" and "Care_UDT_Portal" to which we will apply the custom template and user defined template that we prepared in Step 6a and Step 6b correspondingly.
3. Click CREATE to confirm it.
4. A new entry is then created for each profile in the list. Click Edit to further configure it.

ALTAI Super WiFi

Step 7a: Create Portal Security Profile – Portal Setting



Procedures:

5. Select "Portal" as Authentication Mode.
6. Select "Built-in" as Portal Mode.
7. Choose one of the Service Domains where your portal is created. The Service Domains listed here depend on the "Applicable Sites" setting (Step 2 Item #3) of the Service Domains. In our example, we set up the Service Domain called "Altai WiFi Service" and we have a custom template/user defined template portal built in there.
8. Select the portal that you created in the selected Service Domain. In our example, it is Custom Template Portal/User Defined Template Portal.

Optional Items:

Portal DHCP Lease Time: IP lease time to the portal clients by AP. By default, it is set to be 7200 seconds. Once expired, the clients will then renew the IP with the AP.

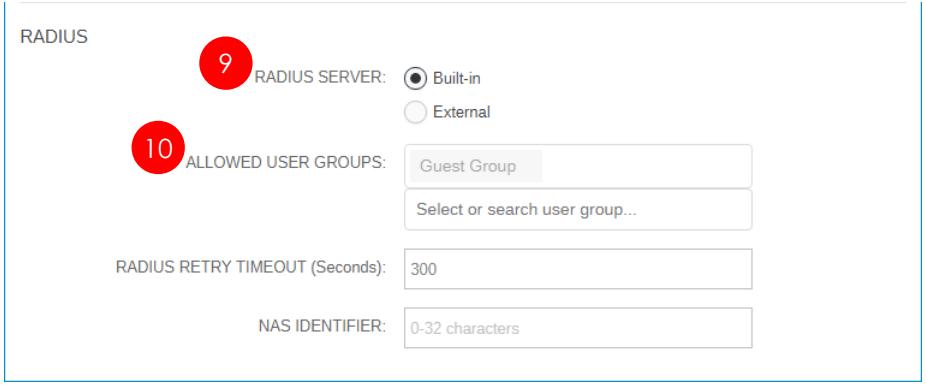
Portal ACL Mode: A Black/White List (or called Walled Garden) designed to control the information and Web sites the user is able to access before and after passing through portal login. Whitelist is the websites to be allowed for portal user access before authentication while blacklist is those to be blocked from access no matter whether it's before or after successful authentication.

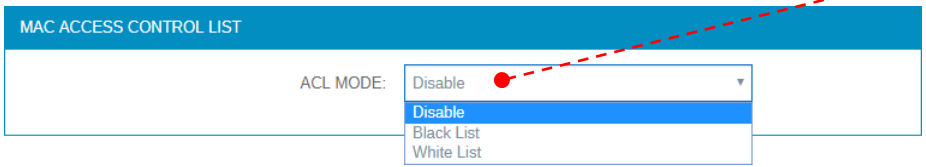
This is generally used with the hyperlink on the login page. When users click on it, they will be redirected to the desired URL which is allowed (whitelisted) in this ACL file without going through the portal authentication.

See here for more details of operation.

ALTAI Super WiFi

Step 7a: Create Portal Security Profile – RADIUS Setting





Procedures:

9. Select "Built-in" for RADIUS Server.
10. Choose the User Group(s) to be allowed for user authentication and accounting via the **Username/Password type** of portal login. As to guest login/sign up/social account of portal logins, the corresponding user groups were earlier assigned in Step 6 and therefore preselected as the Allowed User Group and become greyed-out item. In our example, we select "PP User Group" to be allowed for Username/Password login via User Defined Template Portal.

Note: Remember to click SAVE button at the page bottom to make all changes take effect.

Optional Items:

MAC Access Control List: It is different from the Portal ACL List. Here, you can upload a list of client MAC addresses (in .txt file) to allow or deny wireless connection of the client to the SSID (which uses this security profile to implement the ACL security measures).

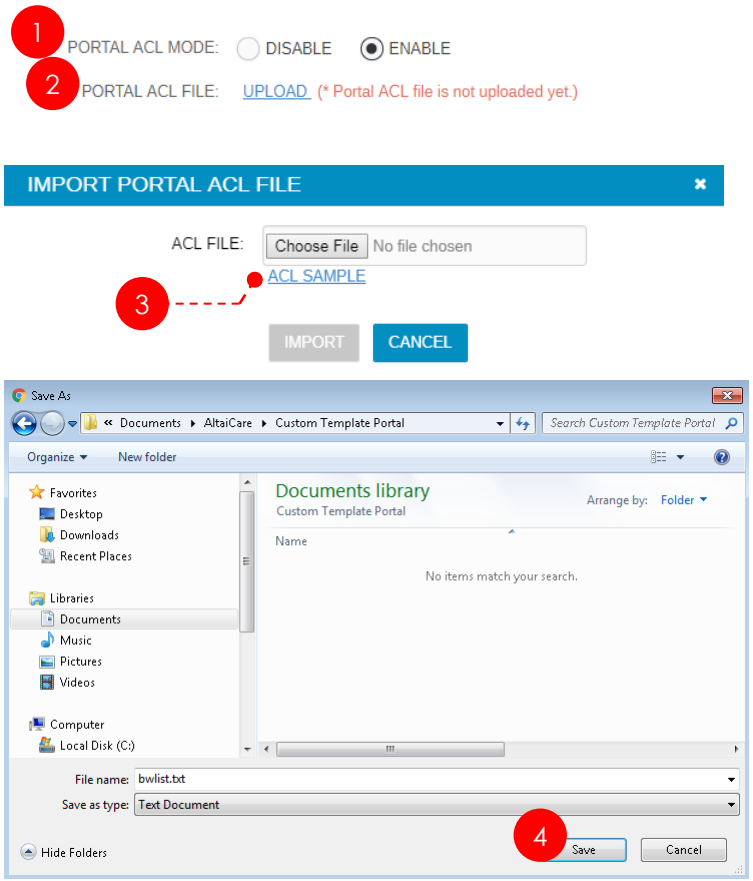
White List is to allow the wireless clients which are specified on the list to connect to the SSID. In other words, for those who are not on the list, they will be denied access.

Black List is a list of wireless clients to be denied access to the SSID. In other words, for those who are not on the list, they can get access to it.

For details of operation, refer to Advanced Configuration Section.

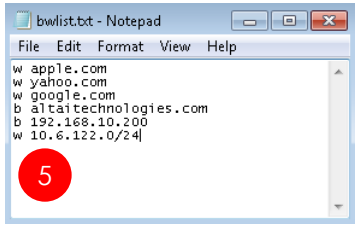
ALTAI Super WiFi

Step 7a: Create Portal Security Profile – Portal ACL Configuration



Procedures:

1. Enable Portal ACL Mode.
2. Click "Upload" of the Portal ACL File and the "Import Portal ACL File" pops up
3. Click "ACL Sample".
4. A window pops up. Select the destination path for file download and then click "Save" button.
5. Open the bwlist.txt file and follow the format below to create your own list.



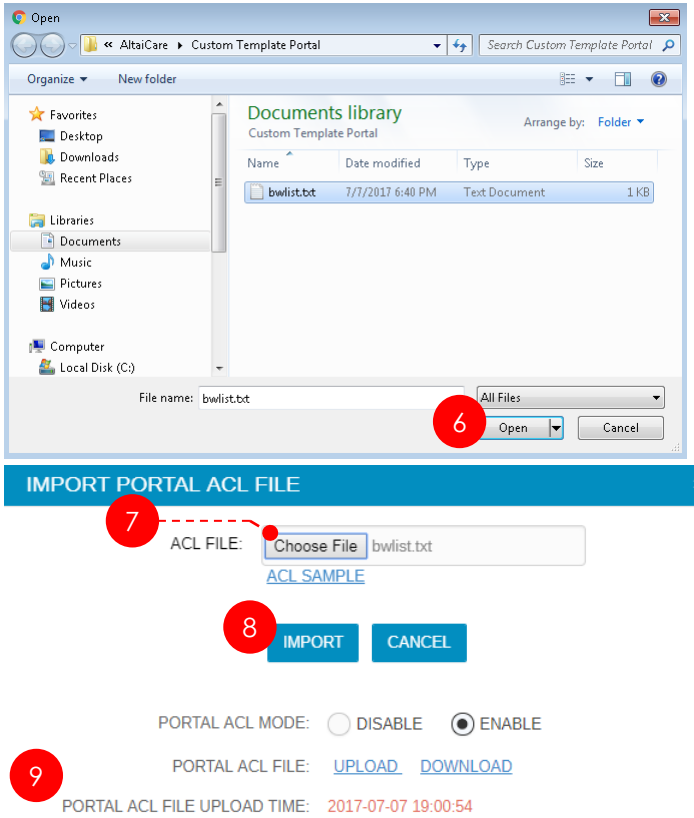
Note: "w" denotes whitelisted website while "b" denotes blacklisted website

Note: The list can consist of domain, single IP or even IP subnet

Note: If we whitelist the domain "apple.com", CNA of IOS devices may regard the open network is Internet accessible and will not pop up a window for user login. Users may manually open a browser and trigger the portal page by entering non-https website in the address bar.

ALTAI Super WiFi

Step 7a: Create Portal Security Profile – Portal ACL Configuration (Cont.)



Procedures:

6. Go back to the "Import Portal ACL File" window and click "Choose File" button to upload the ACL file.
7. A window pops up. Select the modified bwlist.txt file and click "Open" button
8. Click IMPORT button.
9. File uploaded and confirmed with the upload time.

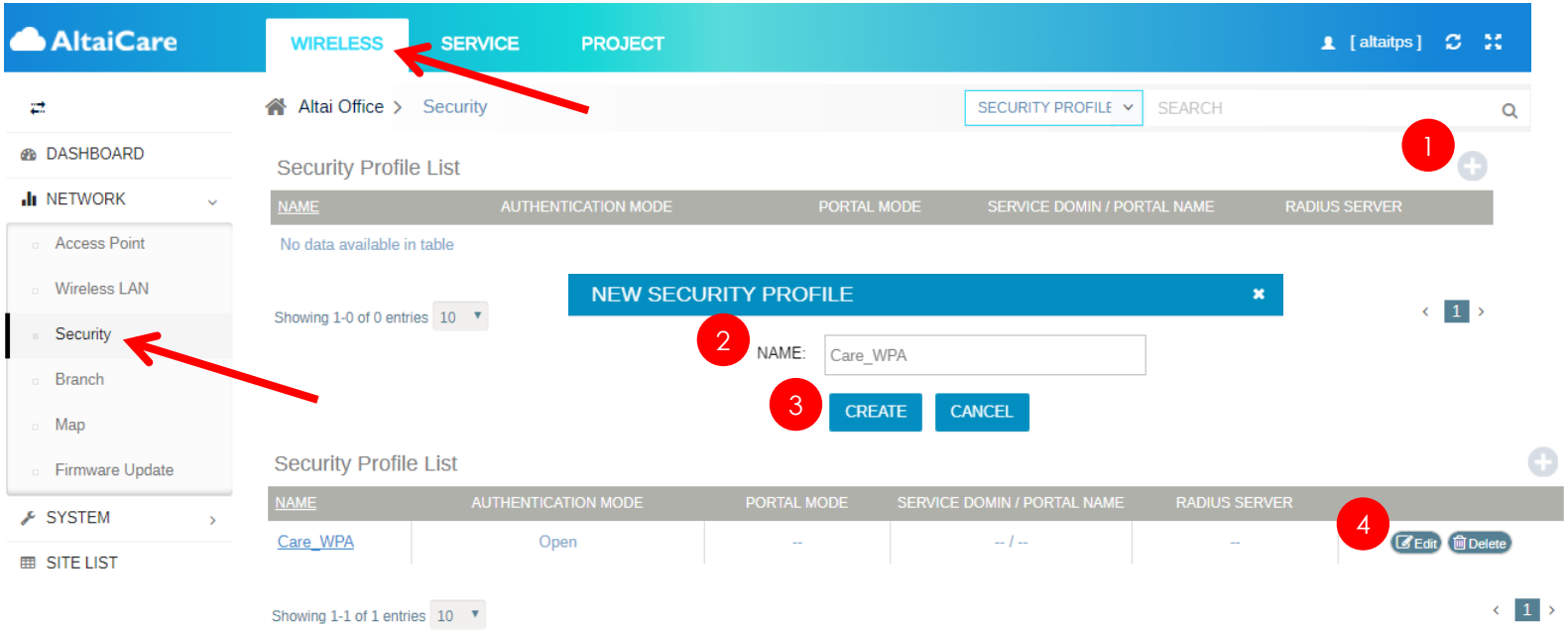
Note: Remember to click SAVE button at the page bottom to make all changes take effect.

ALTAI Super WiFi

Step 7b: Create WPA Security Profile

ALTAI Super WiFi

Step 7b: Create WPA Security Profile

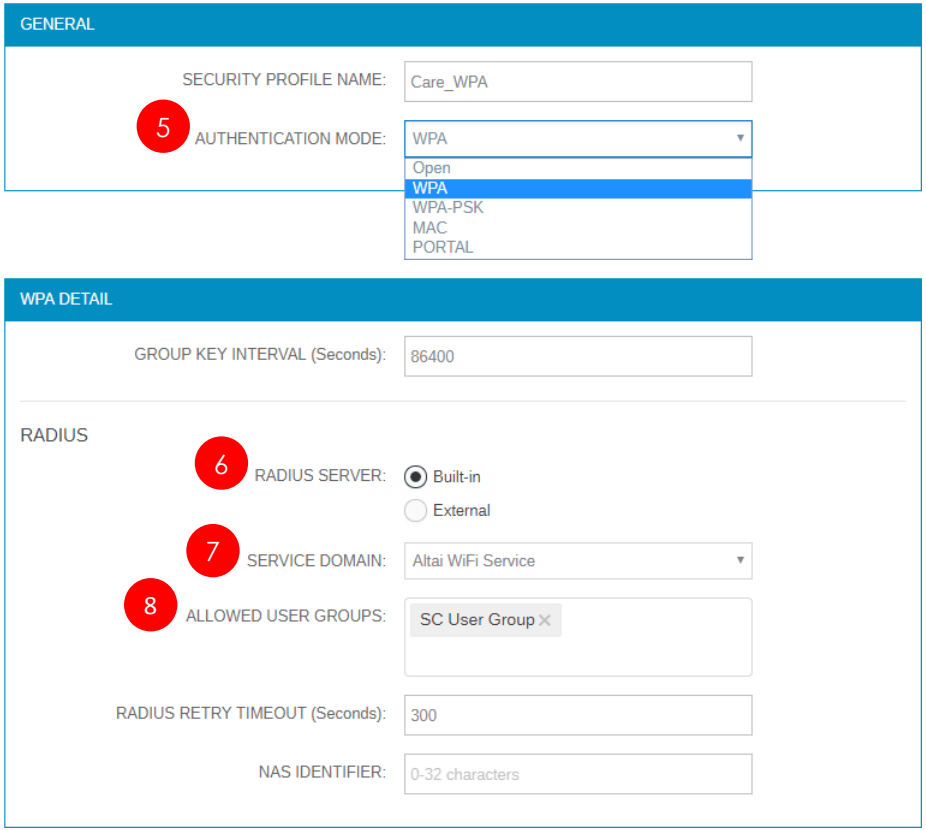


Procedures:

1. Click ⊕ to create a new Security Profile.
2. Give a name for the profile. In our example, we create a profile called "Care_WPA" to which we will apply our previously prepared user group in Step 4 for user authentication via PEAP.
3. Click CREATE to confirm it.
4. A new profile entry is then created in the list. Click Edit to further configure it.

ALTAI Super WiFi

Step 7b: Create WPA Security Profile – RADIUS Setting



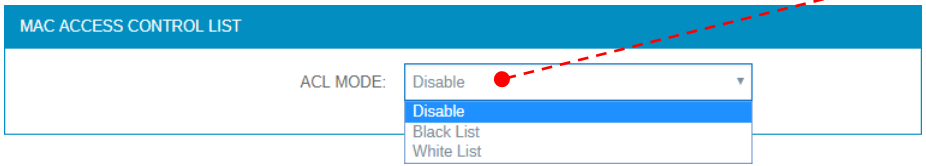
Procedures:

5. Select "WPA" as Authentication Mode.
6. Select "Built-in" for RADIUS Server.
7. Choose one of the Service Domains where your user groups and accounts are created. The Service Domains listed here depend on the "Applicable Sites" setting (Step 2 Item #3) of the Service Domains. In our example, we set up the Service Domain called "Altai WiFi Service" and we have a user group with accounts built in there specifically for WPA authentication.
8. Choose the User Group(s) to be allowed for user authentication and accounting via WPA authentication. In our example, we select "SC User Group" to be allowed for Username/Password login via WPA authentication (PEAP).

Note: Remember to click SAVE button at the page bottom to make all changes take effect.

ALTAI Super WiFi

Step 7b: Create WPA Security Profile – MAC Access Control Setting



Optional Items:

MAC Access Control List: It is where you can upload a list of client MAC addresses (in .txt file) to allow or deny wireless connection of the client to the SSID (which uses this security profile to implement the ACL security measures).

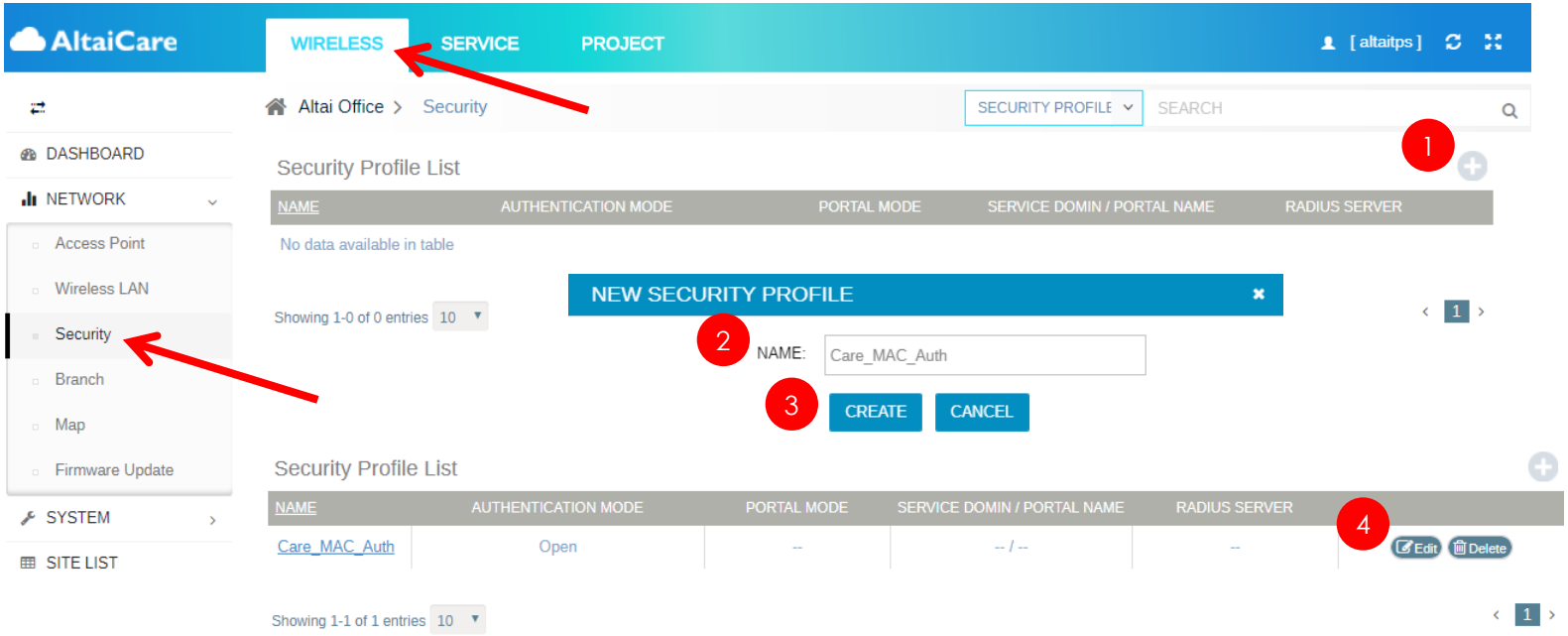
White List is to allow the wireless clients which are specified on the list to connect to the SSID. In other words, for those who are not on the list, they will be denied access.

