



# AltaiCare Training

Version 2.1  
August, 2017

# Training Content

Item	Topic	Duration	Presented By	Participants	Prerequisite	Preparation Required
1	<b>AltaiCare Overview</b>	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	<a href="#">Wireless Network Management Feature Highlights</a>					
1.2	<a href="#">Service Control Feature Highlights</a>					
2	<b>Case Study</b>					
2.1	<a href="#">Typical Network Topology</a>					
2.2	<a href="#">Call Flow for Built-In Portal Auth</a>					
2.3	<a href="#">Call Flow for Built-In RADIUS Auth (WPA)</a>					
2.4	<a href="#">Portal Template Types</a>					
3	<b>Before You Begin – AP Configuration</b>					
3.1	<a href="#">Access to AP WebUI</a>					
3.2	<a href="#">Step 1: Network Setting</a>					
3.3	<a href="#">Step 2 (Optional): Management VLAN Setting (Applicable to local VLAN environment only)</a>					
3.4	<a href="#">Step 3: Enable Remote Management</a>					
3.5	<a href="#">Step 4: Save &amp; Apply AP Configuration Change</a>					
4	<b>Getting Started</b>					
4.1	<a href="#">AltaiCare Hierarchy Overview</a>					
4.2	<a href="#">Multiple Level Access Control</a>					
4.3	<a href="#">AltaiCare Credit System and Policy</a>					
4.4	<a href="#">Access to AltaiCare</a>					
4.5	<a href="#">AltaiCare Web Interface</a>					
4.6	<a href="#">Wireless Management Overview</a>					
4.7	<a href="#">Service Management Overview</a>					
4.8	<a href="#">Project Management Overview</a>					

# Training Content

Item	Topic	Duration	Presented By	Participants	Prerequisite	Preparation Required
5	<b>Basic Configuration</b>	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	<a href="#">Configuration Procedures</a>					
5.2	<a href="#">Step 1: Create new Site</a>					
5.3	<a href="#">Step 2: Create new Service Domain</a>					
5.4	<a href="#">Step 3: Create Admin Account for Site/Service Domain</a>					
5.5	<a href="#">Step 4: Create User Group</a>					
5.6	<a href="#">Step 5: Create User Account</a>					
5.7	<a href="#">Step 5a: Create Single User Account</a>					
5.8	<a href="#">Step 5b: Create Single MAC Account</a>					
5.9	<a href="#">Step 5c: Batch import (in .CSV file) of user accounts</a>					
5.10	<a href="#">Step 5d: Voucher-based user account batch generation</a>					
5.11	<a href="#">Step 6a: Custom Template Portal Setup</a>					
5.12	<a href="#">Step 6b: User Defined Template Portal Setup</a>					
5.13	<a href="#">Step 7a: Create Security Profile for Portal</a>					
5.14	<a href="#">Step 7b: Create Security Profile for WPA</a>					
5.15	<a href="#">Step 7c: Create Security Profile for MAC Auth</a>					
5.16	<a href="#">Step 7d: Create Security Profile for WPA-PSK</a>					
5.17	<a href="#">Step 8: Create SSID (WLAN)</a>					
5.18	<a href="#">Step 9: AP Registration</a>					
5.19	<a href="#">Step 9a: Single AP Registration</a>					
5.20	<a href="#">Step 9b: AP Batch Registration</a>					
6	<b>AP Firmware Update</b>					
6.1	<a href="#">AP Firmware Compatibility Check</a>					
6.2	<a href="#">Single AP Firmware Update</a>					
6.3	<a href="#">AP Batch Firmware Update</a>					

# Training Content

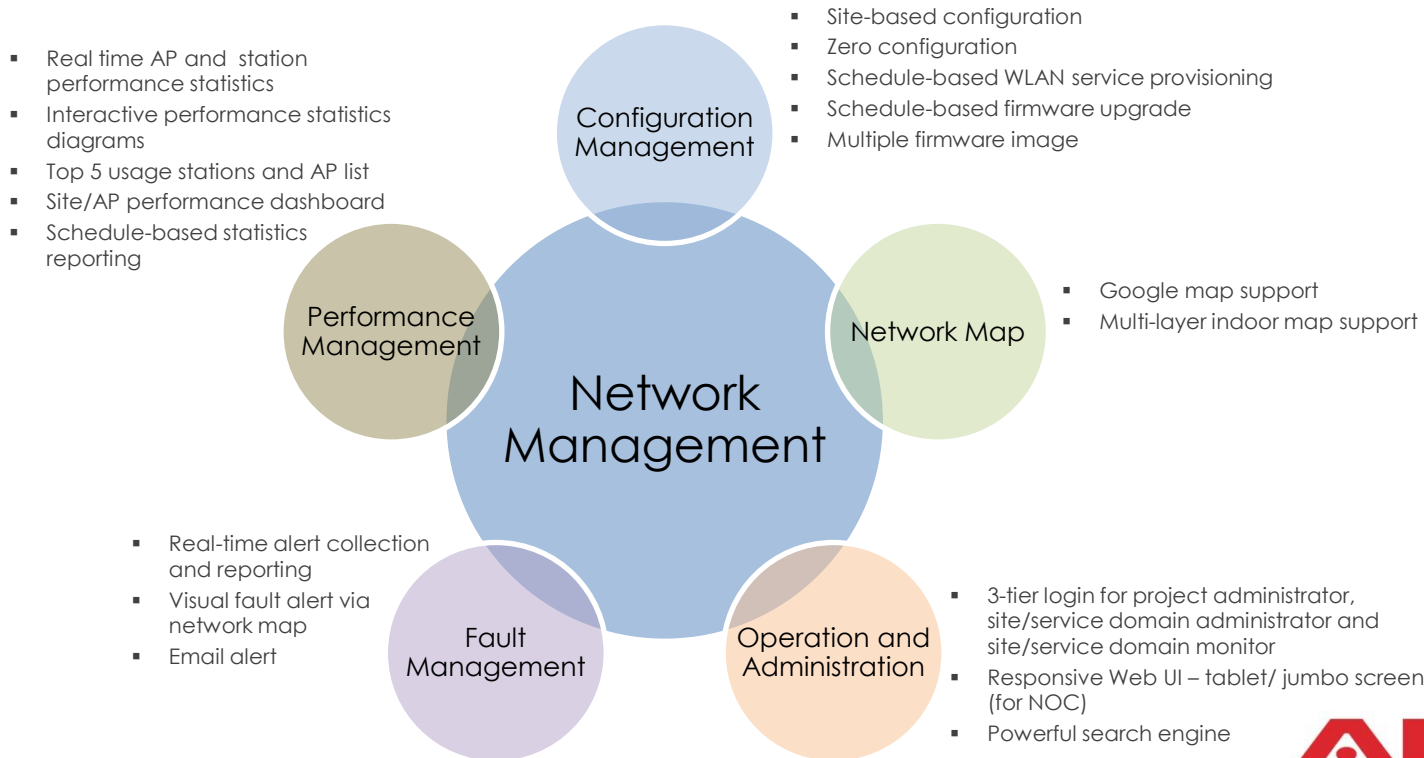
Item	Topic	Duration	Presented By	Participants	Prerequisite	Preparation Required
7	<b>Verification</b>	3 hr	TPS, Altai	Engineers	Basic networking and WiFi knowledge required	1 pcs of AP, AltaiCare account, Internet access for demo if needed
7.1	<a href="#">Verification: Custom Template Portal</a>				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

## AltaiCare Overview

# Wireless Network Management Feature Highlights

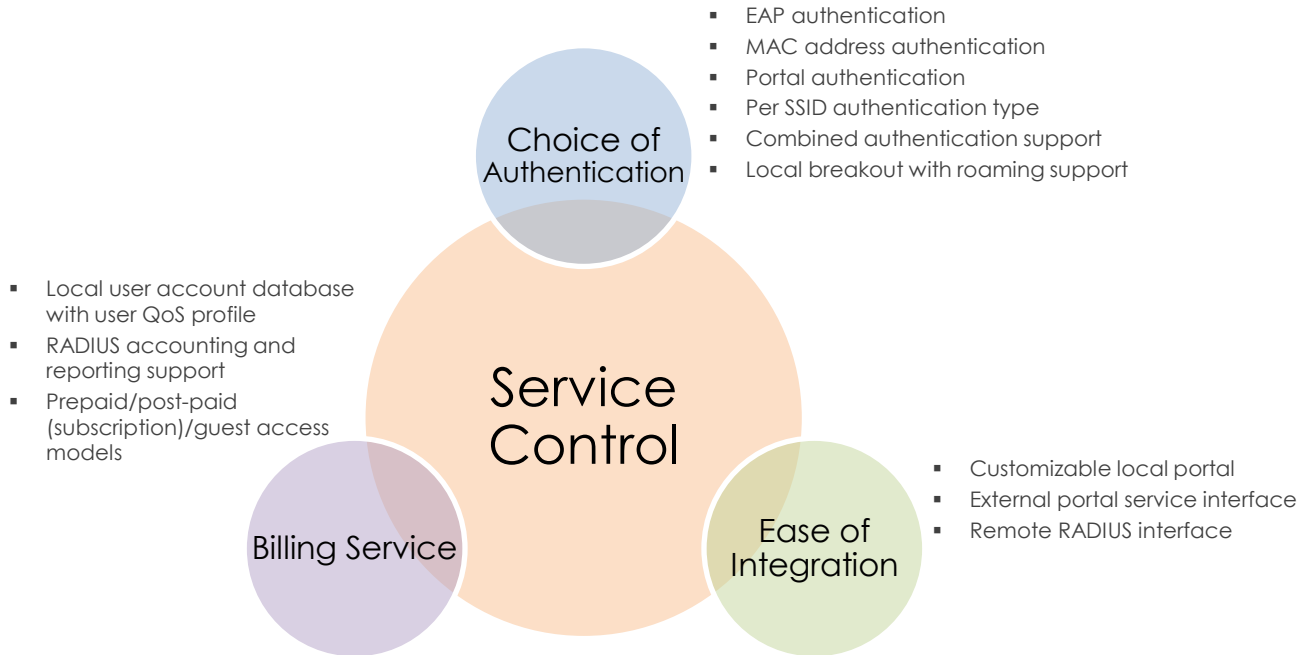
AltaiCare is a cloud-based wireless network management and service control system. The goal is to help end users deploy their WiFi service as easy as possible, using this All-in-One system.