Black List is a list of wireless clients to be denied access to the SSID. In other words, for those who are not on the list, they can get access to it.

For details of operation, refer to Advanced Configuration Section.

Step 7c: Create MAC Auth Security Profile

Step 7c: Create MAC Auth Security Profile

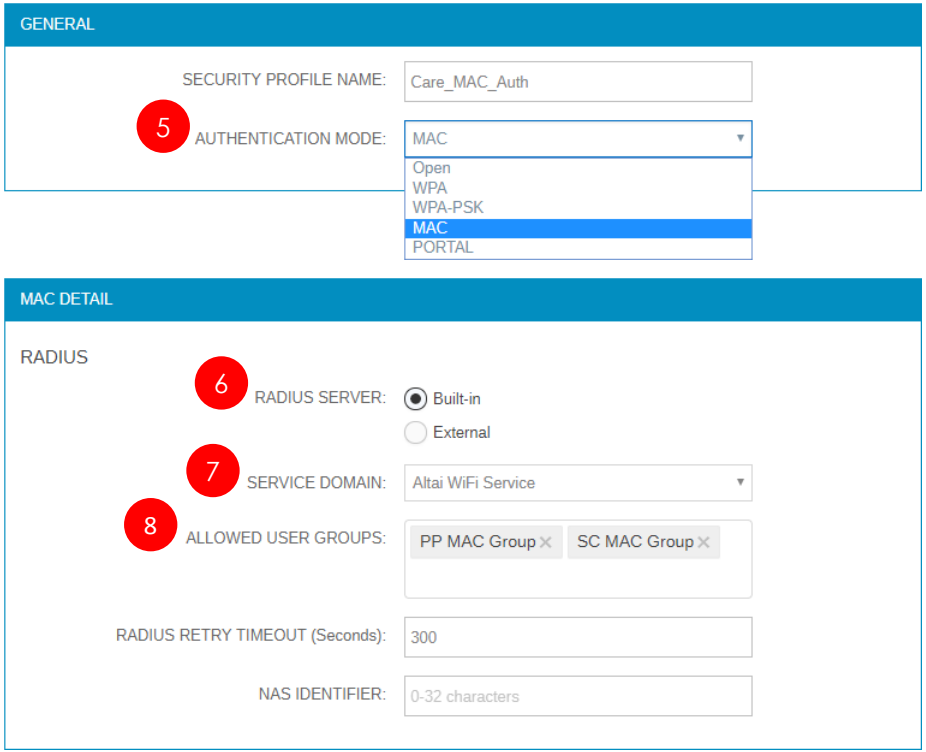


Procedures:

1. Click ⊕ to create a new Security Profile.
2. Give a name for the profile. In our example, we create a profile called "Care_MAC_Auth" to which we will apply our previously prepared user group in Step 4 for mac authentication.
3. Click CREATE to confirm it.
4. A new profile entry is then created in the list. Click Edit to further configure it.

ALTAI Super WiFi

Step 7c: Create MAC Auth Security Profile – RADIUS Setting

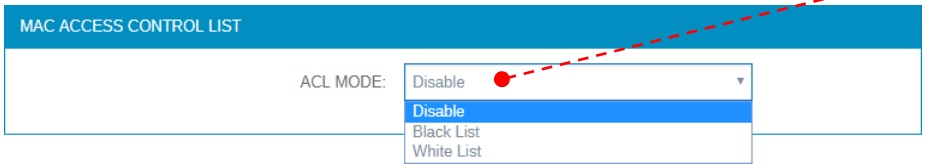


Procedures:

5. Select "MAC" as Authentication Mode.
6. Select "Built-in" for RADIUS Server.
7. Choose one of the Service Domains where your user groups and MAC entries are created. The Service Domains listed here depend on the "Applicable Sites" setting (Step 2 Item #3) of the Service Domains. In our example, we set up the Service Domain called "Altai WiFi Service" and we have two user groups with MAC entries built in there specifically for MAC authentication.
8. Choose the User Group(s) to be allowed for MAC authentication. In our example, we select "PP MAC Group" and "SC MAC Group" to be allowed for authentication with device MAC.

Note: Remember to click SAVE button at the page bottom to make all changes take effect.

Step 7c: Create WPA Security Profile – MAC Access Control Setting



Optional Items:

MAC Access Control List: It is where you can upload a list of client MAC addresses (in .txt file) to allow or deny wireless connection of the client to the SSID (which uses this security profile to implement the ACL security measures).

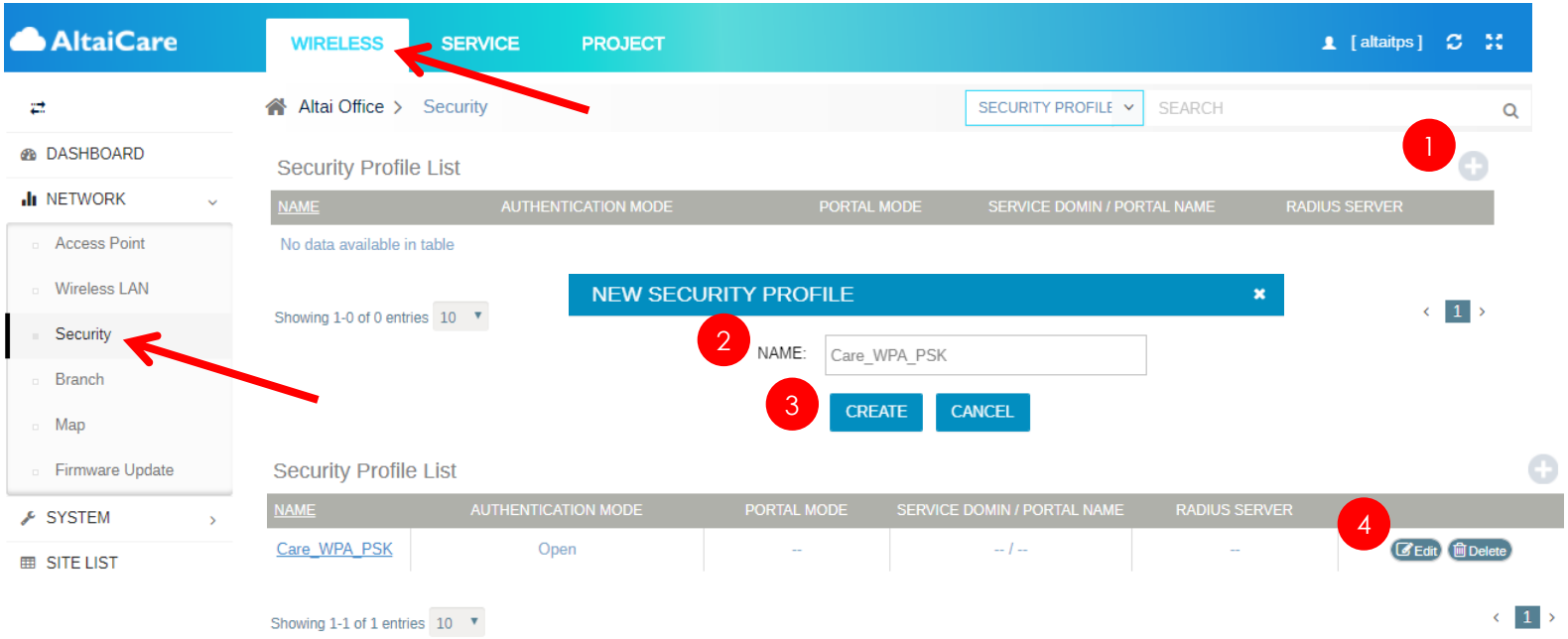
White List is to allow the wireless clients which are specified on the list to connect to the SSID. In other words, for those who are not on the list, they will be denied access.

Black List is a list of wireless clients to be denied access to the SSID. In other words, for those who are not on the list, they can get access to it.

For details of operation, refer to Advanced Configuration Section.

Step 7d: Create WPA-PSK Security Profile

Step 7d: Create WPA-PSK Security Profile

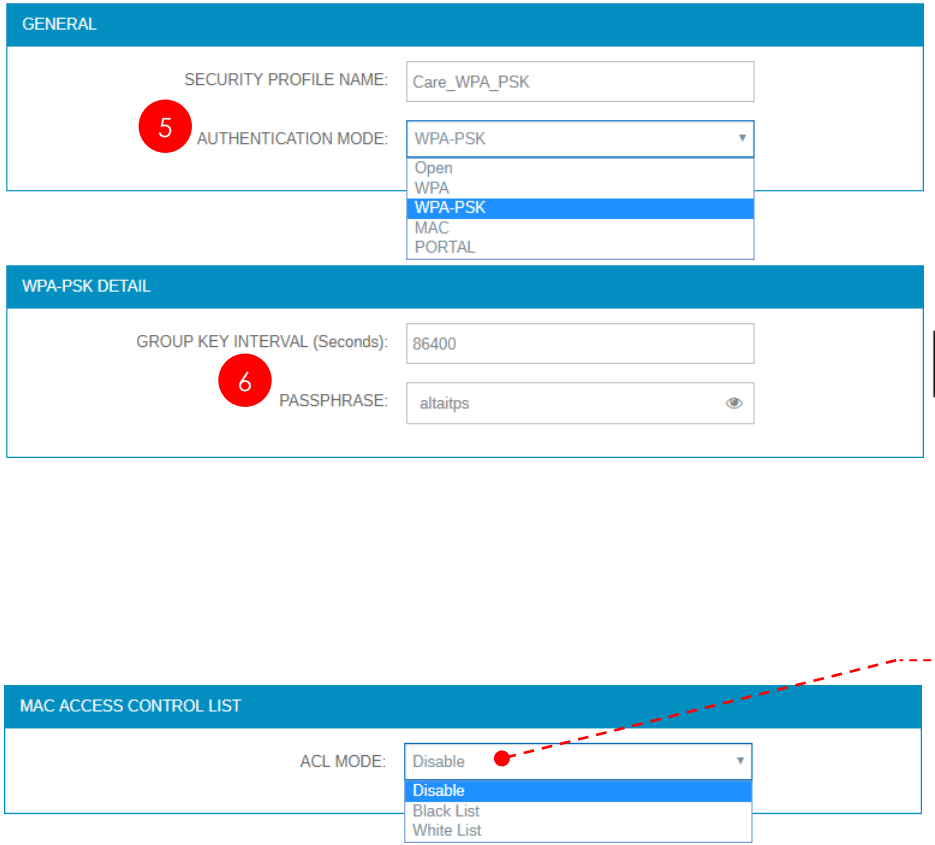


Procedures:

1. Click ⊕ to create a new Security Profile.
2. Give a name for the profile. In our example, we create a profile called "Care_WPA_PSK" for WPA-PSK authentication.
3. Click CREATE to confirm it.
4. A new profile entry is then created in the list. Click Edit to further configure it.

ALTAI Super WiFi

Step 7d: Create WPA-PSK Security Profile



Procedures:

5. Select "WPA-PSK" as Authentication Mode.
6. Input a string not less than 8 characters for the Passphrase which the WiFi users will have to use this credential for network access.

Note: Remember to click SAVE button at the page bottom to make all changes take effect.

Optional Items:

MAC Access Control List: It is where you can upload a list of client MAC addresses (in .txt file) to allow or deny wireless connection of the client to the SSID (which uses this security profile to implement the ACL security measures).

White List is to allow the wireless clients which are specified on the list to connect to the SSID. In other words, for those who are not on the list, they will be denied access.

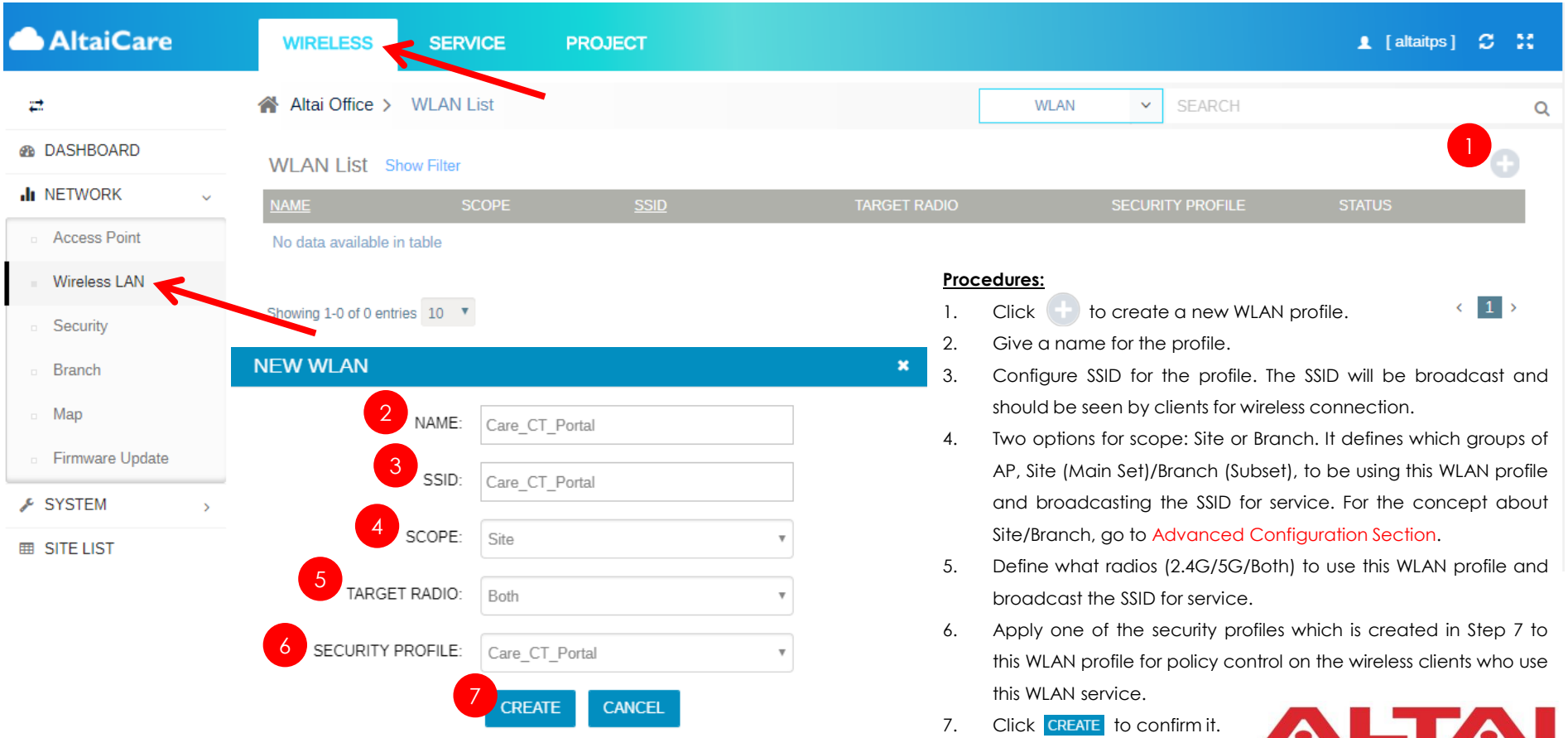
Black List is a list of wireless clients to be denied access to the SSID. In other words, for those who are not on the list, they can get access to it.

For details of operation, refer to Advanced Configuration Section.

ALTAI Super WiFi

Step 8: Create SSID (WLAN)

Step 8: Create New WLAN – Basic Setting

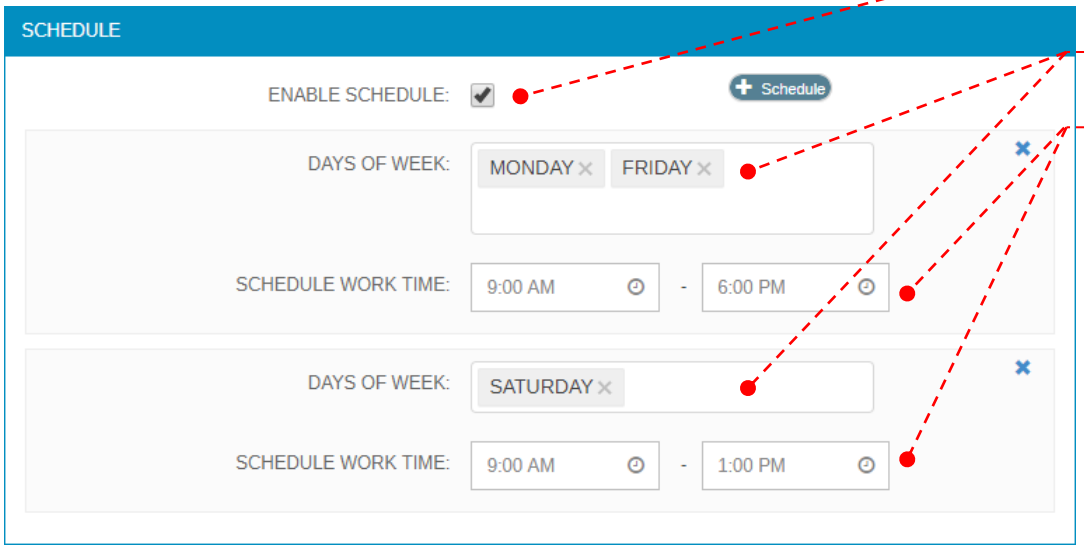


Procedures:

1. Click ⊕ to create a new WLAN profile.
2. Give a name for the profile.
3. Configure SSID for the profile. The SSID will be broadcast and should be seen by clients for wireless connection.
4. Two options for scope: Site or Branch. It defines which groups of AP, Site (Main Set)/Branch (Subset), to be using this WLAN profile and broadcasting the SSID for service. For the concept about Site/Branch, go to Advanced Configuration Section.
5. Define what radios (2.4G/5G/Both) to use this WLAN profile and broadcast the SSID for service.
6. Apply one of the security profiles which is created in Step 7 to this WLAN profile for policy control on the wireless clients who use this WLAN service.
7. Click CREATE to confirm it.

ALTAI Super WiFi

Step 8: Create New WLAN – WLAN Scheduler



Optional Items:

Enable Schedule: Check the box to enable the scheduler. It controls the periods for the WLAN service by enabling/disenabling the WLAN according to the periods defined in the following items. You can add multiple periods by clicking + Schedule button

Days of Week: To set which week days (From Sunday to Saturday) to enable the WLAN service.

Schedule Work Time: To set the time to start and stop the WLAN service on the week days defined above.