## Wireless Network Management Feature Highlights:



# Service Control Feature Highlights

## Service Control Feature Highlights:



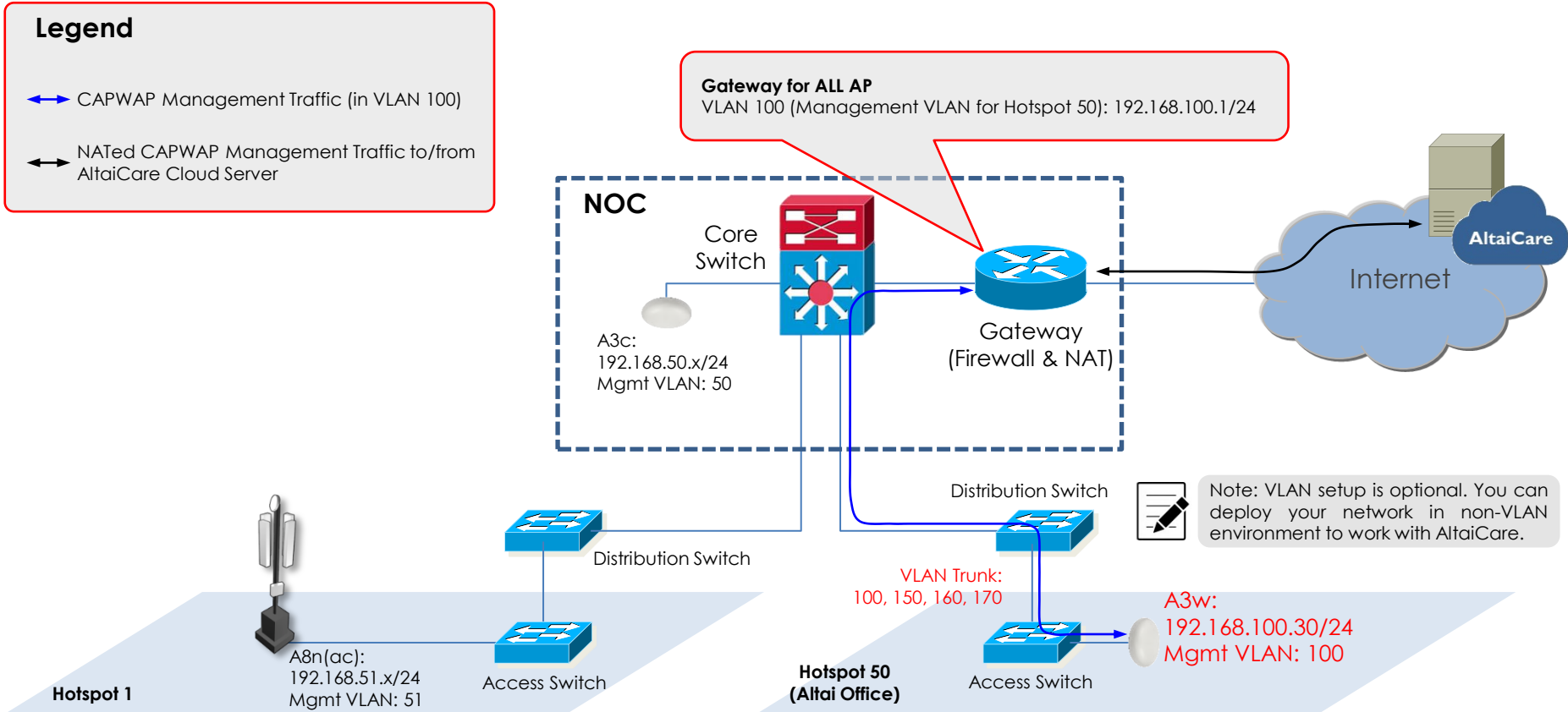
## Case Study

# Typical Network Topology and Management Traffic

## Legend

↔ CAPWAP Management Traffic (in VLAN 100)

↔ NATed CAPWAP Management Traffic to/from AltaiCare Cloud Server



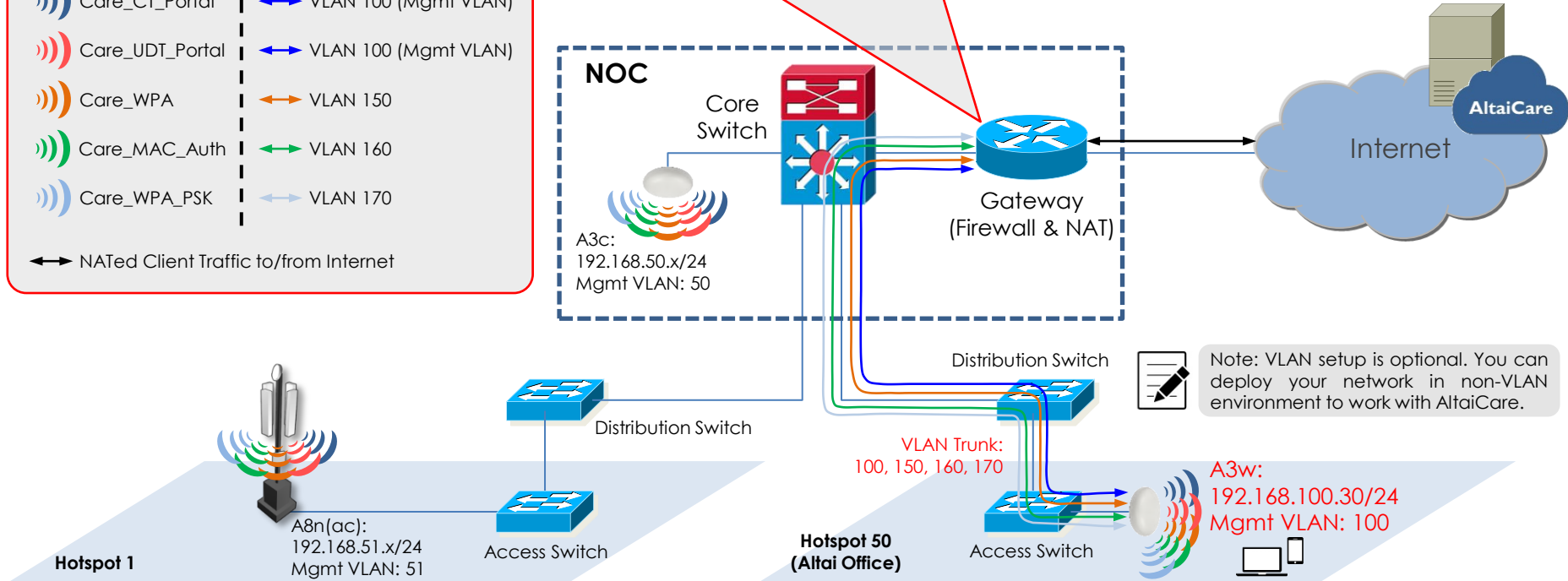
# Typical Network Topology and Client Traffic

## Legend

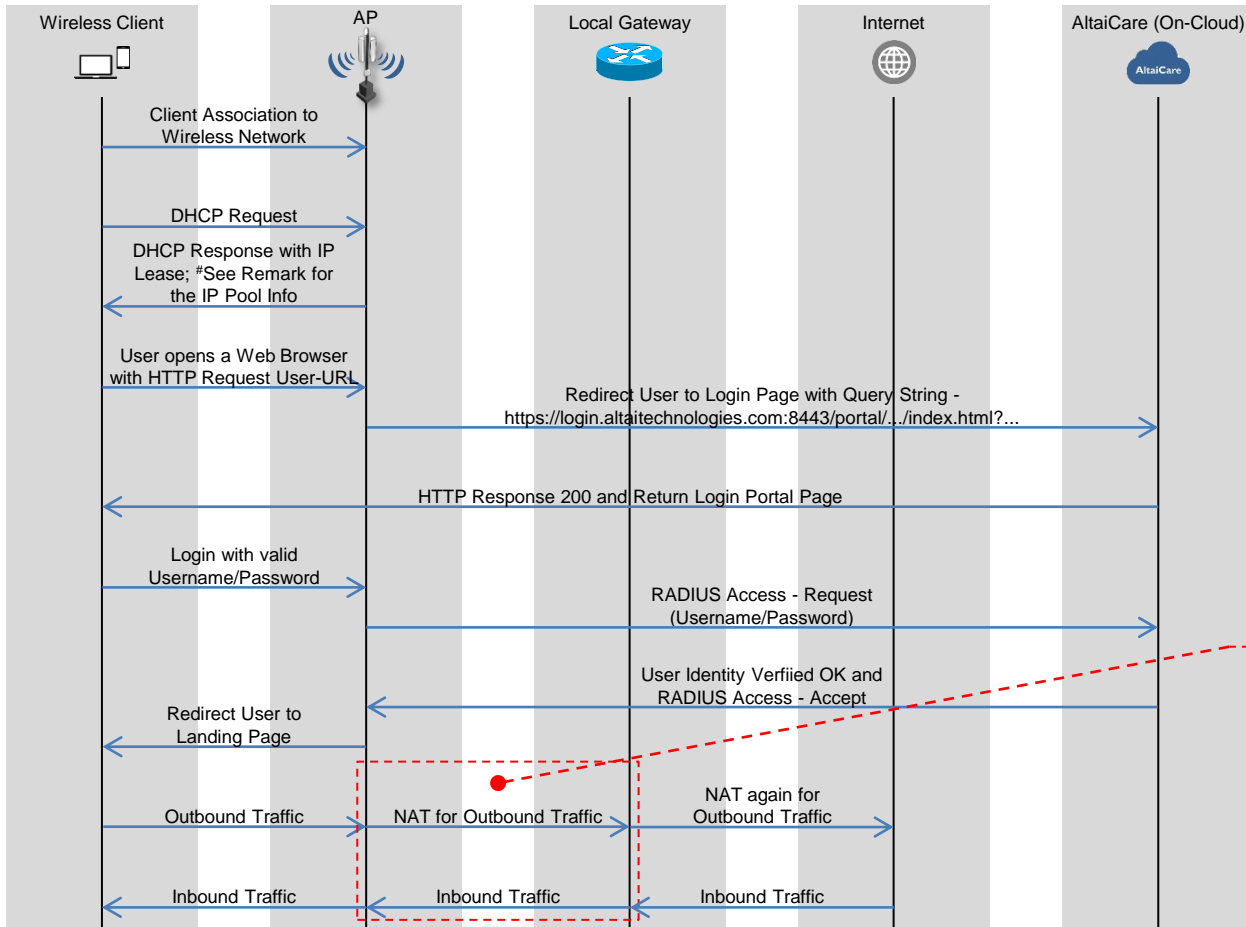
WiFi	Ethernet
))) Care_CT_Portal	← VLAN 100 (Mgmt VLAN)
))) Care_UDT_Portal	← VLAN 100 (Mgmt VLAN)
))) Care_WPA	← VLAN 150
))) Care_MAC_Auth	← VLAN 160
))) Care_WPA_PSK	← VLAN 170
↔ NATed Client Traffic to/from Internet	

### Gateway for ALL AP and wireless clients

VLAN 100 (Management VLAN for Hotspot 50): 192.168.100.1/24  
 VLAN 150: 192.168.150.1/24 with DHCP Server for WPA clients  
 VLAN 160: 192.168.160.1/24 with DHCP Server for MAC-Auth clients  
 VLAN 170: 192.168.170.1/24 with DHCP Server for WPA-PSK clients