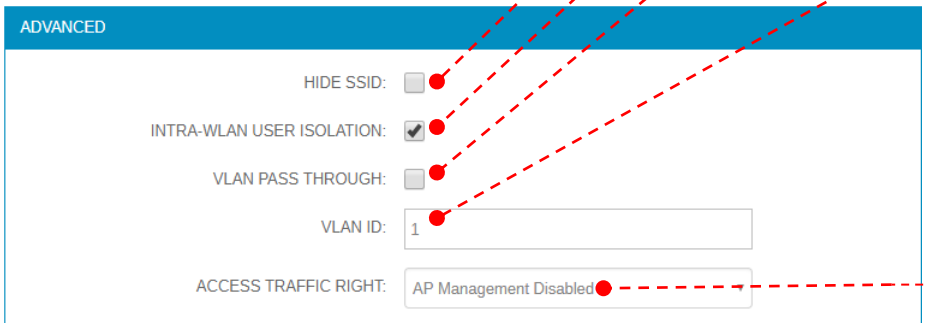
In this example, we turn on our guest SSID "Care_CT_Portal" in the following periods ONLY:

- From Mon to Fri, 9:00 – 18:00
- Sat 9:00 – 13:00

Note: Make sure a correct local Time Zone setting for the site so that the scheduler can run its scheduler accurately.

ALTAI Super WiFi

Step 8: Create New WLAN – Advanced Setting



Hide SSID: To hide/unhide SSID name for broadcast

Intra-WLAN User Isolation: To block Layer 2 communication among the 2.4G and 5G clients within the same WLAN under the same AP.

VLAN Pass Through: Applicable for VLAN environment only. It is usually used for WDS bridging. With the box checked, the WLAN will carry all VLAN traffic and therefore establish a trunk link over the WDS bridge to the remote Station.

VLAN ID: Applicable for VLAN environment only. It adds/removes the VLAN tag with ID specified here to the client traffic from/to the WiFi interface to/from the Ethernet interface. In other words, the WLAN will be as a VLAN access interface for the wireless clients.

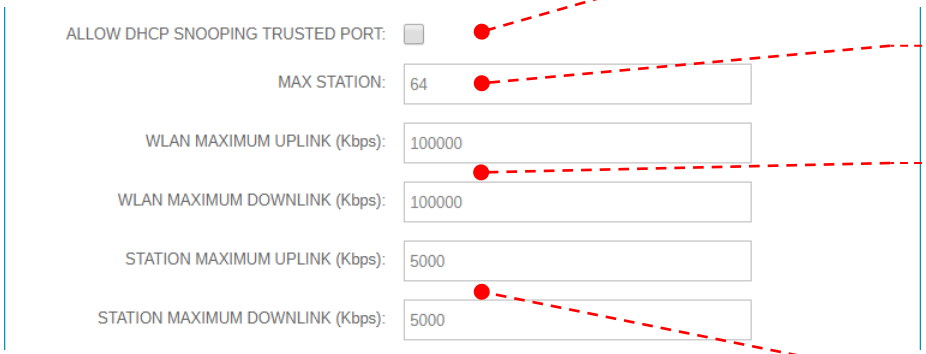
This VLAN ID option is not applicable for portal authentication because AP will be as a gateway for the portal users. Their traffic will be "NATed" by AP's IP and routed to the local gateway and then to Internet through management VLAN.

Access Traffic Right: To impose access right control on the client traffic under this WLAN. Three available options:

- **Full Access**: Client associating to this WLAN can manage AP through wireless interface and gain access to the local network or Internet via Ethernet interface.
- **AP Management Only**: Client associating to this WLAN can manage AP through wireless interface but not able to access to the local network or Internet via Ethernet interface.
  In VLAN environment, make sure the VLAN ID assigned to the WLAN the same as AP Management VLAN; otherwise, clients cannot access to AP even if either of the above two options (Full Access or AP Management Only) is selected.
- **AP Management Disabled:** Client associating to this WLAN can gain access to the local network or Internet via Ethernet interface but not able to manage AP through wireless interface.

ALTAI Super WiFi

Step 8: Create New WLAN – Advanced Setting (Cont.)



Allow DHCP Snooping Trusted Port: With the box checked, it allows DHCP servers in the WLAN to offer IP address to clients via wireless interface.

As usual, the box is unchecked to prevent illegal DHCP servers offering IP address from the untrusted wireless network.

Max Station: Set maximum associated clients to the WLAN interface for maintaining good WiFi service to the clients. The supported maximum client number depends on the AP models. By default, it is set to be 64.

WLAN Maximum Uplink/Downlink (Kbps): Set upper limit to the total uplink/downlink throughput for the whole group of associated clients under the same WLAN. The unit is in kbps. In other words, setting of 100000 means 100Mbps of throughput limit for the whole WLAN group traffic.

Station Maximum Uplink/Downlink (Kbps): Set upper limit to the total uplink/downlink throughput for individual associated clients under the same WLAN. The unit is in kbps. In other words, setting of 10000 means each of the individual clients can enjoy 10Mbps of throughput limit.

This setting is not applicable for those users who are authenticated through AltaiCare Service Domain with their own bandwidth control setting configured in the user account. For example, for a user account which is configured with bandwidth control of 10Mbps, you will still get 10Mbps of data speed even though the SSID you are connecting with is configured with 5Mbps of per-user bandwidth control.

Step 8: Create New WLAN – Advanced Setting (Cont.)

Reject Station if SNR less than (dB): Set the minimum required uplink SNR when clients make association requests to this WLAN. In case of lower uplink SNR than the threshold value defined here, AP will reject its association request. This approach can let the clients actively search better APs in the surroundings for network access. Default value is 0 which means the feature disabled and AP will not reject any client association due to low SNR.

Disassociate Station if SNR drops more than (dB): Used with the above item. This is to set a differential (in dB) below the association requirement (the above item) for kicking the associated clients out due to low SNR. The higher the value, the more room there will be for uplink signal fluctuation due to client's movement and hence more stable WiFi connection status.

For consecutive … packets: Used with the above 2 items. This is to set how many consecutive packets with uplink SNR lower than the association requirement (the first item) by a defined amount (the second item) for kicking the associated clients out due to low SNR. The lower the value, the higher sensitivity for the AP for the kick action.

Note: Remember to click SAVE button at the page bottom to make all changes take effect.

ALTAI Super WiFi

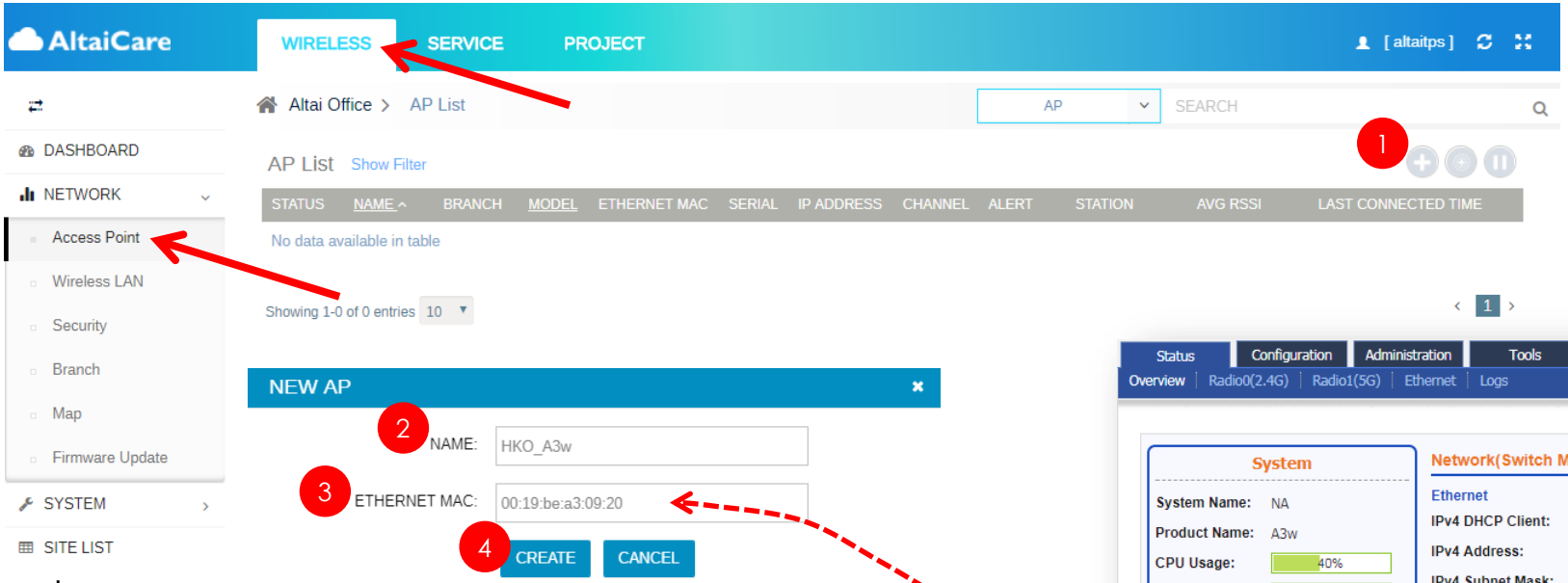
Step 8: Create New WLAN – Configuration Summary

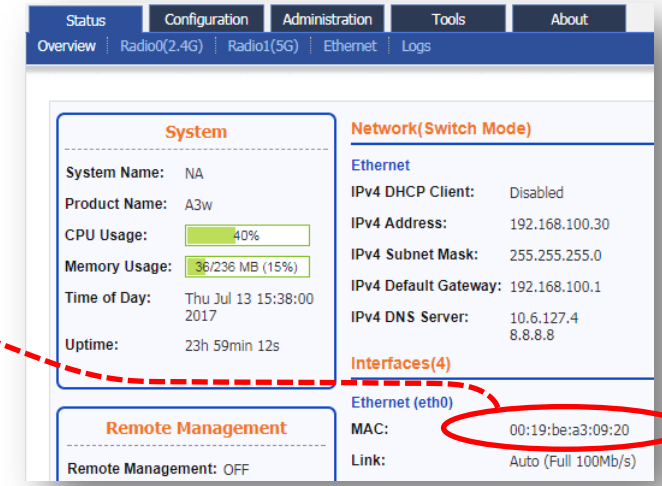
WLAN Profile	SSID to be broadcast	Security Profile to be applied	VLAN ID
Care_CT_Portal	Care_CT_Portal	Care_CT_Portal	N/A (You can enter ANY integer here, e.g. 1-4094)
Care_UDT_Portal	Care_UDT_Portal	Care_UDT_Portal	N/A (You can enter ANY integer here, e.g. 1-4094)
Care_WPA	Care_WPA	Care_WPA	150
Care_MAC_Auth	Care_MAC_Auth	Care_MAC_Auth	160
Care_WPA_PSK	Care_WPA_PSK	Care_WPA_PSK	170

Note: For simplicity, we use the same name for WLAN Profile, SSID and Security Profile in this example.

Step 9: AP Registration

Step 9a: Single AP Registration





AP WebUI

Procedures:

1. Click ⊕ to register a new AP.
2. A "New AP" window pops up. Give a name for the AP. This name setting will be provisioned to AP as "System Name" once the AP is connected with AltaiCare.
3. Enter the AP Ethernet MAC address in **colon-separated** or **hyphen-separated** format with either **uppercase** or **lowercase** alphabets, e.g. **XX:XX:XX:XX:XX:XX** or **xx-xx-xx-xx-xx-xx**. You can directly copy it from AP WebUI "Status > Overview > Interfaces > Ethernet(eth0) > MAC".
4. Click CREATE button to confirm the AP registration to the site.

ALTAI Super WiFi

Step 9a: Single AP Registration (Cont.)

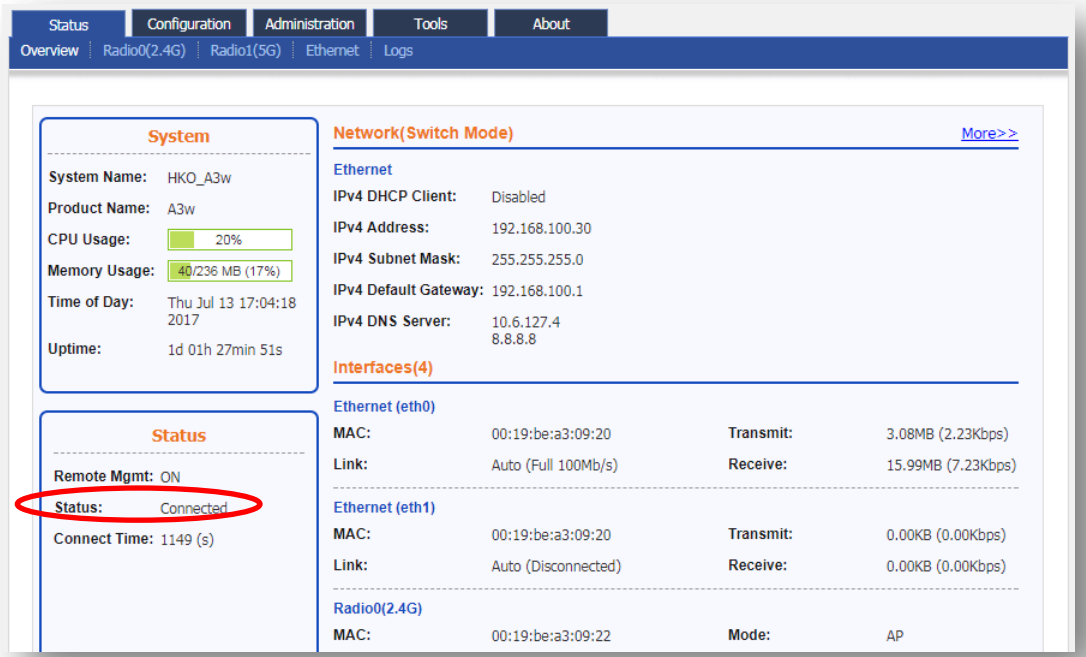
AP List Show Filter

STATUS	NAME	BRANCH	MODEL	ETHERNET MAC	SERIAL	IP ADDRESS	CHANNEL	ALERT	STATION	AVG RSSI	LAST CONNECTED TIME
	HKO_A3w	--	A3w	00:19:be:a3:09:20	A3W053300009	223.255.161.226(WAN) 192.168.100.30(LAN)	Radio1: 1 Radio2: 36	0	2.4G: 0 5G: 0	2.4G: -- 5G: --	2017-07-13 15:16:25

Showing 1-1 of 1 entries 10

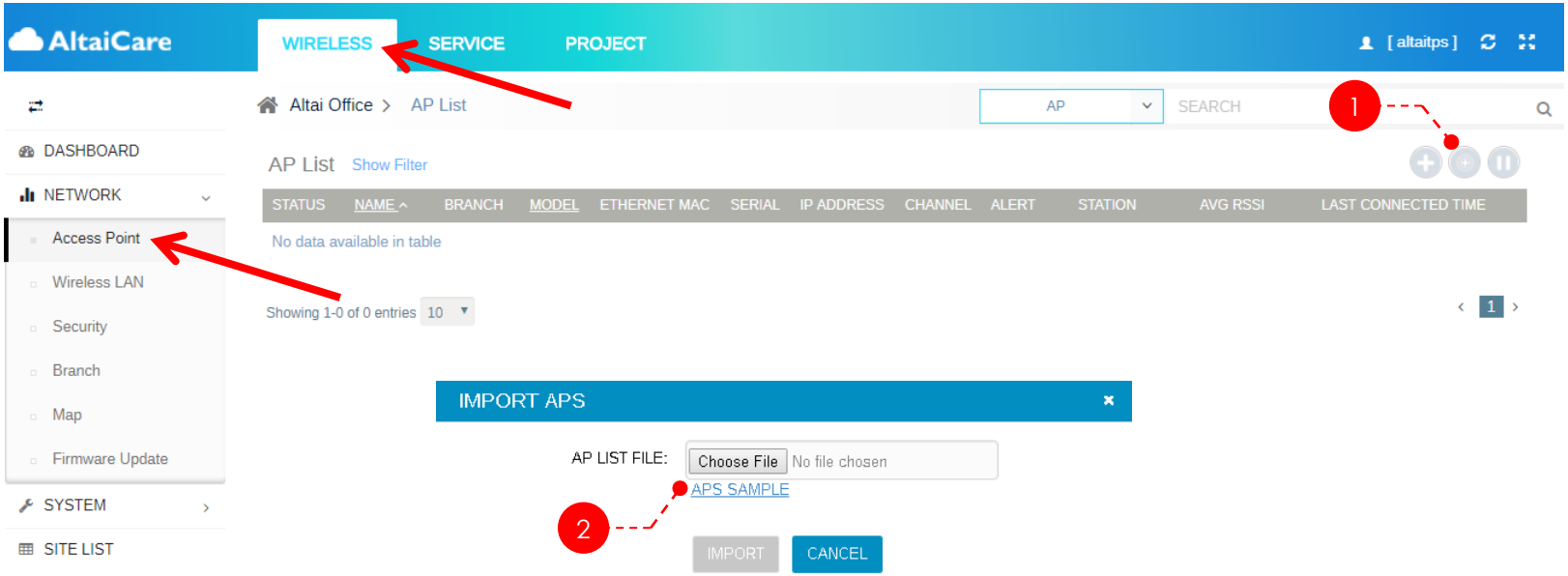
The status will turn from to for the AP entry once the AP is successfully connected with AltaiCare.

On AP WebUI, it will also show the status of Remote Mgmt as "Connected".



AP WebUI

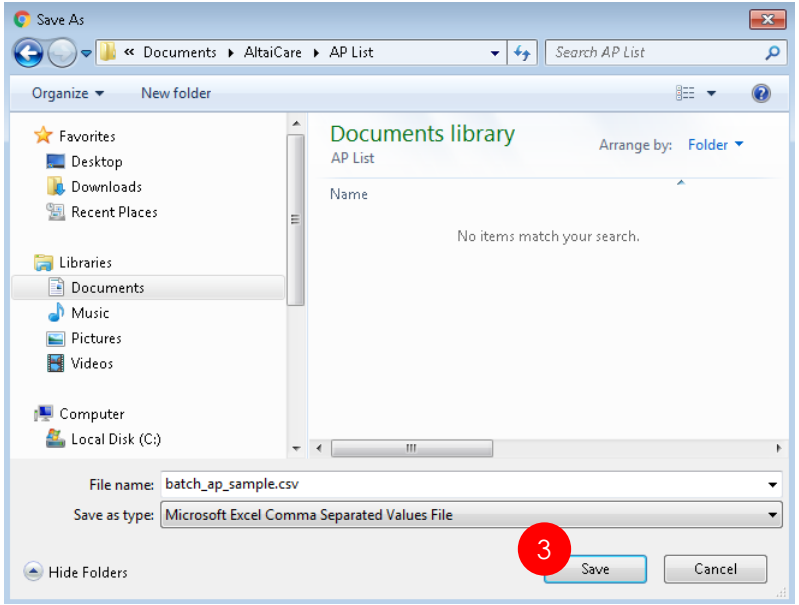
Step 9b: AP Batch Registration

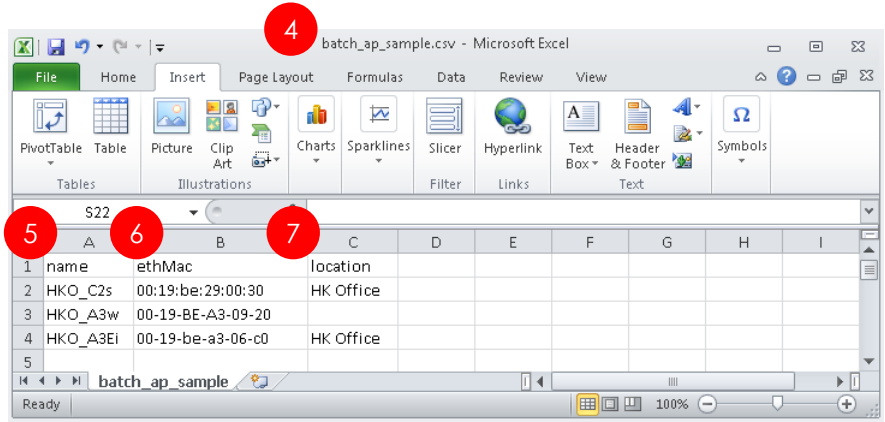


Procedures:

1. Click to pop up a window for importing AP list file.
2. Click "APs Sample" to download a AP list template.

Step 9b: AP Batch Registration (Cont.)



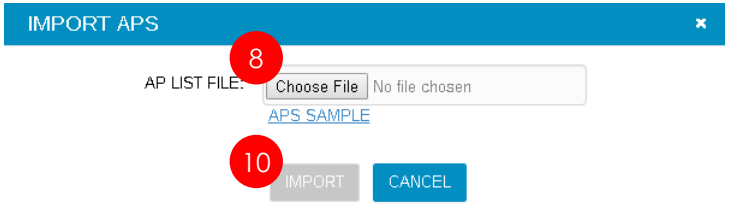


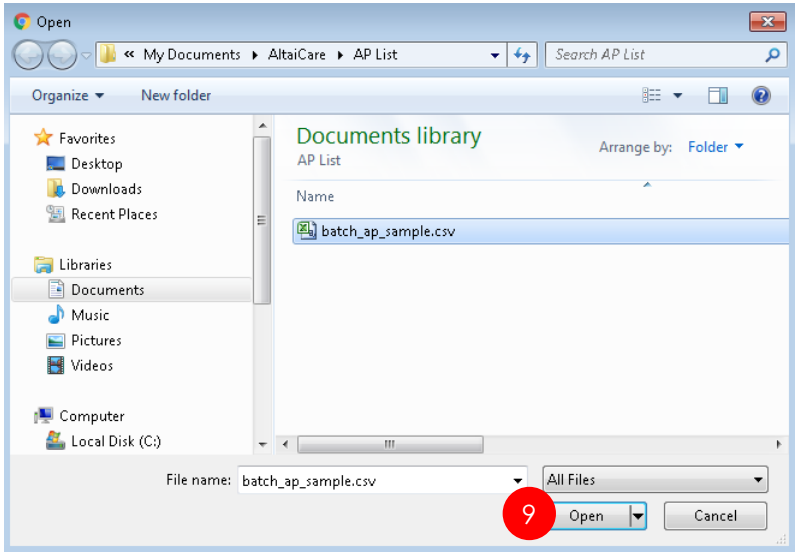
Procedures:

3. Click "Save" button.
4. Open the file "batch_ap_sample.csv".
5. Give a name for each AP.
6. Input the AP Ethernet MAC address in **colon-separated** or **hyphen-separated** format with either **uppercase** or **lowercase** alphabets,
   e.g. **XX:XX:XX:XX:XX:XX** or **xx-xx-xx-xx-xx-xx**
7. Enter AP location. It is an optional item and you can keep it blank.

ALTAI Super WiFi

Step 9b: AP Batch Registration (Cont.)





Procedures:

8. Go back to the "Import APs" window and click "Choose File" button to upload the AP batch file.
9. A window pops up. Select the modified batch_ap_sample.csv file and click "Open" button.
10. Click IMPORT button.

ALTAI Super WiFi

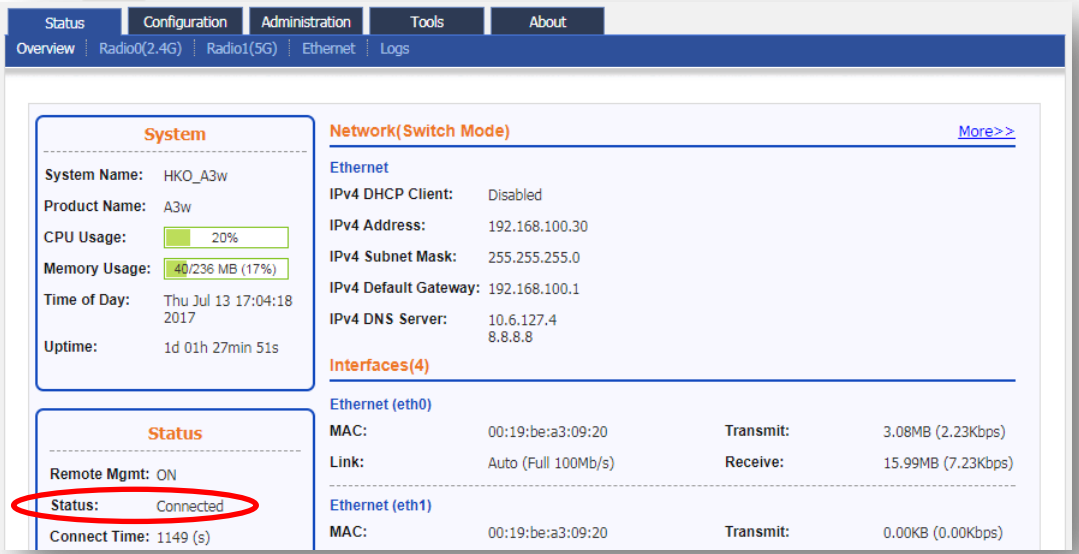
Step 9b: AP Batch Registration (Cont.)

AP List Show Filter

STATUS	NAME	BRANCH	MODEL	ETHERNET MAC	SERIAL	IP ADDRESS	CHANNEL	ALERT	STATION	AVG RSSI	LAST CONNECTED TIME
	HKO_A3Ei	--	--	00:19:be:a3:06:c0	--	--	--	0	2.4G: 0 5G: 0	2.4G: -- 5G: --	--
	HKO_A3w	--	A3w	00:19:be:a3:09:20	A3W053300009	223.255.161.226(WAN) 192.168.100.30(LAN)	Radio2: 36 Radio1: 1	0	2.4G: 0 5G: 0	2.4G: -- 5G: --	2017-07-31 14:43:50
	HKO_C2s	--	C2s	00:19:be:29:00:30	C2S161100013	223.255.161.226(WAN) 192.168.100.50(LAN)	Radio2: 52 Radio1: 6	0	2.4G: 0 5G: 0	2.4G: -- 5G: --	2017-07-31 14:43:52

Showing 1-3 of 3 entries 10

‹ 1 ›



The status will turn from to for the AP entry once the AP is successfully connected with AltaiCare.

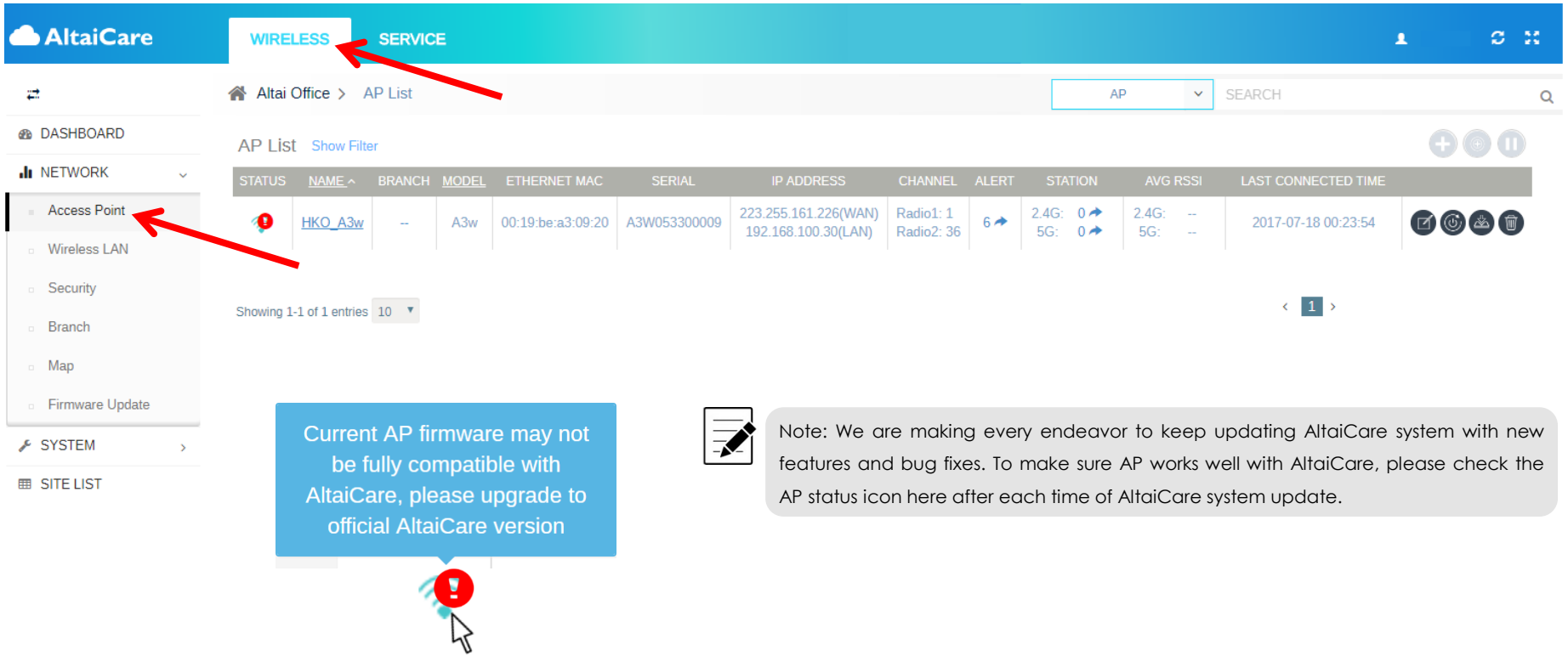
On AP WebUI, it will also show the status of Remote Mgmt as "Connected".

AP WebUI

ALTAI Super WiFi

AP Firmware Update

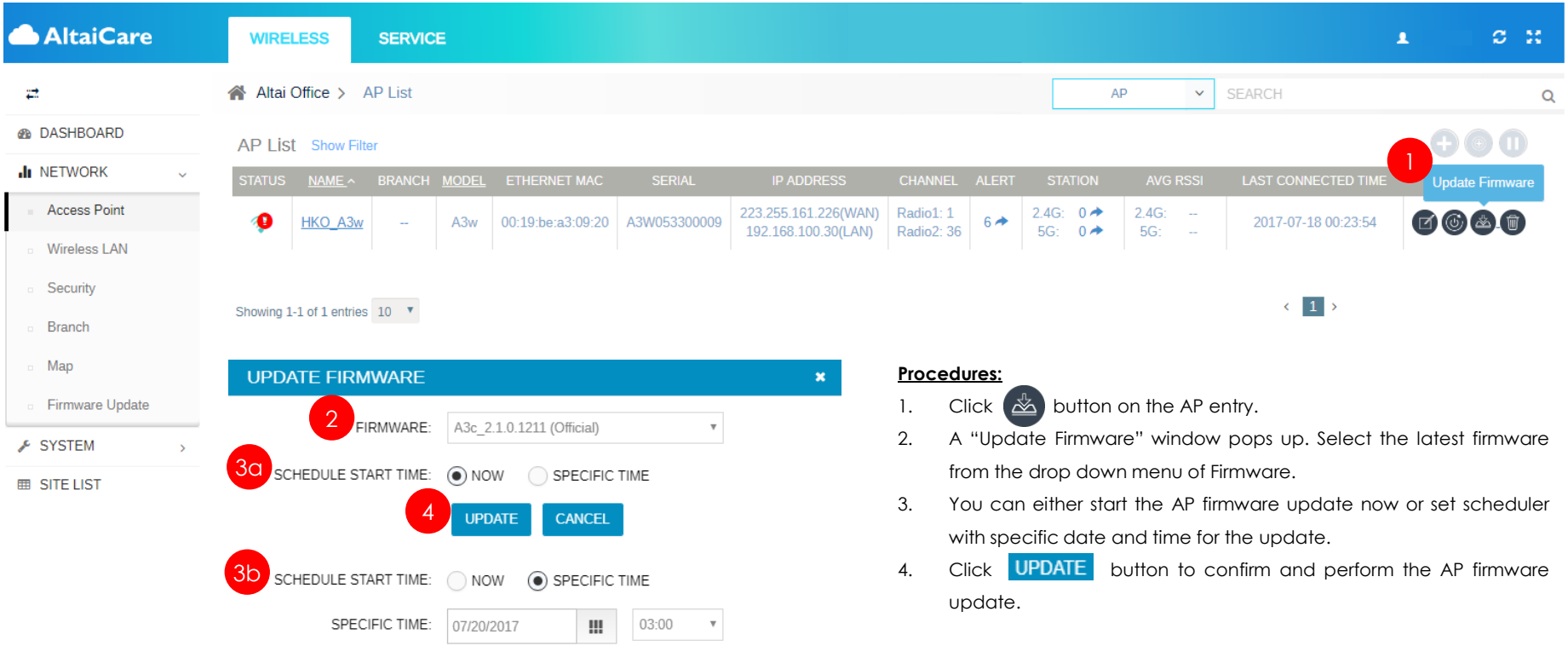
AP Firmware Compatibility Check



Note: We are making every endeavor to keep updating AltaiCare system with new features and bug fixes. To make sure AP works well with AltaiCare, please check the AP status icon here after each time of AltaiCare system update.

ALTAI Super WiFi

Single AP Firmware Update



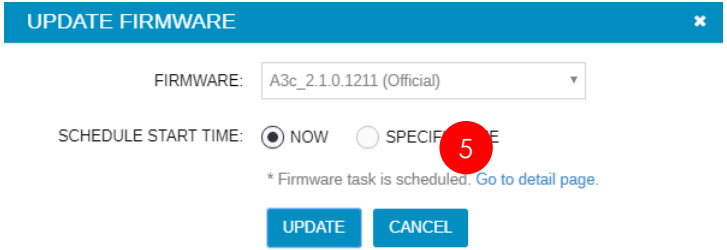
Procedures:

1. Click button on the AP entry.
2. A "Update Firmware" window pops up. Select the latest firmware from the drop down menu of Firmware.
3. You can either start the AP firmware update now or set scheduler with specific date and time for the update.
4. Click **UPDATE** button to confirm and perform the AP firmware update.

Warning: Make sure the AP unit is powered up throughout the whole firmware update process! Failure to do so might cause firmware crash.

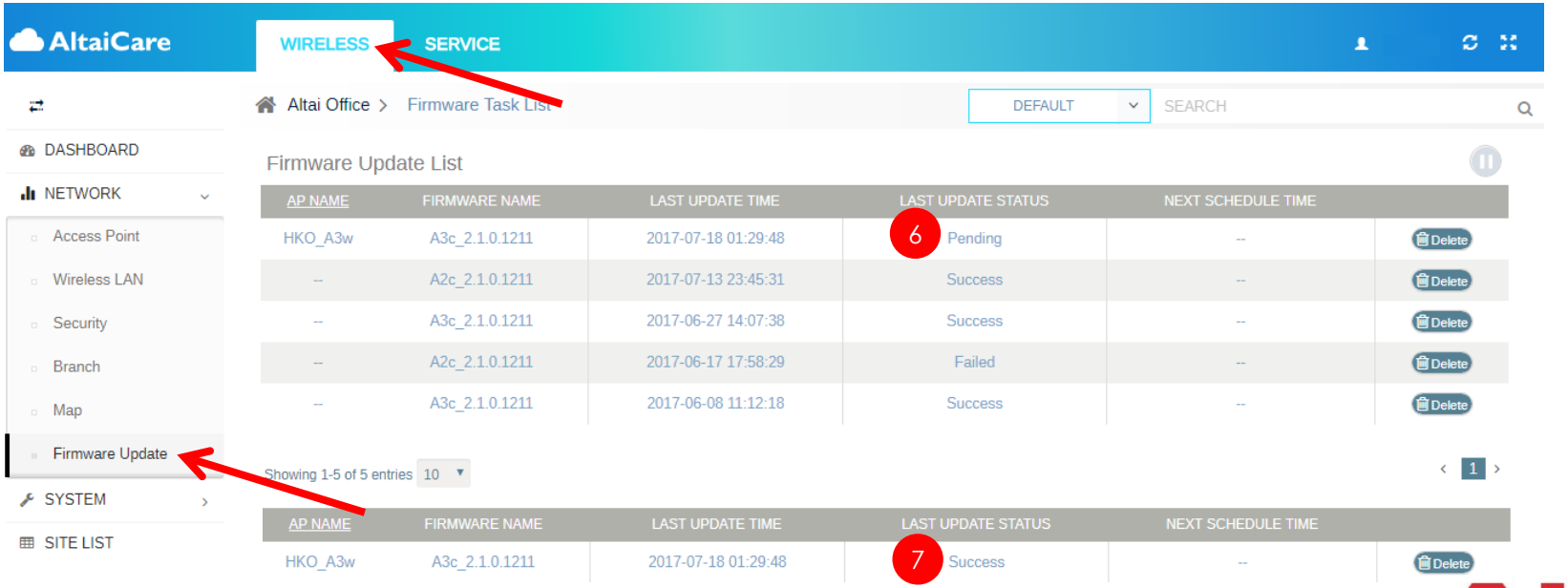
ALTAI Super WiFi

Single AP Firmware Update (Cont.)



Procedures:

5. Click "Go to detail page" to view the update status and it jumps to Wireless > Firmware Update.
6. Check the update status which is updated in every 30 seconds. Normally, it goes through several stages for the entire process: 1. Pending (which initiating the update); 2. In Progress; 3. Success or Failure.
7. Make sure the status becomes "Success" in the end.



Single AP Firmware Update (Cont.)

Procedures:

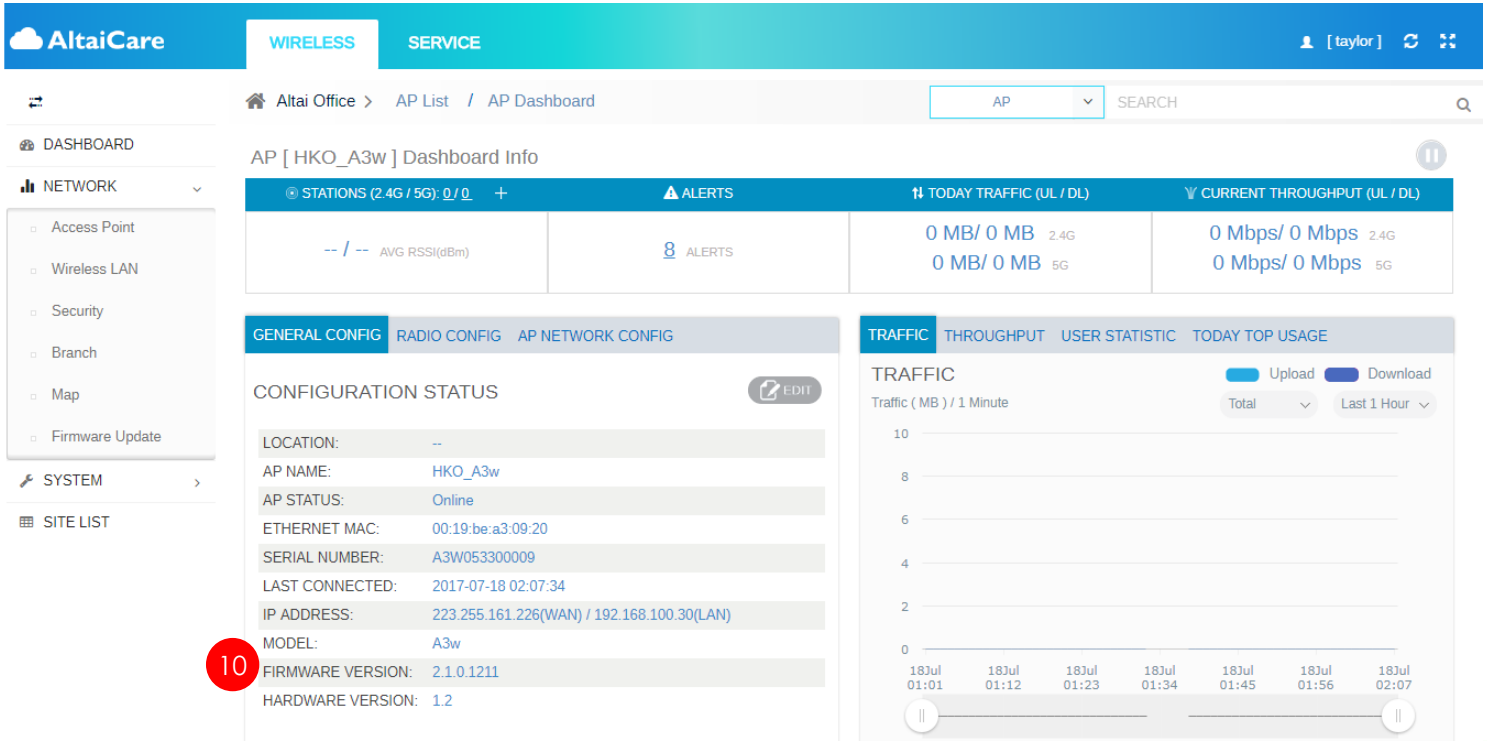
8. The AP status should turn from to
9. Click the AP Name and you will get the individual AP status dashboard.