# Call Flow for Built-In Portal Auth



## Remark:



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

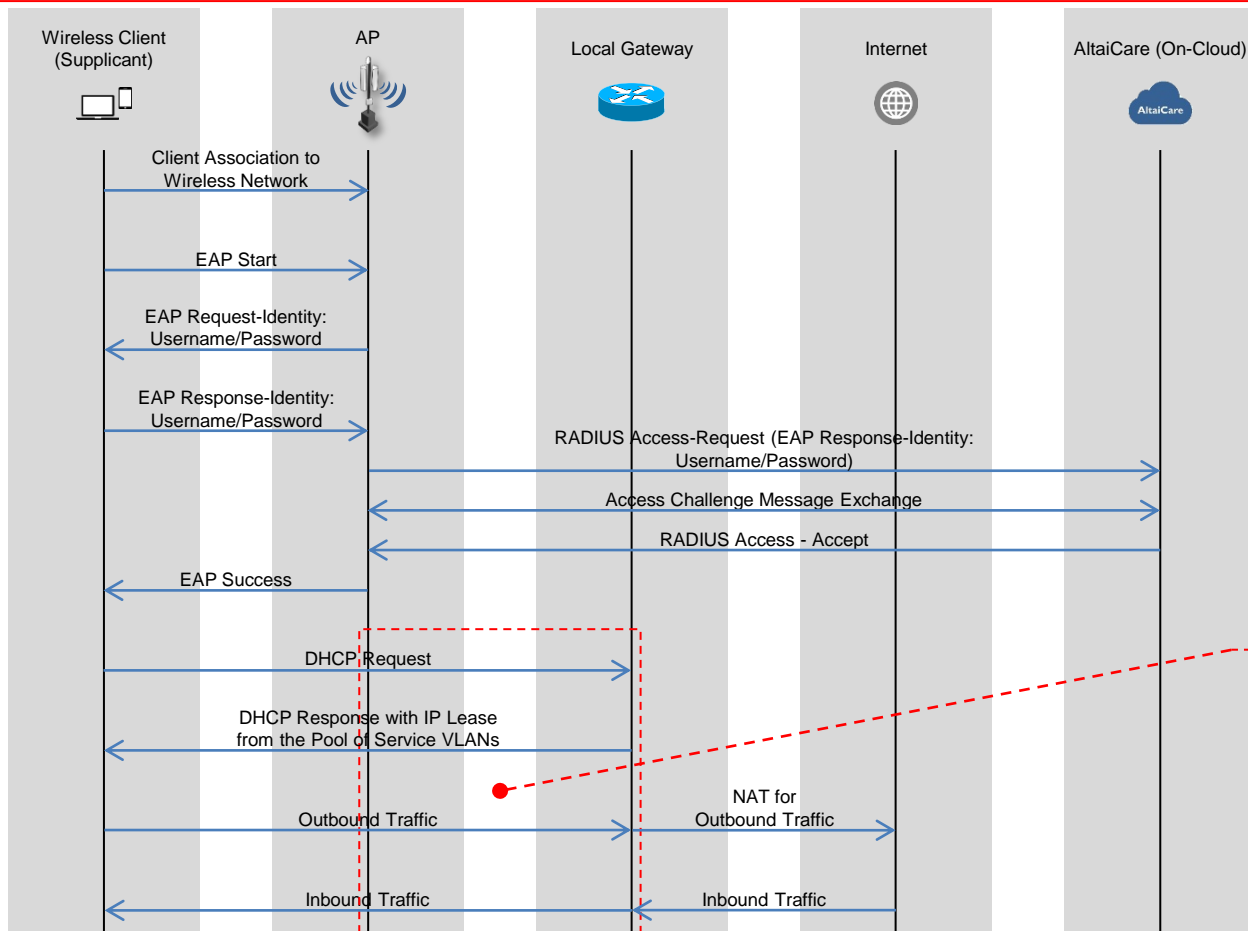


AltaiCare as RADIUS server and web portal hosting server

# 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

# Call Flow for Built-In RADIUS Auth (WPA)



## Remark:



AP as RADIUS client & authenticator



AltaiCare as RADIUS server



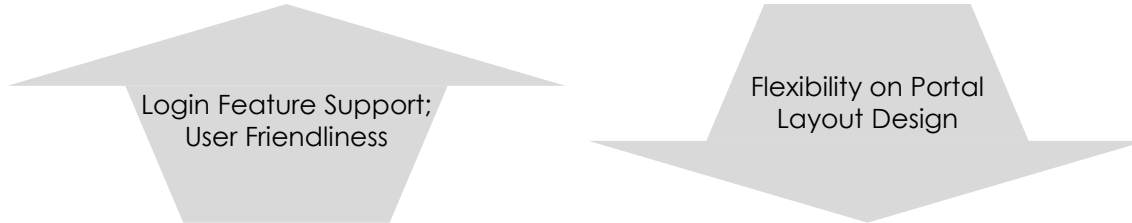
Local Gateway as DHCP server for wireless clients and NAT implementation on their traffic

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

# 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)



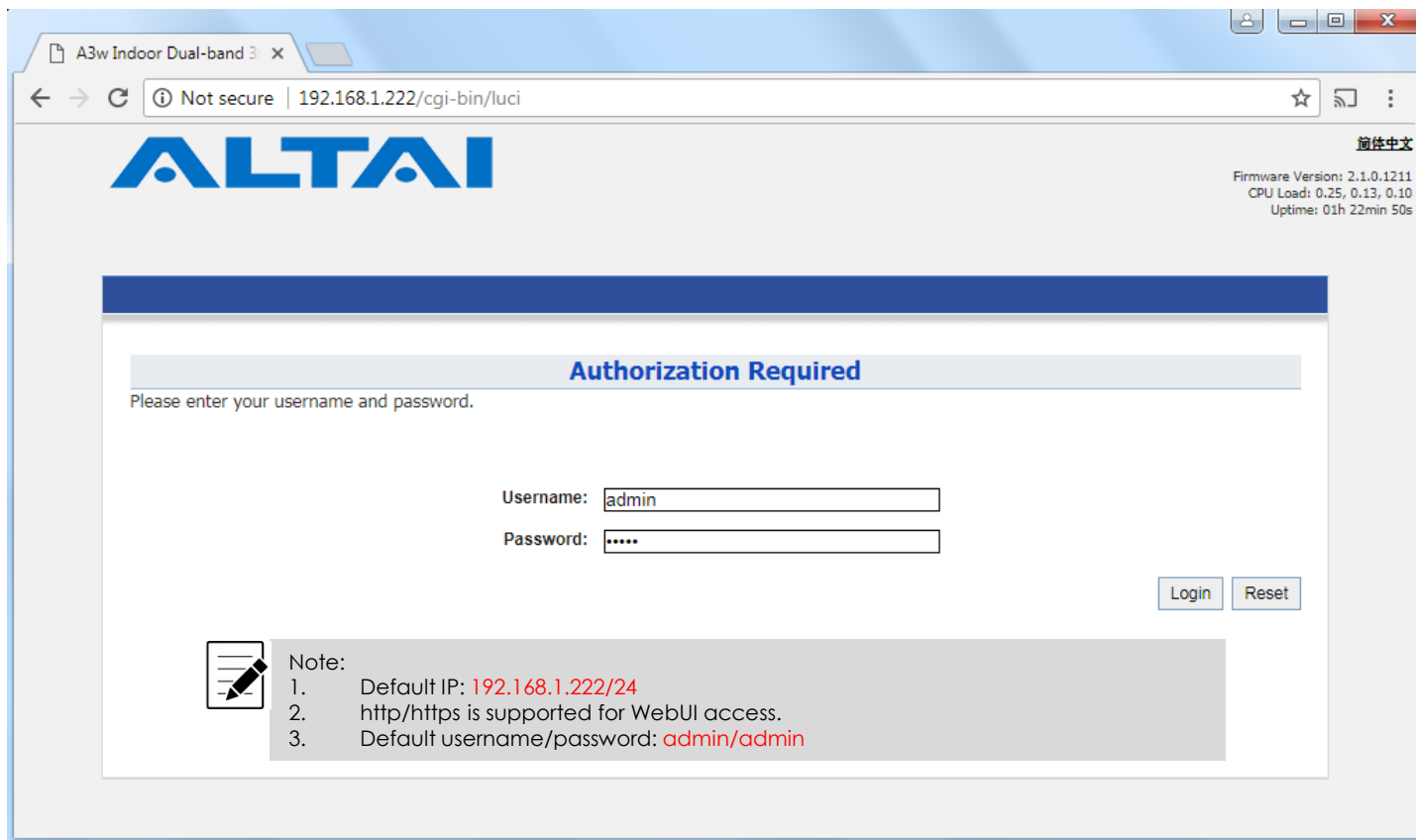
### 3. Package Upload (Built-In/External)