ALTAI Super WiFi

Single AP Firmware Update (Cont.)

Procedures:

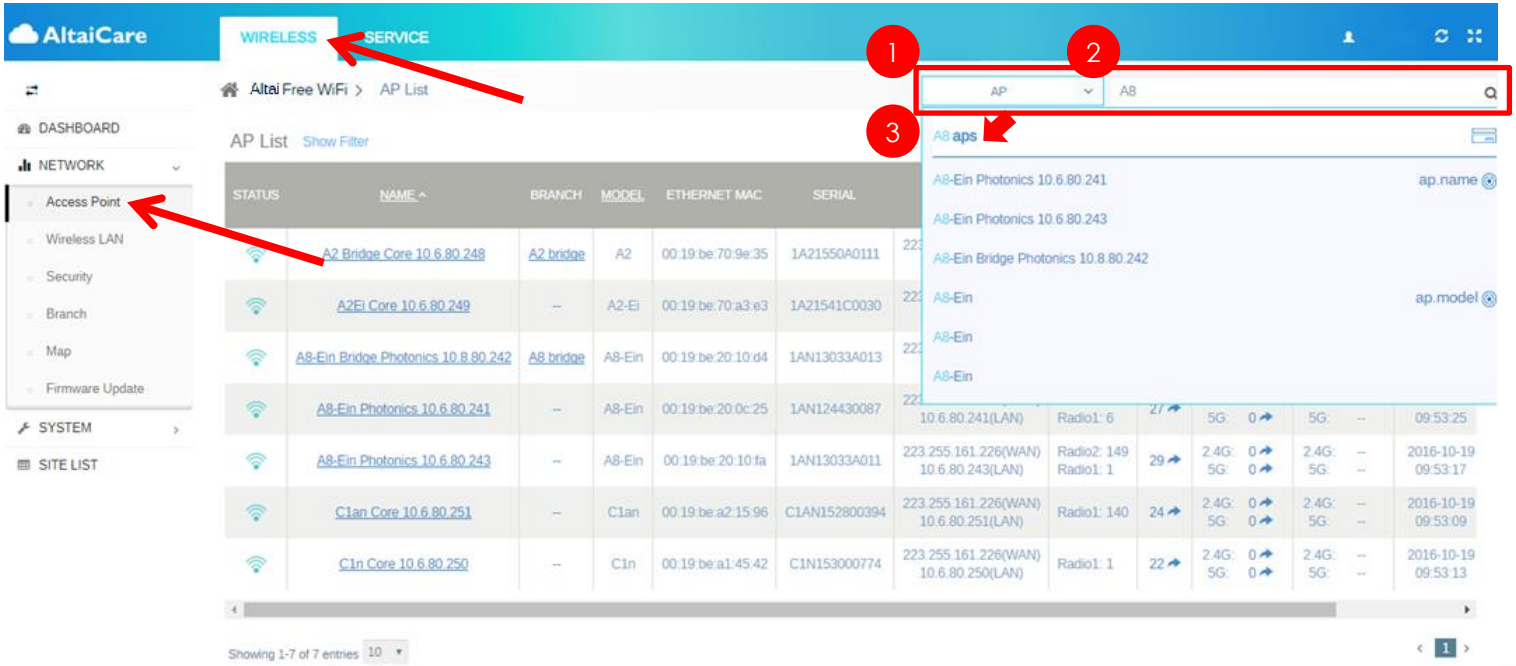
10. Now, you should be able to double check if the current AP firmware version is the target one.



AP Batch Firmware Update

Procedures:

1. Go to the Search Engine and select "AP" in the category.
2. Input the AP series name as keyword, e.g. A8, A3, A2, C1,C2.
3. A number of search targets will pop up. Hit the first one which is in form of <AP series name> aps, e.g. "A8 aps" on the screenshot below.



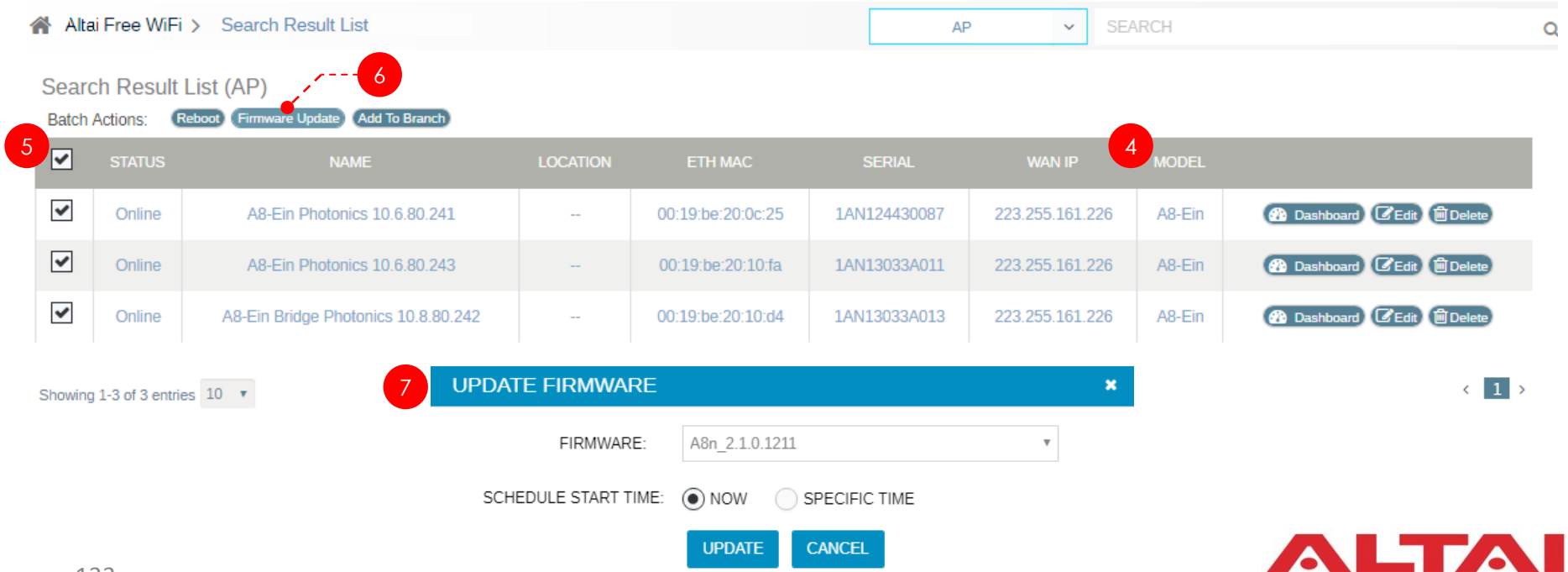
ALTAI Super WiFi

AP Batch Firmware Update (Cont.)

Procedures:

4. In this example, the result shows and filter out the A8n series products only based on the keyword "A8".
5. Check the box in the header row and all the boxes will then be checked automatically.
6. Hit the button "Firmware Update".
7. It will pop up a window for firmware batch update. Follow the same procedures from Step #2 to Step #10 in Section: Single AP Firmware Update for the batch update.

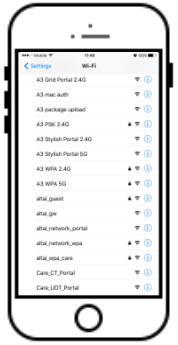
Warning: Make sure the AP unit is powered up throughout the whole firmware update process! Failure to do so might cause firmware crash.



Verification (Custom Template Portal)

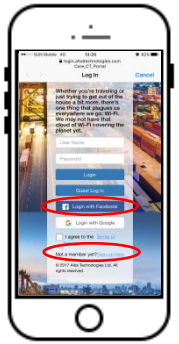
Verification: Custom Template Portal (Facebook Account Login – iOS Device)

1



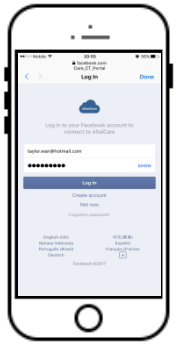
Turn on WiFi and Select SSID

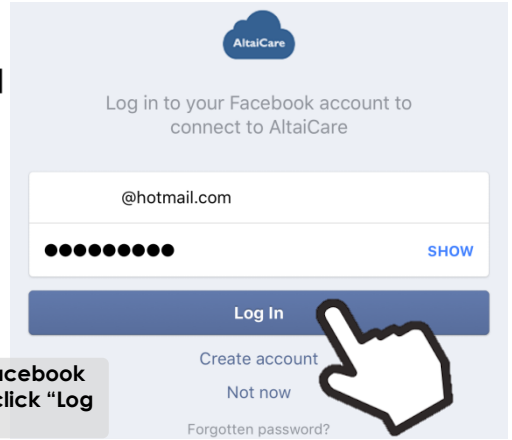
2



Portal Page pops up. Check the box and agree the Terms of Service. Then click Facebook Login Button

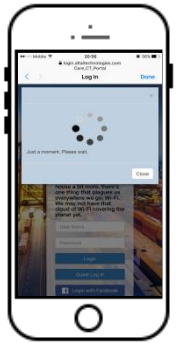
3





Sign up with Facebook account and click "Log In" button

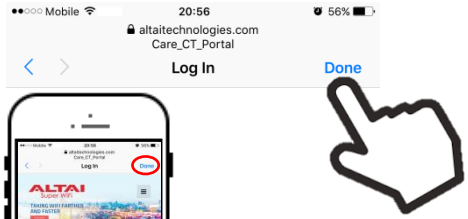
4



Upon click on "Log In" button, Facebook will verify your identity. If successful, it will then send your basic #personal information to AltaiCare for user account registration. It may take seconds

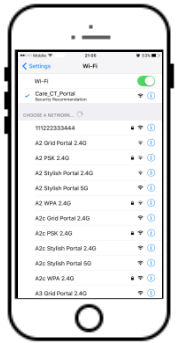
Basic personal Information include:
- Facebook Username
- Email
- Age Range (i.e. <21 or >21)
- Gender
- Locale

5

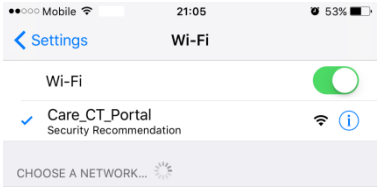


Once the account is successfully created, you will be redirected to a landing page. Click "DONE" to close the CNA window

6

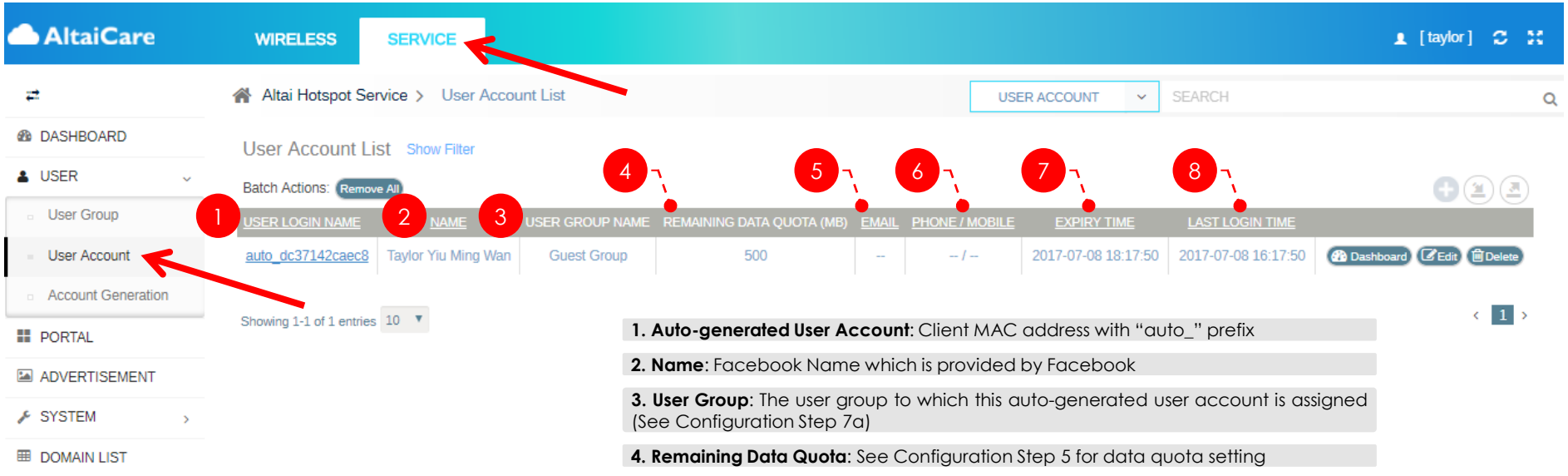


DONE! You are now connected with Care WiFi! Enjoy it ☺



ALTAI Super WiFi

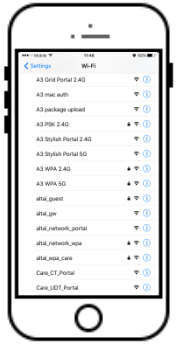
Verification: Custom Template Portal (Facebook Account Login)



1. **Auto-generated User Account**: Client MAC address with "auto_" prefix
2. **Name**: Facebook Name which is provided by Facebook
3. **User Group**: The user group to which this auto-generated user account is assigned (See Configuration Step 7a)
4. **Remaining Data Quota**: See Configuration Step 5 for data quota setting
5. **Email**: Email info which is provided by Facebook. Sometimes, you will no Email info received from Facebook because of the privacy setting of the individual users on their Facebook account
6. **Phone/Mobile**: Not applicable for Facebook Login
7. **Expiry Time**: Account validity which is counted from the Start at the first login. (See Configuration Step 5 for account validity setting)
8. **Last Login Time**

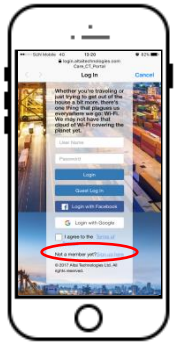
Verification: Custom Template Portal (Email Sign Up with Passcode Return – iOS Device)

1



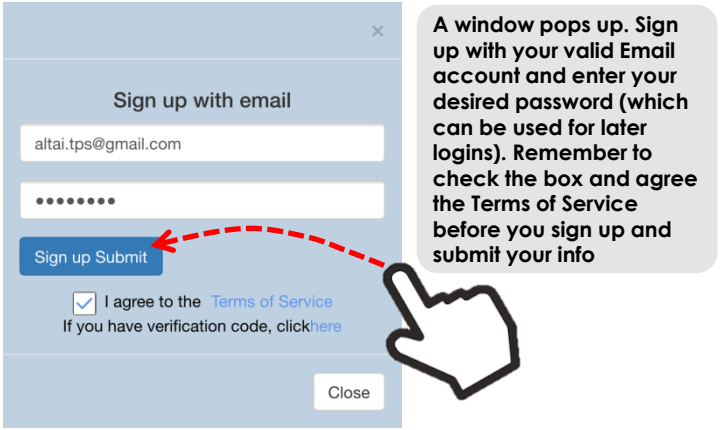
Turn on WiFi and Select SSID

2



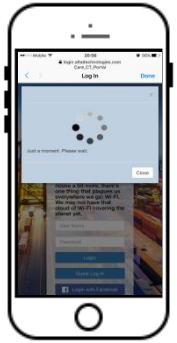
Portal Page pops up. For first time login, click the Sign Up link and use your Email for registration

3



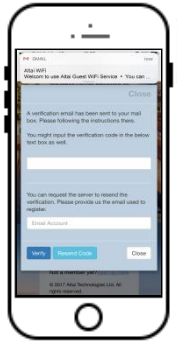
A window pops up. Sign up with your valid Email account and enter your desired password (which can be used for later logins). Remember to check the box and agree the Terms of Service before you sign up and submit your info

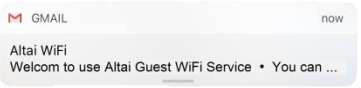
4



Upon click on "Sign up Submit" button, you will have 2 min for Internet access. In this time window, AltaiCare will generate passcode and send verification Email to your account. You are required to submit the code back in this timeslot for system verification and get Internet access

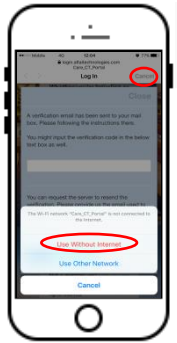
5

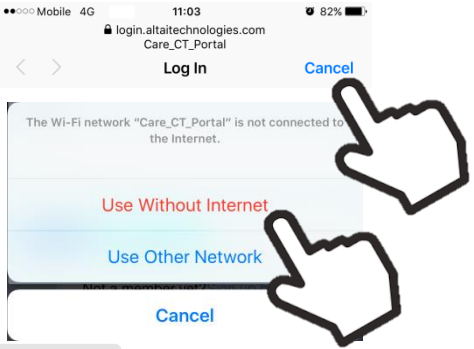




You will receive Email with verification code from AltaiCare System shortly

6



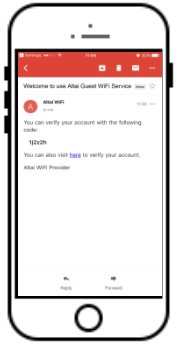


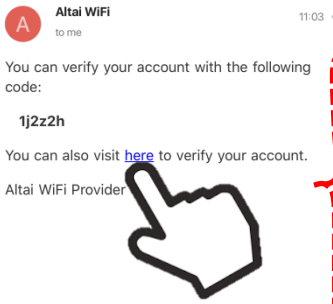
Click "Cancel" to close the CNA window and then click "Use Without Internet"

ALTAI Super WiFi

Verification: Custom Template Portal (Email Sign Up with Passcode Return – iOS Device)

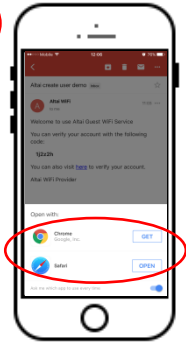
7





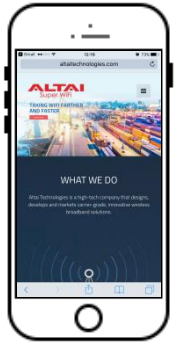
Open the Email and click the URL to send the passcode back to the system for verification