- 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)						✓

## Before You Begin - AP Configuration

# Access to AP WebUI



# Step 1: Network Setting

The screenshot shows the configuration interface for a device. The top navigation bar includes 'Status', 'Configuration', 'Administration', 'Tools', and 'About'. The 'Configuration' tab is active, and the 'Network' sub-tab is selected. The 'General Network Setting' page is displayed, with the following sections:

- Network Setting:** Network Setting: Switch Mode (dropdown), Enable IPv6:
- WAN Setting (IPv4):** Internet Connection Type: Static (dropdown), IPv4 Address: 192.168.100.30, IPv4 Subnet Mask: 255.255.255.0, IPv4 Default Gateway: 192.168.100.1, IPv4 DNS Server IP Address: 10.6.127.4 and 8.8.8.8
- WAN Setting (IPv6):** Internet Connection Type: Static (dropdown)
- STP Setting:** Enable STP Mode:
- WAN/LAN Interface Assignment:** Enable NAT Mode: NA, Submit button
- LAN Setting (IPv4):** LAN IP Address: NA, LAN IP Address Mask: NA
- Ethernet Setting:** Table with columns Mode and Speed.

	Mode	Speed
eth0	Auto Detect	100Mbps/Full
eth1	Auto Detect	100Mbps/Full

Red annotations: A red circle with '1' highlights the 'Network Setting' dropdown. A red circle with '2' highlights the 'WAN Setting (IPv4)' section. A red circle with '3' highlights the 'Submit' button.

## 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.altaittechnologies.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

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

The screenshot shows the 'VLAN Configuration' page. At the top, the 'Configuration' tab is selected. Below it, the 'VLAN' sub-tab is active. A red circle with the number '1' highlights the 'Enable VLAN:

The 'VLAN Profiles' section contains a table with the following data:

VLAN ID	Interfaces	IPv4 Address/Subnet Mask	Management VLAN
1	eth0 eth1 AP0_0(Superwifi Network 0) AP1_0(Superwifi Network 0)	192.168.1.222 / 255.255.255.0	<input checked="" type="radio"/>

A red circle with the number '3' highlights the 'Add VLAN...' button. Below the table is the 'Interfaces' section with a table:

Interface	Type	PVID	Default VLAN Tagging	VLAN(s)	Edit
eth0	Trunk	1	<input type="checkbox"/>	all	Edit
eth1	Access	NA	NA	1	Edit
AP0_0(Superwifi Network 0)	Access	NA	NA	1	Edit
AP1_0(Superwifi Network 0)	Access	NA	NA	1	Edit

A red circle with the number '2' highlights the 'Submit' button. Below the interfaces is the 'Create VLAN' section:

4. VLAN ID:  (1-4094)  
IPv4 Address:  .  .  .   
IPv4 Subnet Mask:  .  .  .

5.

### 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.

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

The screenshot shows the configuration interface for VLANs. The top navigation bar includes Status, Configuration, Administration, Tools, and About. The main menu has System, Network, Wireless, and Remote Mgmt. The current page is VLAN Configuration, with sub-menus for General, VLAN, DHCP, Port Forward, and Safe Mode. The 'Enable VLAN' checkbox is checked.

**VLAN Profiles**

VLAN ID	Interfaces	IPv4 Address/Subnet Mask	Management VLAN
1	eth0 eth1 AP0_0(Superwifi Network 0) AP1_0(Superwifi Network 0)	0.0.0.0 / 255.255.255.0	<input type="radio"/>
100	eth0	192.168.100.30 / 255.255.255.0	<input checked="" type="radio"/>

**Interfaces**

Interface	Type	PVID	Default VLAN Tagging	VLAN(s)	Edit
eth0	Trunk	1	<input type="checkbox"/>	all	<a href="#">Edit</a>
eth1	Access	NA	NA	1	<a href="#">Edit</a>
AP0_0(Superwifi Network 0)	Access	NA	NA	1	<a href="#">Edit</a>
AP1_0(Superwifi Network 0)	Access	NA	NA	1	<a href="#">Edit</a>

Red circles with numbers 6, 7, and 8 are overlaid on the interface. Circle 6 is on the Management VLAN column of the VLAN Profiles table. Circle 7 is on the Type column of the Interfaces table. Circle 8 is on the Submit button.

### Procedures:

- Click "Management VLAN" button on the newly created VLAN entry, i.e. VLAN 100, in the VLAN Profile list
- 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"
- 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

The screenshot shows the 'Remote Management' configuration page in the AltaiCare web interface. The page is titled 'Remote Management' and contains the following configuration options:

- 1** Enable Remote Management:
- 2** Management Type:
- Connection Type:
- 3** Radio0(2.4G):
- Radio1(5G):
- 4** Submit

### 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.altaiterhnologies.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

---

[简体中文](#) | [Reboot AP](#) | [Logout](#)

Firmware Version: 2.1.0.1211

CPU Load: 0.48, 0.16, 0.04

Uptime: 18h 20min 40s

[Unsaved Changes: 13](#) | [Save & Apply](#)

[Download Logs](#)