8a



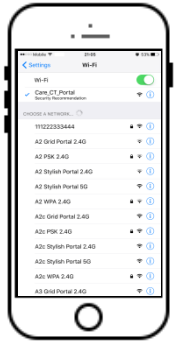
Open a browser and send the URL

9

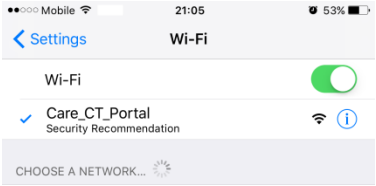


Once the code is verified OK, AltaiCare will automatically generate a user account using your registered email as username for you. In the meanwhile, you will be redirected to a landing page

10

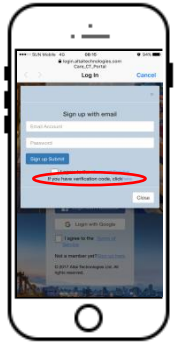


DONE! You are now connected with Care WiFi! Enjoy it ☺



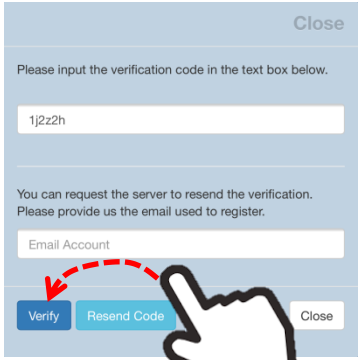
In case the 2-min window is over without completing the code verification process, then follow Step #8b instead of Step #8a

8b



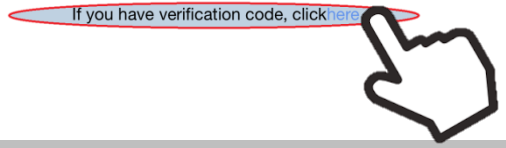
Follow Step #2 and bring you to this page again. Now, you already got the verification code, so click the link at the bottom

8b

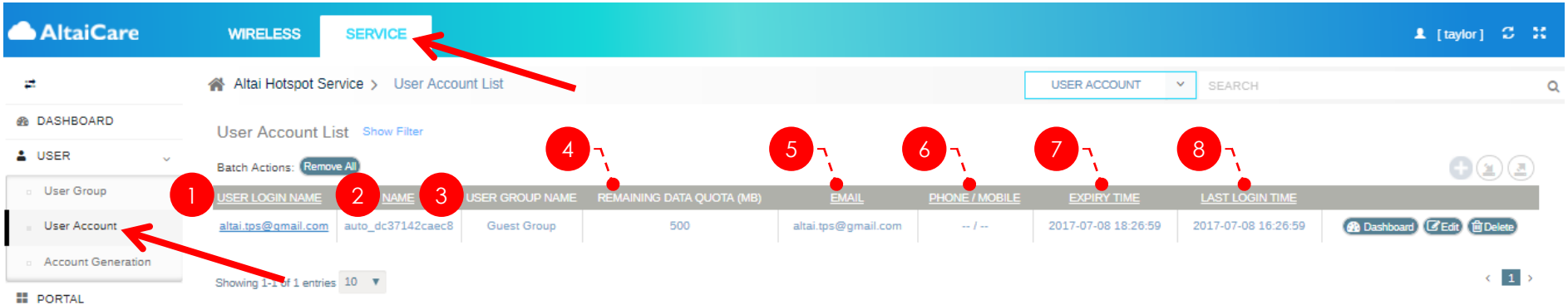


Enter the verification code and click "Verify" button

You can open a browser and type non-https website in the address bar to pop up the portal page. And then input the code in there to complete the remaining process and get the Internet access



Verification: Custom Template Portal (Email Sign Up with Passcode Return)



1. Auto-generated User Account: Email address that has been used as registration during sign up process

2. Name: Client MAC address with "auto_" prefix

3. User Group: The user group to which this auto-generated user account is assigned (See Configuration Step 7a)

4. Remaining Data Quota: See Configuration Step 5 for data quota setting

5. Email: Email info which is provided by the user during sign up process

6. Phone/Mobile: Not applicable for Email sign up Login

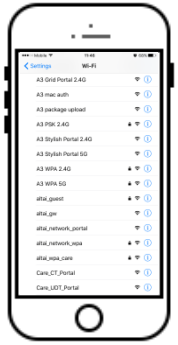
7. Expiry Time: Account validity which is counted from the Start at the first login. (See Configuration Step 5 for account validity setting)

8. Last Login Time

ALTAI Super WiFi

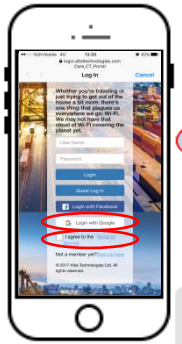
Verification: Custom Template Portal (Google Account Login – iOS Device)

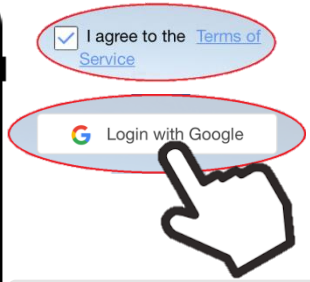
1



Turn on WiFi and Select SSID

2





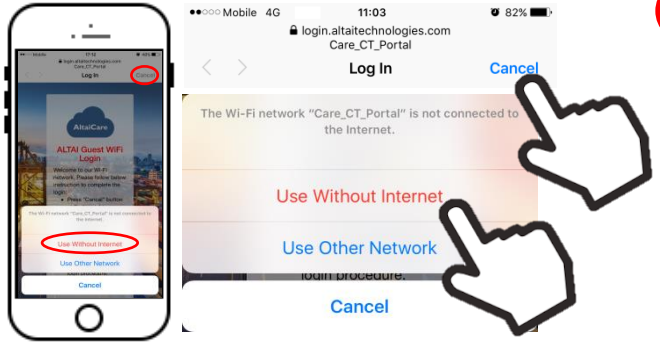
Portal Page pops up. Check the box and agree the Terms of Service. Then click Google Login Button

3

We cannot proceed Google Login through IOS CNA, so there is #instruction popping up to guide users how to bypass CNA and get access to network via Google login

#The system pops up the instruction page for Google login in IOS device by default, no matter whether the CNA detection is enabled or not

4

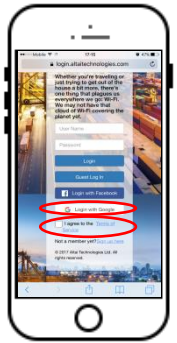


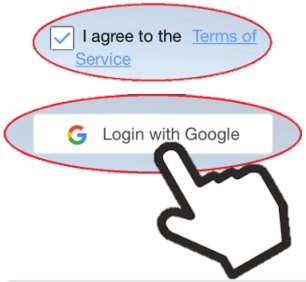
Click "Cancel" to close the CNA window and then click "Use Without Internet"

5

Open a browser and type non-https website in the address bar to pop up the portal page again

6



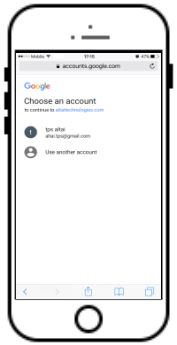


Same as Step #2. Check the box again and agree the Terms of Service. Then click Google Login Button

ALTAI Super WiFi

Verification: Custom Template Portal (Google Account Login – iOS Device)

7 **Sign up with Google account**



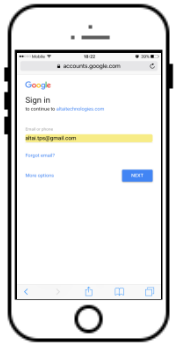
Google

Choose an account

to continue to altaitechnologies.com

t tps altai
altai.tps@gmail.com

Use another account



Google

Sign in

to continue to altaitechnologies.com

Email or phone

altai.tps@gmail.com

Forgot email?

More options NEXT

Google

Hi tps

t altai.tps@gmail.com

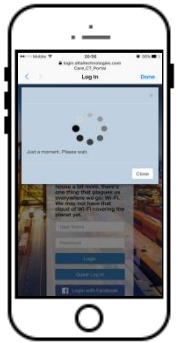
To continue, first verify it's you

Enter your password

••••••••••••

Forgot password? NEXT

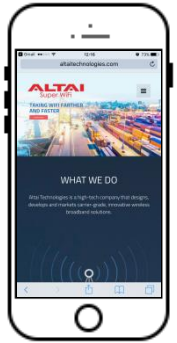
8



Upon submission of Google account credentials, Google will verify your identity. If successful, it will then send your basic #personal information to AltaiCare for user account registration. It may take seconds

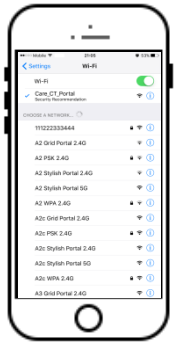
Basic personal Information include:
- Username
- Email
- Gender

9

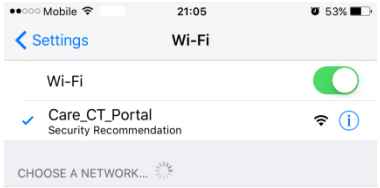


Once the account is successfully created, you will be redirected to a landing page.

10

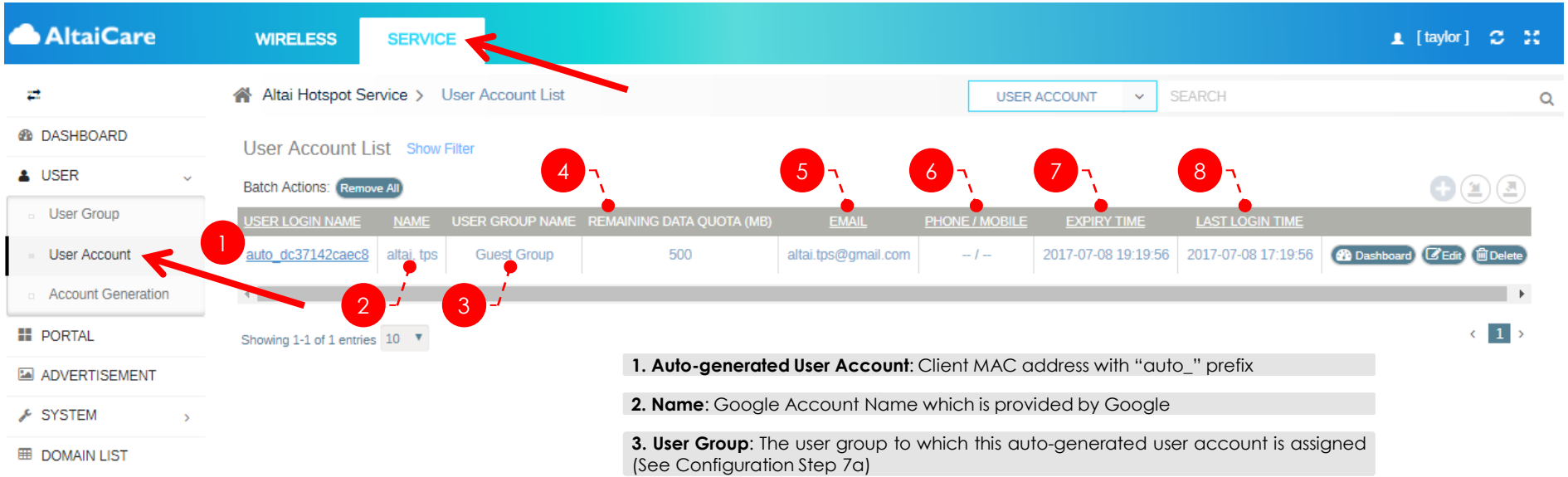


DONE! You are now connected with Care WiFi! Enjoy it ☺



ALTAI Super WiFi

Verification: Custom Template Portal (Google Account Login)



1. **Auto-generated User Account**: Client MAC address with "auto_" prefix

2. **Name**: Google Account Name which is provided by Google

3. **User Group**: The user group to which this auto-generated user account is assigned (See Configuration Step 7a)

4. **Remaining Data Quota**: See Configuration Step 5 for data quota setting

5. **Email**: Email info which is provided by Google

6. **Phone/Mobile**: Not applicable for Google Login

7. **Expiry Time**: Account validity which is counted from the Start at the first login. (See Configuration Step 5 for account validity setting)

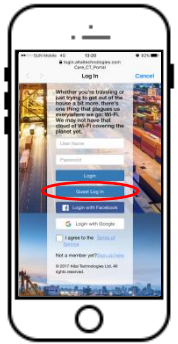
8. **Last Login Time**

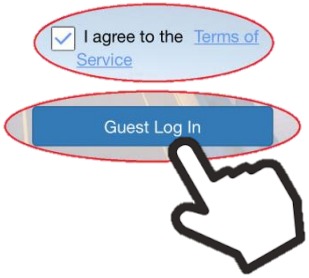
Verification: Custom Template Portal (Guest Login – iOS Device)

1

Turn on WiFi and Select SSID

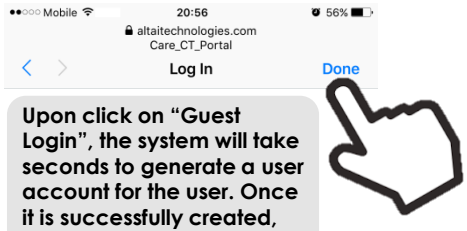
2





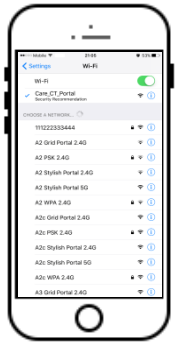
Portal Page pops up. Check the box and agree the Terms of Service. Then click Guest Login Button

3

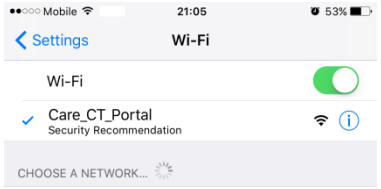


Upon click on "Guest Login", the system will take seconds to generate a user account for the user. Once it is successfully created, you will be redirected to a landing page. Click "DONE" to close the CNA window

4



DONE! You are now connected with Care WiFi! Enjoy it ☺

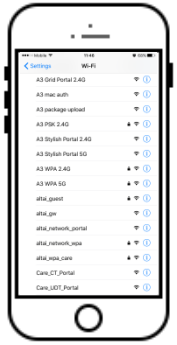


ALTAI Super WiFi

Verification (User Defined Template Portal)

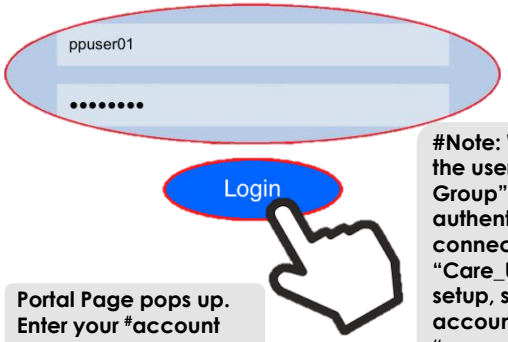
Verification: User Defined Template Portal (Username/Password Login – iOS Device)

1



Turn on WiFi and Select SSID

2



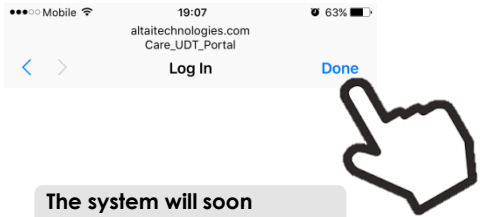
Portal Page pops up. Enter your #account Username/Password. Then click Login Button

#Note: We only allowed the user group "PP User Group" for user authentication and connection with the SSID "Care_UDT_Portal" in our setup, so we use the user account "ppuser01/ppuser01" for portal login

3

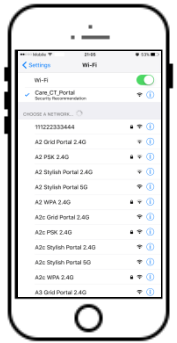
Upon click on Login button, AltaiCare will verify your identity against its user database. If successful, it will return you a message "Login Successfully!". It may take seconds

4

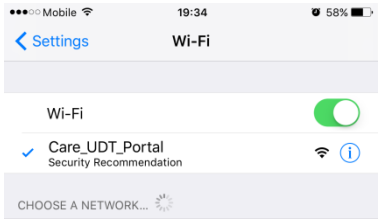


The system will soon redirect you to a landing page. Click "DONE" to close the CNA window

5

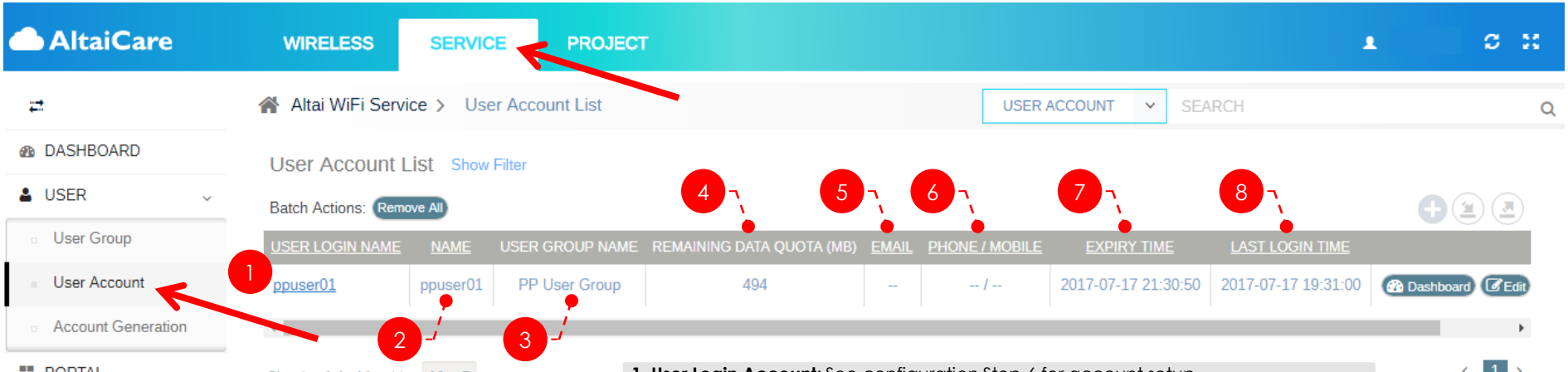


DONE! You are now connected with Care WiFi! Enjoy it ☺



ALTAI Super WiFi

Verification: User Defined Template Portal (Username/Password Login – iOS Device)



1. **User Login Account**: See configuration Step 6 for account setup
2. **Account Name**: See configuration Step 6 for account setup
3. **User Group**: The user group to which this user account belongs (See configuration Steps 5 and 6)
4. **Remaining Data Quota**: See Configuration Steps 5 or 6 for data quota setting
5. **Email**: Email info which is optional during account setup
6. **Phone/Mobile**: Phone/Mobile info which is optional during account setup
7. **Expiry Time**: Account validity which is counted from the Start at the first login. (See Configuration Step 5 for account validity setting)
8. **Last Login Time**

Verification: User Defined Template Portal (Guest Login – iOS Device)

1

Turn on WiFi and Select SSID

2

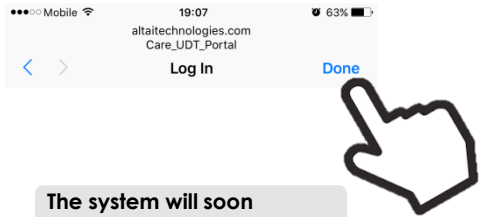
Portal Page pops up. Then click Guest Button

3

…a few sec later

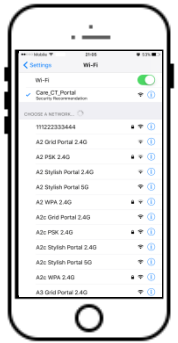
Upon click on Guest button, AltaiCare will take seconds to generate a user account for the user. Once it is successfully created, you will get a message “Login Successfully!”.

4

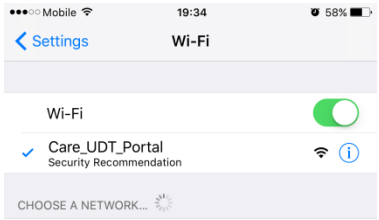


The system will soon redirect you to a landing page. Click “DONE” to close the CNA window

5

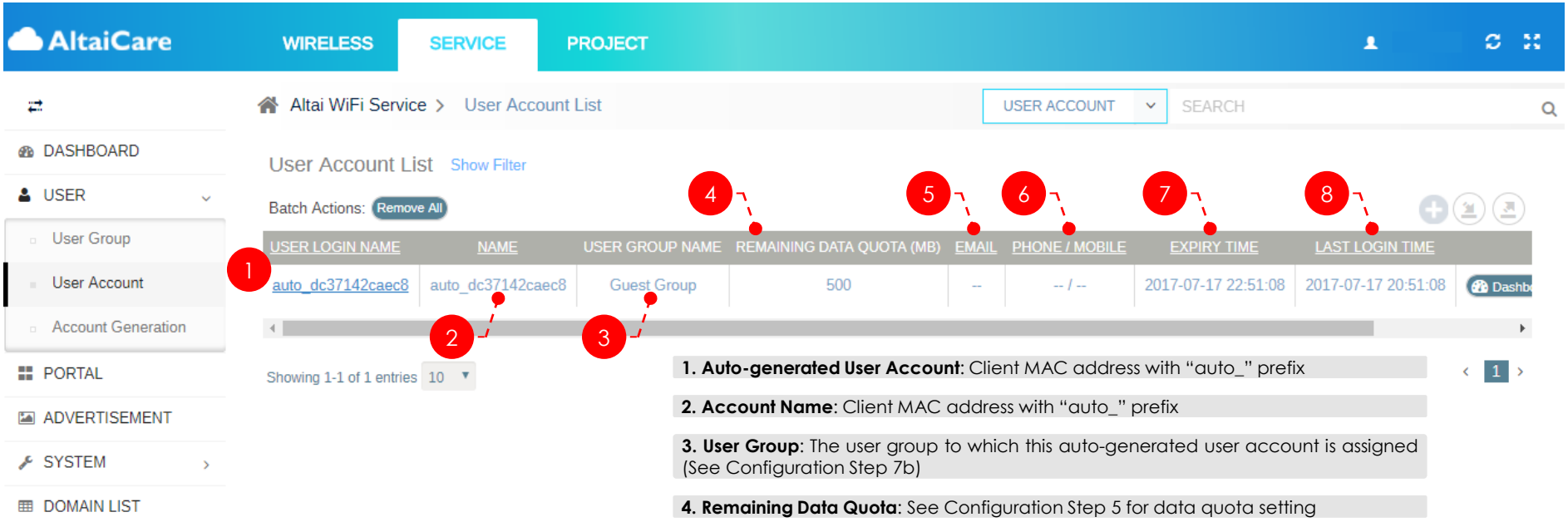


DONE! You are now connected with Care WiFi! Enjoy it ☺



ALTAI Super WiFi

Verification: User Defined Template Portal (Guest Login – iOS Device)



1. **Auto-generated User Account**: Client MAC address with "auto_" prefix
2. **Account Name**: Client MAC address with "auto_" prefix
3. **User Group**: The user group to which this auto-generated user account is assigned (See Configuration Step 7b)
4. **Remaining Data Quota**: See Configuration Step 5 for data quota setting
5. **Email**: Not applicable for Guest Login
6. **Phone/Mobile**: Not applicable for Guest Login
7. **Expiry Time**: Account validity which is counted from the Start at the first login. (See Configuration Step 5 for account validity setting)
8. **Last Login Time**

ALTAI Super WiFi

Verification: User Defined Template Portal (Sign Up Login – iOS Device)

1

Turn on WiFi and Select SSID

2

Portal Page pops up. Then click Sign-Up button

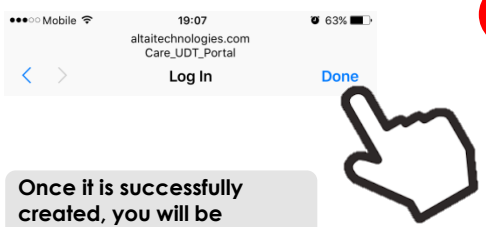
3

It jumps to Sign Up Page. Sign up with your personal info. Then click Confirm button

4

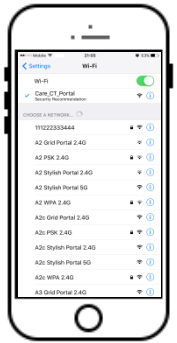
…a few sec later

Upon click on Confirm button, AltaiCare will take seconds to process your submitted data and generate a user account for the user.

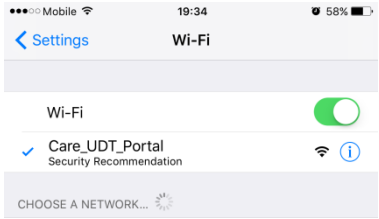


Once it is successfully created, you will be redirected to a landing page. Click “DONE” to close the CNA window

5

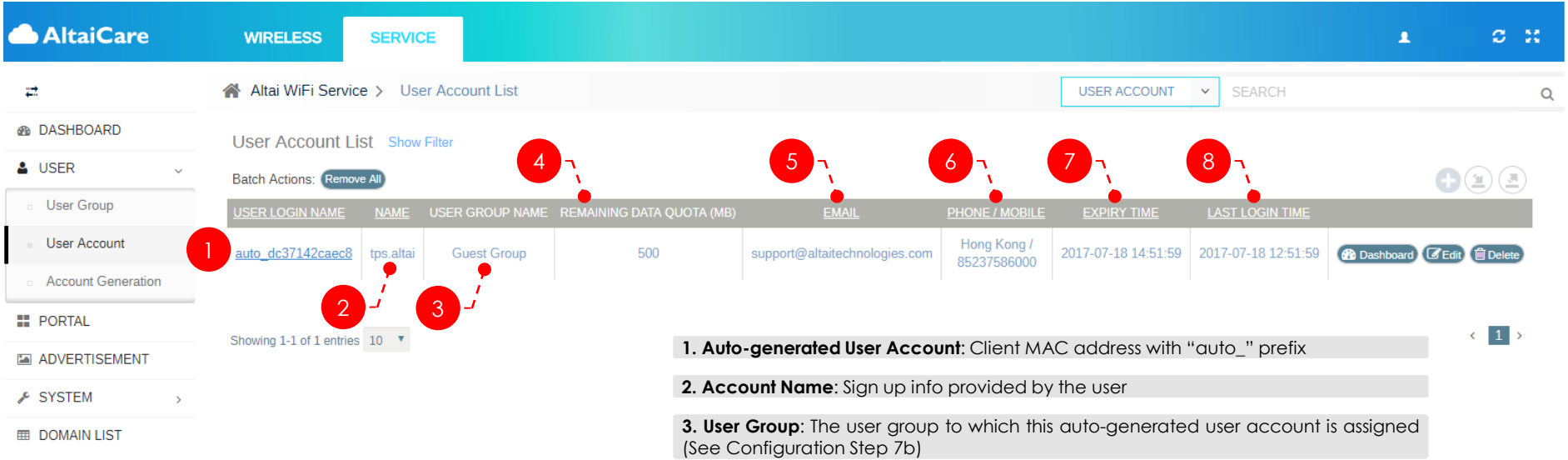


DONE! You are now connected with Care WiFi! Enjoy it ☺



ALTAI Super WiFi

Verification: User Defined Template Portal (Sign Up Login – iOS Device)



1. **Auto-generated User Account**: Client MAC address with "auto_" prefix
2. **Account Name**: Sign up info provided by the user
3. **User Group**: The user group to which this auto-generated user account is assigned (See Configuration Step 7b)
4. **Remaining Data Quota**: See Configuration Step 5 for data quota setting
5. **Email**: Sign up info provided by the user
6. **Phone/Mobile**: Sign up info provided by the user
7. **Expiry Time**: Account validity which is counted from the Start at the first login. (See Configuration Step 5 for account validity setting)
8. **Last Login Time**

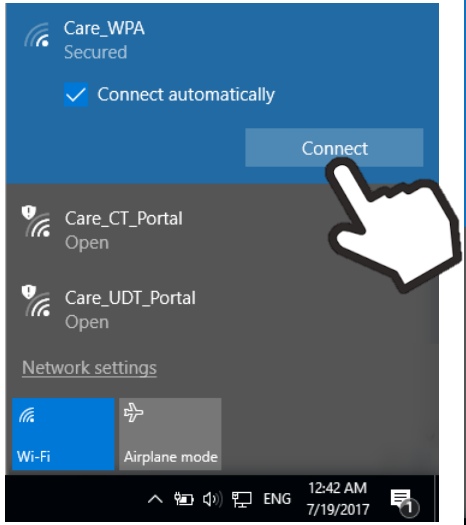
ALTAI Super WiFi

Verification (WPA – PEAP)

Verification: WPA (PEAP – Windows 10 Client)

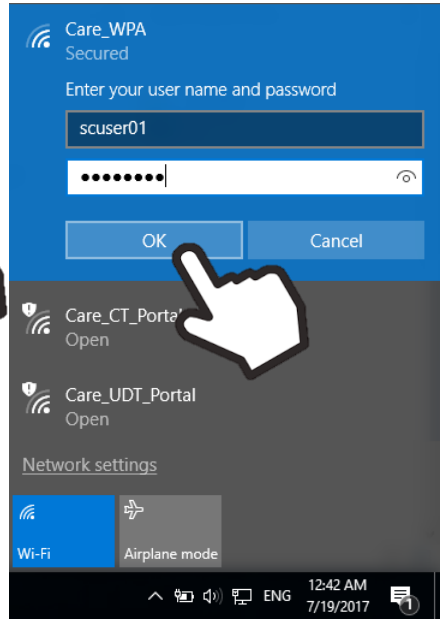
1

Turn on WiFi and Select SSID, i.e. Care_WPA for our case. Check the box of "Connect automatically" and click "Connect"



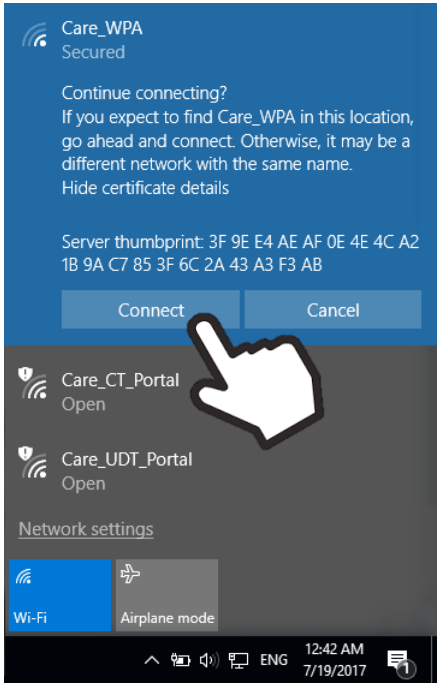
2

Enter your credentials, i.e. scuser01/scuser01 and then click "OK"



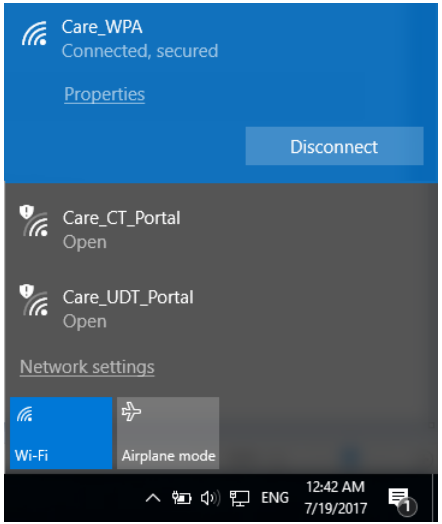
3

Click "Connect" when being asked for your confirmation to connect to the network with the above certificate for the first time login



4

DONE! You are now connected with Care WiFi! Enjoy it ☺

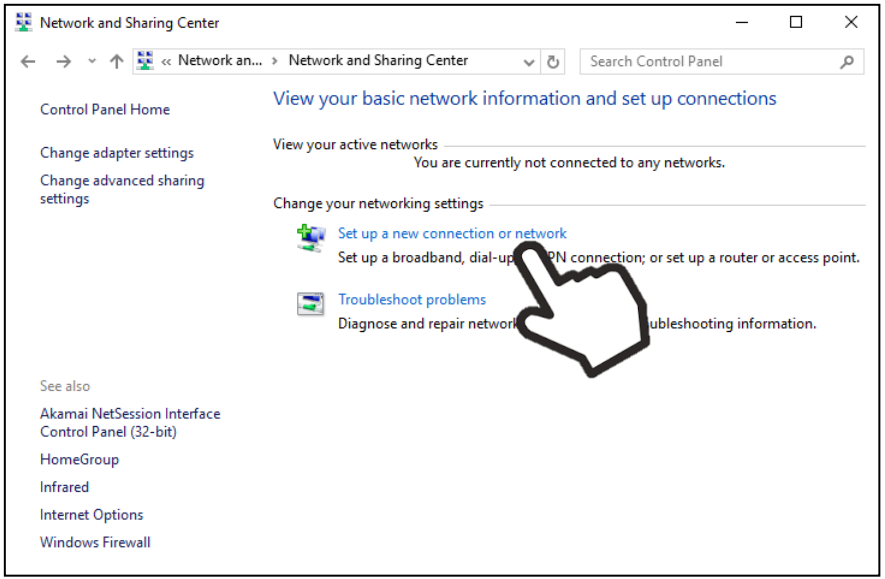


ALTAI Super WiFi

Verification: WPA (PEAP – Windows 10 Client)

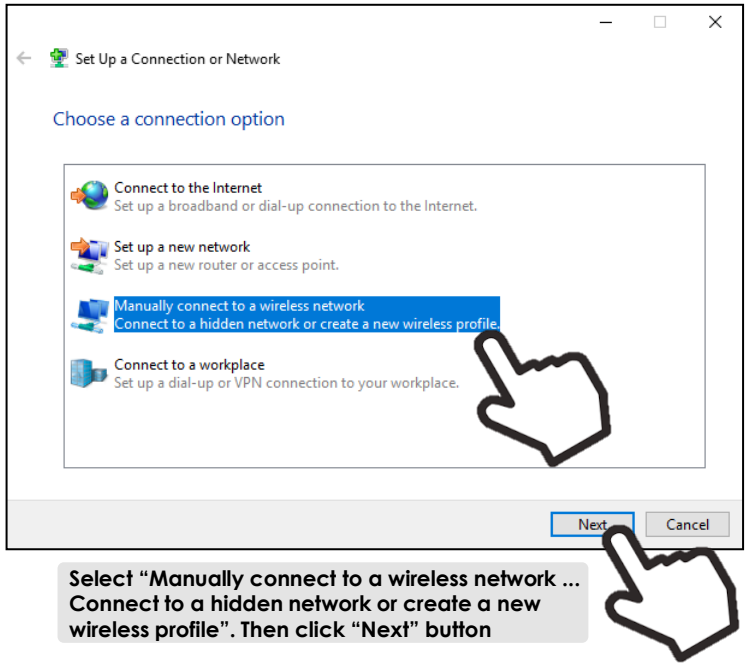
Note: In some of the cases such as hidden network, your may need to manually create wireless profile for connection to the wireless network.

1



Open Network and Sharing Center. Click "Set up a new connection or network" to create a new wireless network profile

2

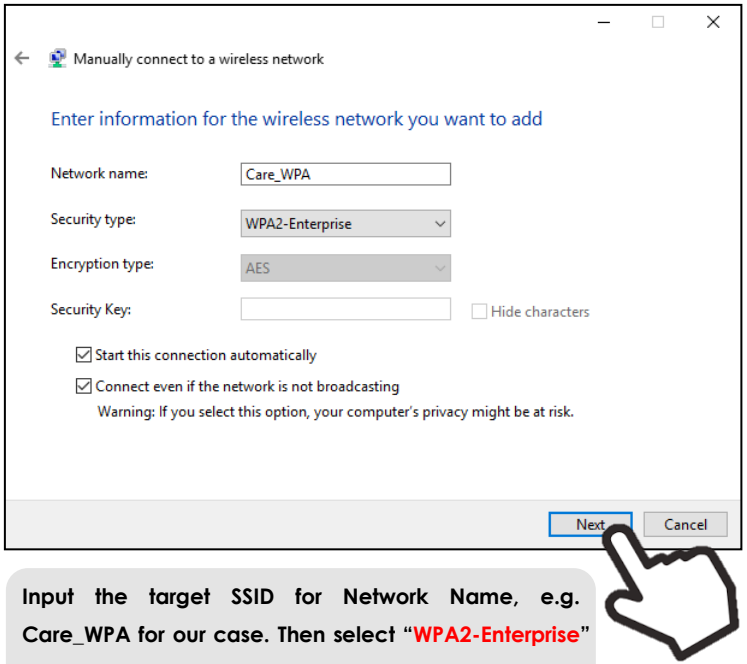


Select "Manually connect to a wireless network ... Connect to a hidden network or create a new wireless profile". Then click "Next" button

ALTAI Super WiFi

Verification: WPA (PEAP – Windows 10 Client)

3

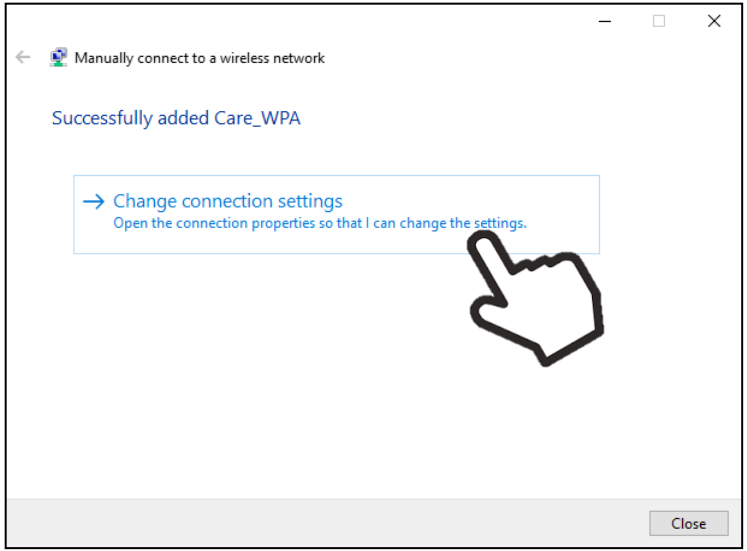


Input the target SSID for Network Name, e.g. Care_WPA for our case. Then select "WPA2-Enterprise" as Security Type and "AES" as Encryption Type. Check the boxes for the following two items:

- Start this connection automatically
- Connect even if the network is not broadcasting

Click "Next" to finish the wireless profile settings

4

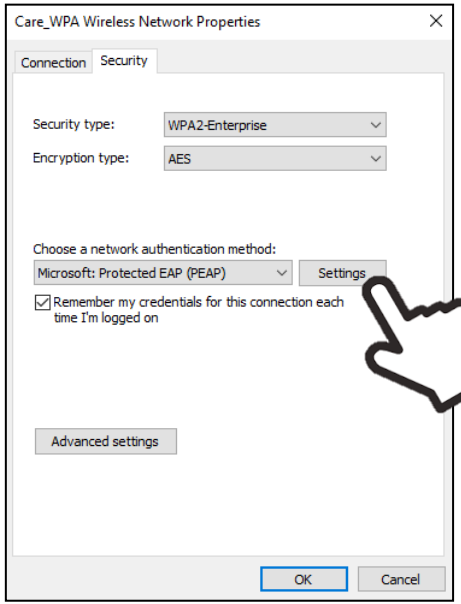


The wireless profile for SSID, i.e. "Care_WPA" has just been created. Click "Change connection settings" for further configuration changes