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



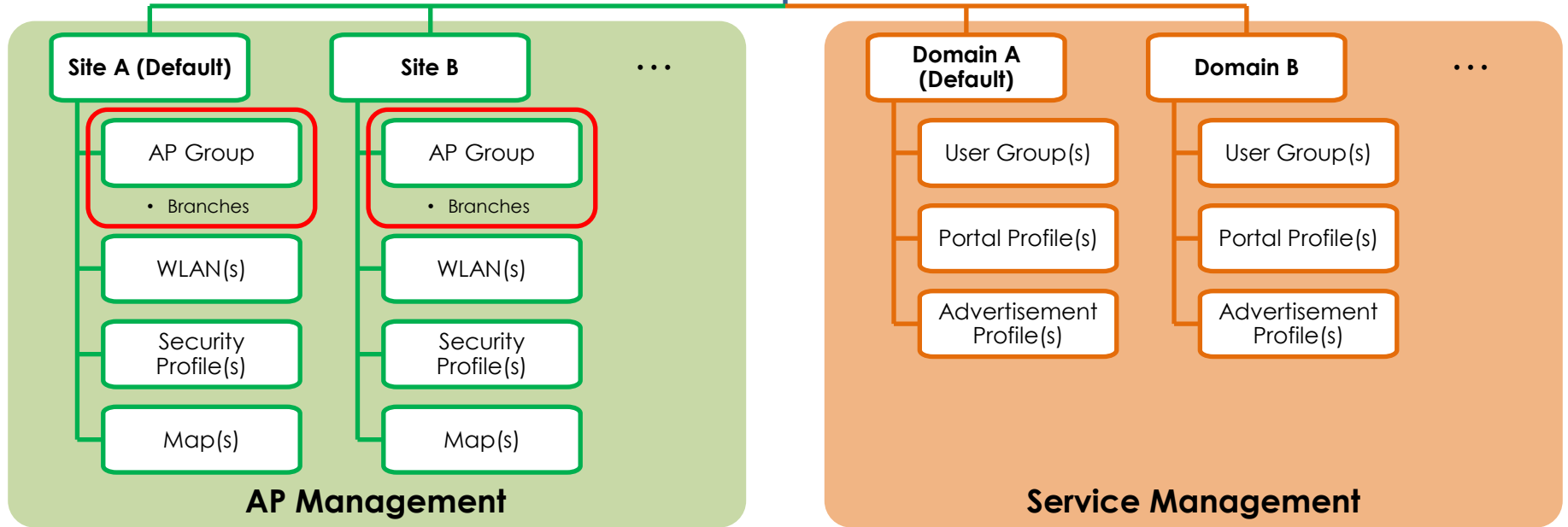
## Getting Started

# 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.

Project



## 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

## Project Admin

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



## Site Admin

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

## Site Monitor

- Monitor site status and site statistics

## Domain Admin

- 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

## Domain Monitor

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

# 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 ( $100 / (2 \times 8 + 2 \times 2) = 5$  days)

**Scenario 4:** 5 x A2c and 10 x C1n for 5 days ( $100 / (5 \times 2 + 10 \times 1) = 5$  days)

**Scenario 5:** 1 x A3Ei and 5 x A3c for 2 days ( $100 / (1 \times 8 + 5 \times 6) = 2$  days with 24 credits left).

In Scenario 5, the remaining 24 credits will not be processed for the 3<sup>rd</sup> 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](#).

# Access to AltaiCare

The screenshot shows a web browser window titled "AltaiCare Admin Console" with the URL "https://care.altatechnologies.com/login". The page features the AltaiCare logo at the top center. Below the logo is a sign-in form titled "ACCOUNT SIGN IN" with fields for "USER NAME" and "PASSWORD", and a "SIGN IN" button. Three numbered callouts provide instructions: 1. Enter "care.altatechnologies.com" in the address bar. 2. Enter the project account credentials. 3. Click the SIGN IN button.



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

# AltaiCare Web Interface

Management Tabs

Current Directory

Search Engine

Function Buttons

AltaiCare

WIRELESS SERVICE PROJECT

[altaitps] [refresh] [full screen]

Altai Office > Dashboard

DEFAULT SEARCH

Site [Altai Office] Dashboard

ACCESS POINT (1/1)	STATIONS : 1	TODAY TRAFFIC (UL / DL)	TOTAL THROUGHPUT (UL / DL)
29% / -96 dBm 2.4G 0% / -103 dBm 5G	49 AVG SNR(dB) -47 AVG RSSI(dBm)	1.24 GB/2.72 GB 2.4G 0 MB/0 MB 5G	0.00 Mbps/0.00 Mbps 2.4G 0 Mbps/0 Mbps 5G