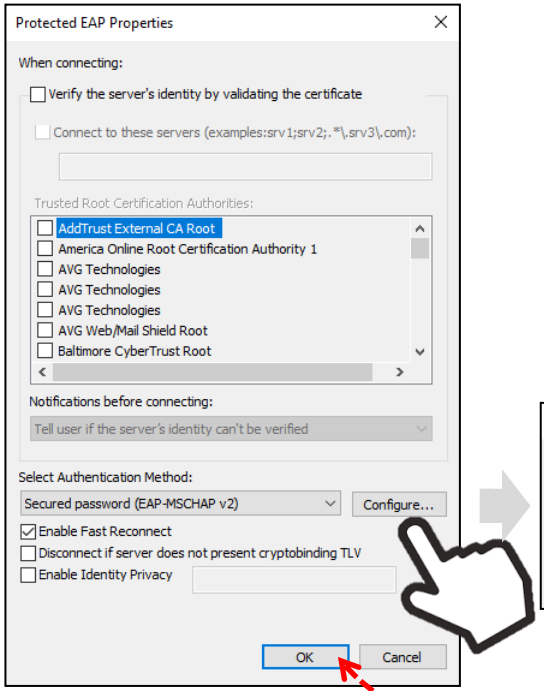
ALTAI Super WiFi

Verification: WPA (PEAP – Windows 10 Client)

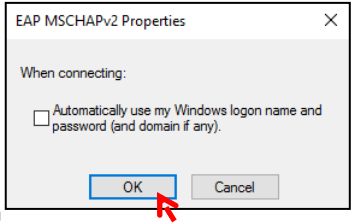
5



"Wireless Network Properties" window pops up. Select "PEAP" as Authentication Method and click "Settings" for further configuration



Uncheck the box of "Verify the server's identity by validating the certificate". Select "EAP-MSCHAP v2" as Authentication Method and then click "Configure…" for further changes

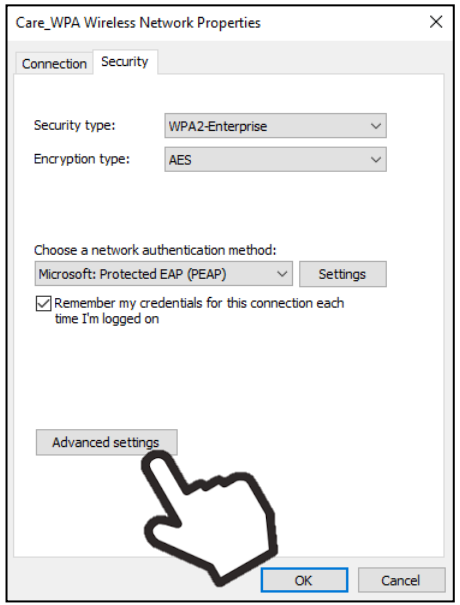


Uncheck the box of "Automatically use my Windows logon name and password (and domain if any)." and then click "OK" to go back to "Protected EAP Properties" Window. Click "OK" again to go back to "Wireless Network Properties" window

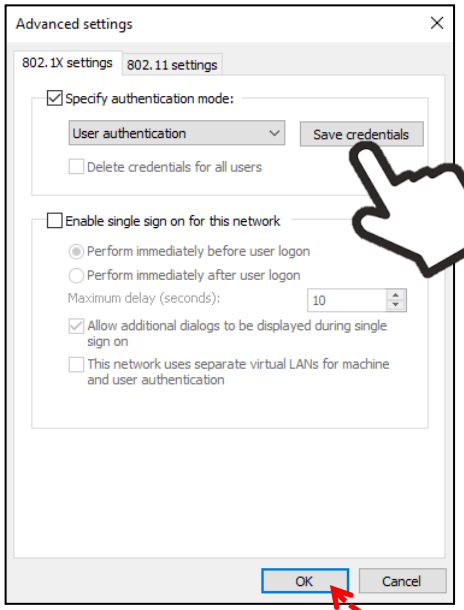
ALTAI Super WiFi

Verification: WPA (PEAP – Windows 10 Client)

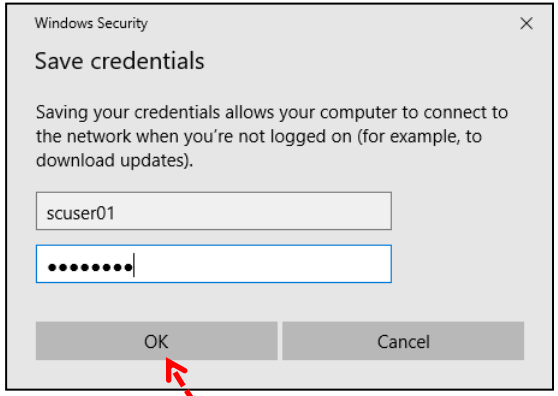
6



Click "Advanced settings"



Click the tab "802.1X settings" and choose "User authentication" as authentication mode. Then click "Save credentials"

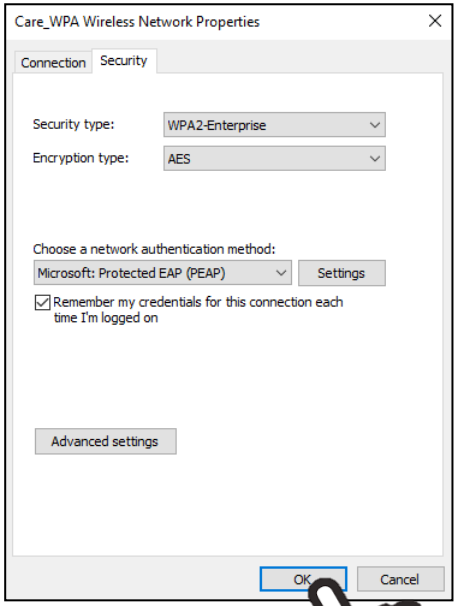


Input username and password. Then click "OK" to go back to "Advanced settings" window. Click "OK" again to go back to "Wireless Network Properties" window.

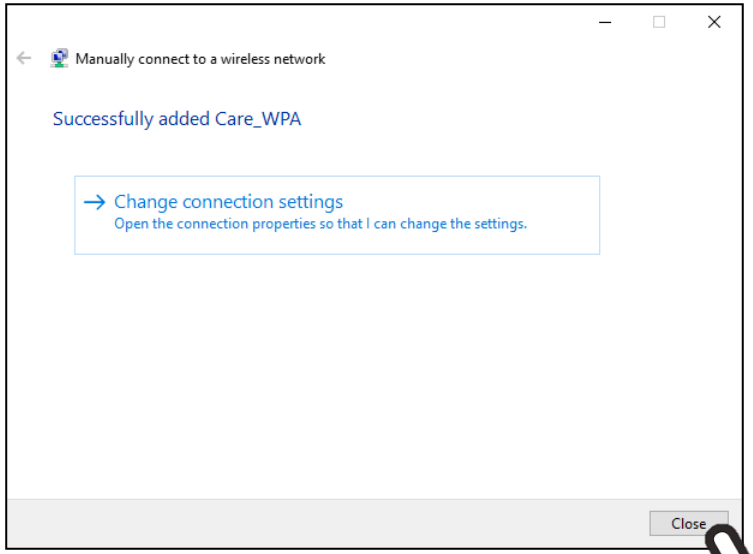
ALTAI Super WiFi

Verification: WPA (PEAP – Windows 10 Client)

7

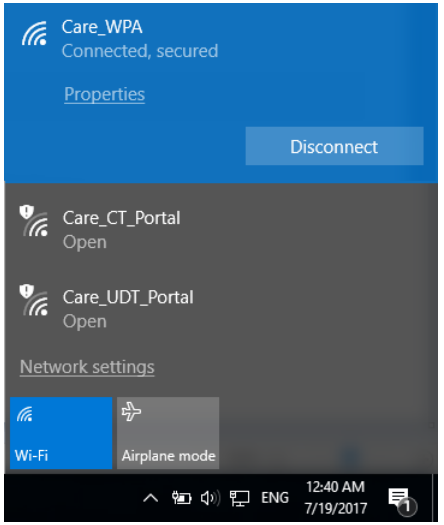


Click "OK" to close "Wireless Network Properties" window



Click "Close" to finish the wireless network profile setting

8

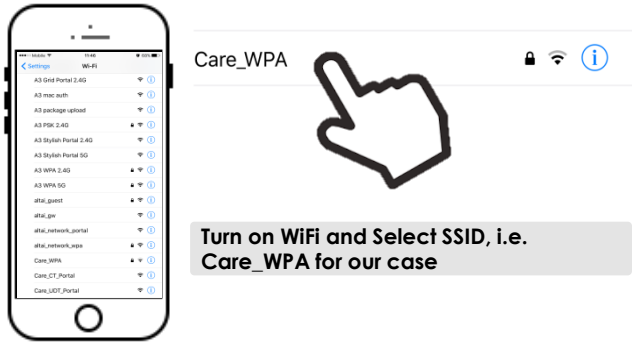


DONE! The client will then automatically connect with Care WiFi! Enjoy it ☺

ALTAI Super WiFi

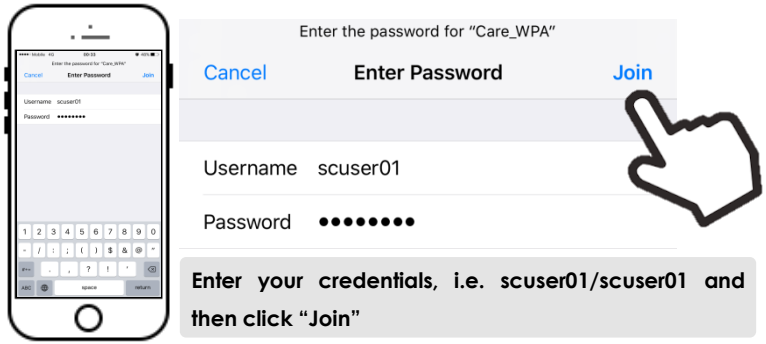
Verification: WPA (PEAP – iOS Device)

1



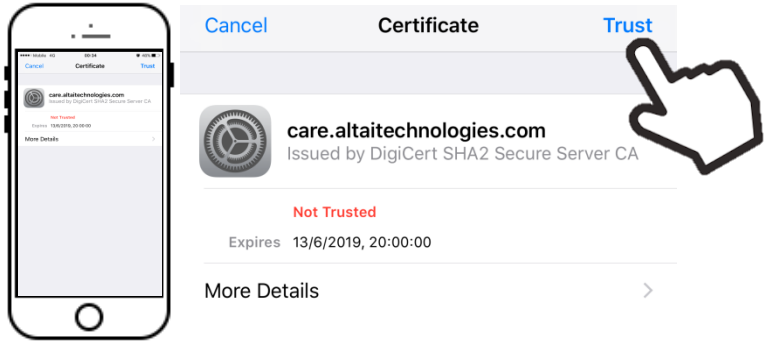
Turn on WiFi and Select SSID, i.e. Care_WPA for our case

2



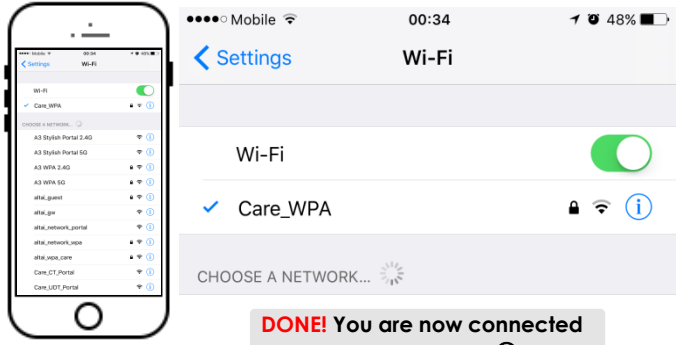
Enter your credentials, i.e. scuser01/scuser01 and then click "Join"

3



Press "Trust" when prompt with the above certificate for the first time login

4



DONE! You are now connected with Care WiFi! Enjoy it ☺

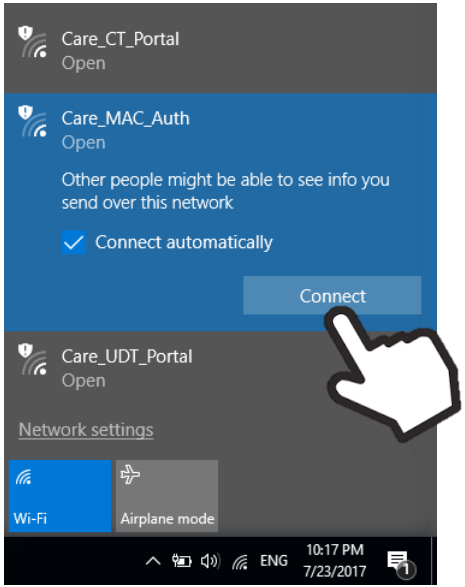
ALTAI Super WiFi

Verification (MAC Authentication)

Verification: MAC Auth (Windows 10 Client)

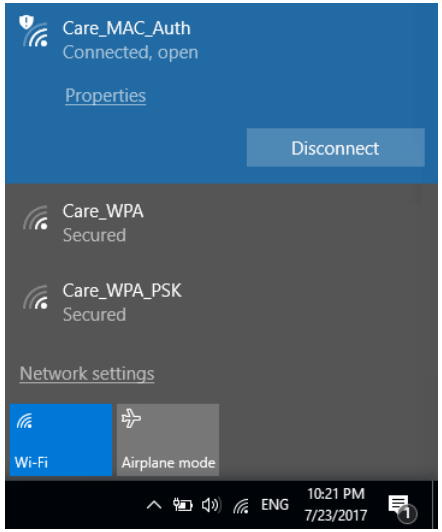
1

Turn on WiFi and Select SSID, i.e. Care_MAC_Auth for our case. Check the box of "Connect automatically" and click "Connect"



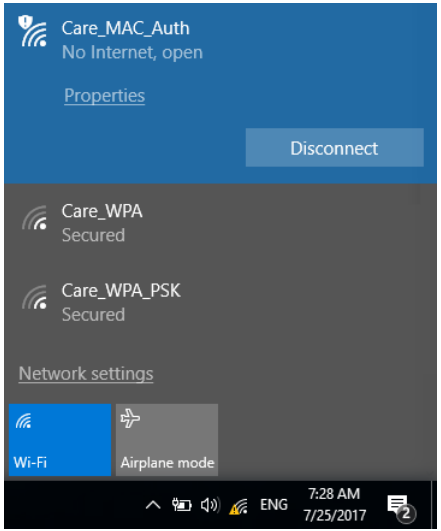
2a

DONE! You are now connected with Care WiFi! Enjoy it ☺



2b

For those clients which are not in the registered MAC addresses list of the allowed user group(s), they will not be allowed to get Internet access

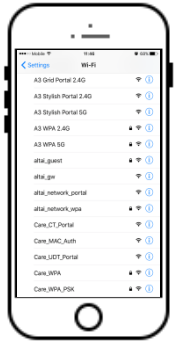


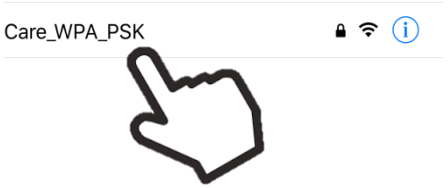
ALTAI Super WiFi

Verification (WPA-PSK)

Verification: WPA-PSK (iOS Device)

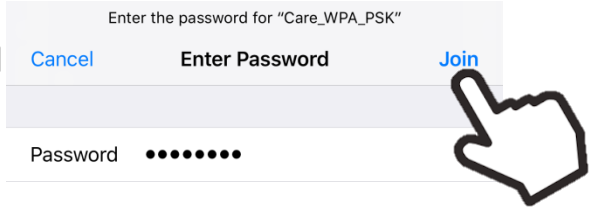
1





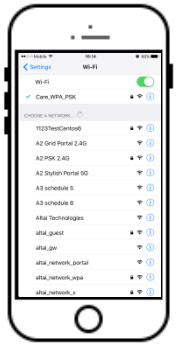
Turn on WiFi and Select SSID, i.e. Care_WPA_PSK for our case

2



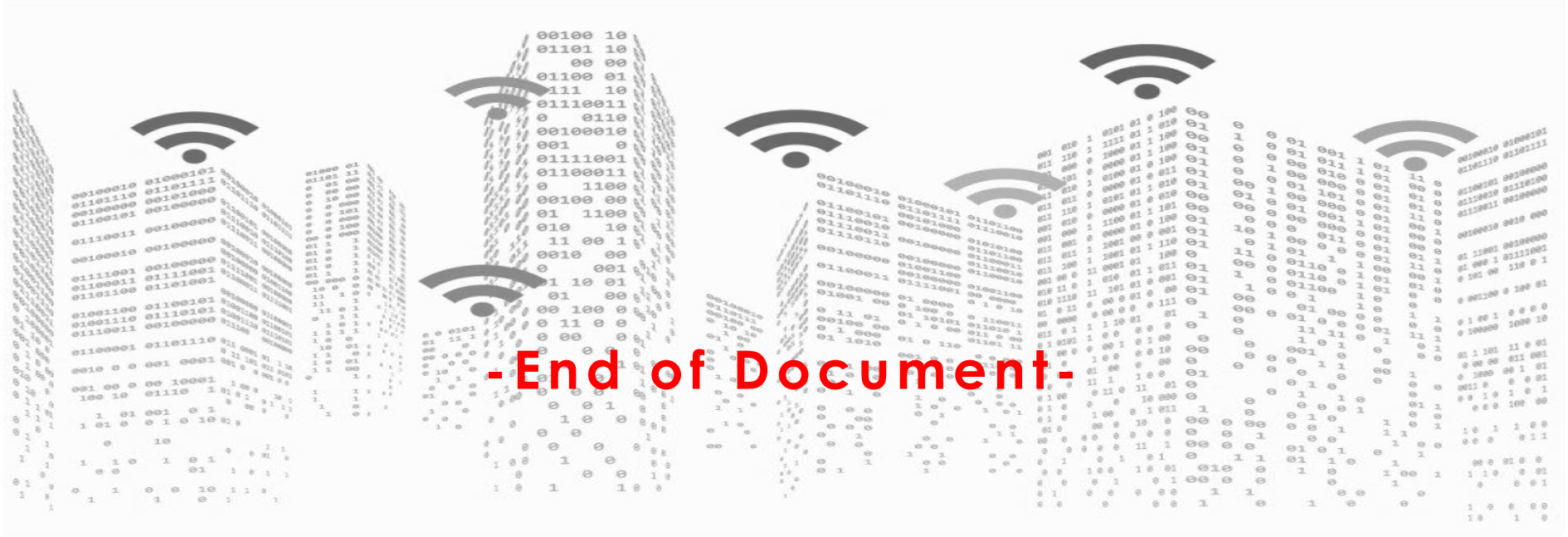
Enter the Password and then click "Join"

3



DONE! You are now connected with Care WiFi! Enjoy it ☺

ALTAI Super WiFi



Altai Technologies Limited
Unit 209, 2/F, Lakeside 2,
10 Science Park West Avenue,
Hong Kong Science Park,
Shatin, New Territories,
Hong Kong

Telephone: +852 3758 6000
Fax: +852 2607 4021
Web: www.altaitechnologies.com

Customer Support Centre:
Email: support@altaitechnologies.com

ALTAI Super WiFi