TRAFFIC THROUGHPUT TODAY TOP USAGE TODAY BOTTOM USAGE

TRAFFIC

Traffic (MB) / 1 Minute

Upload Download

Traffic Last 24 Hours

23Jul 12:03 23Jul 12:58 23Jul 13:53 23Jul 14:48 23Jul 15:43 23Jul 16:36

MAP

Map Satellite

Map

Science Park W Ave

Science Park E Ave

YuuZoo Corporation

Green 18 綠園樓

Pak Shek Kok Promenade 白石角海濱長廊

Harbour View 1 Podium 海濱大樓一區平台

Lakeside 2 濱湖樓

Charles K. Kao Auditorium 高錕會議中心

Lakeside 1 Podium 濱湖樓平台

Enterprise Place 企業廣場

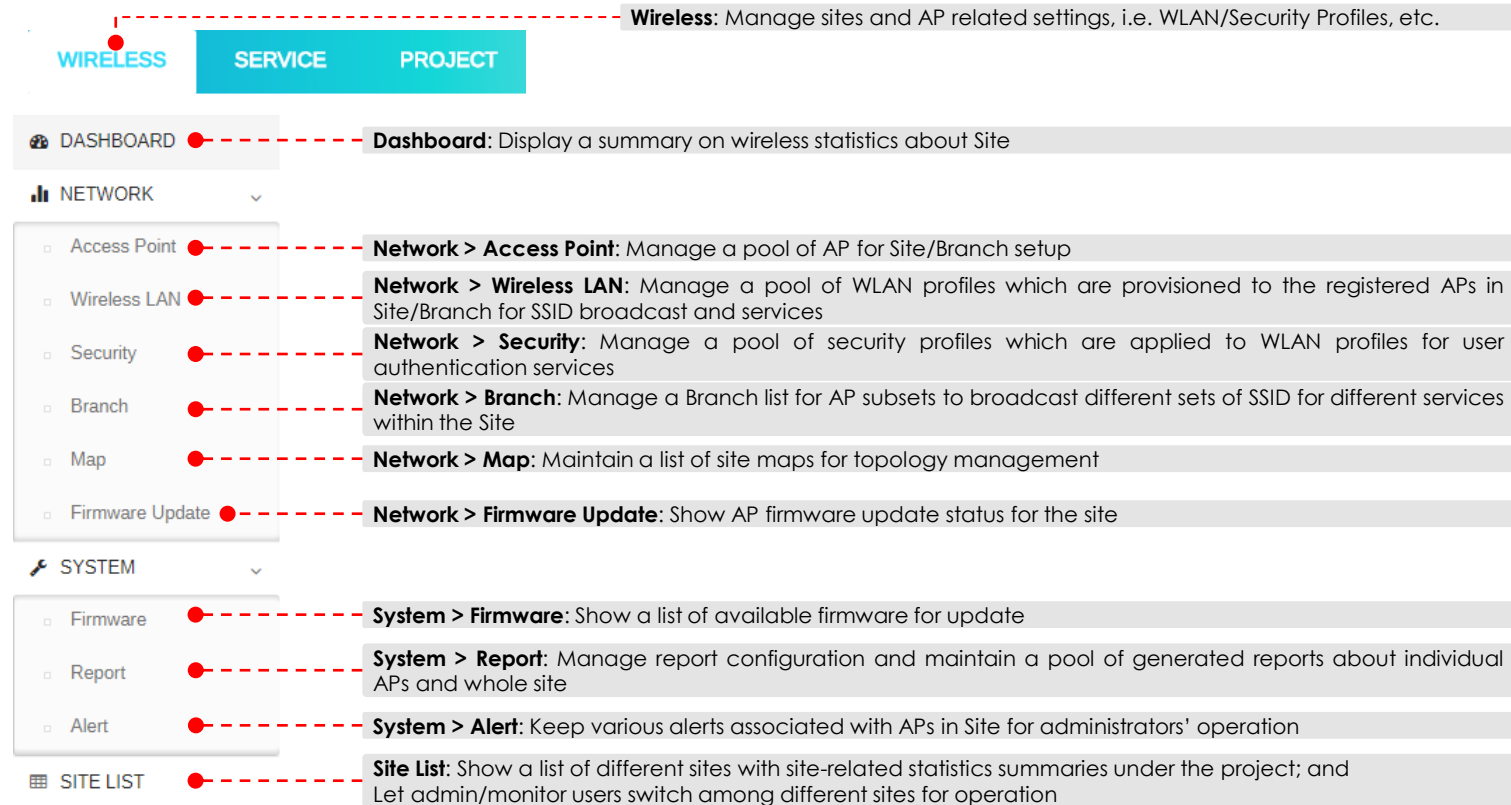
Biotech Centre 2 生物科技中心二區

ClubONE 會所一號 科學園

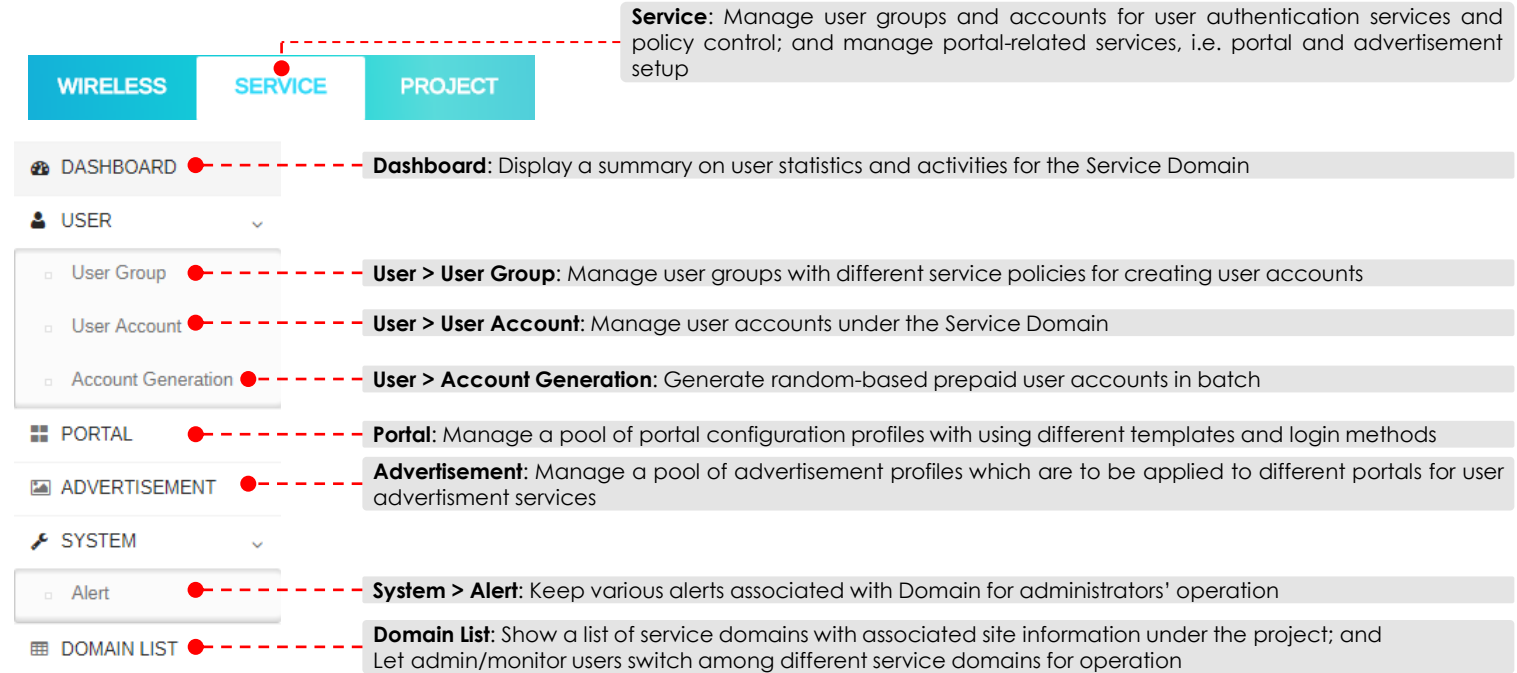
Tesla Supercharger 超級充電站

創新路

# Wireless Management Overview

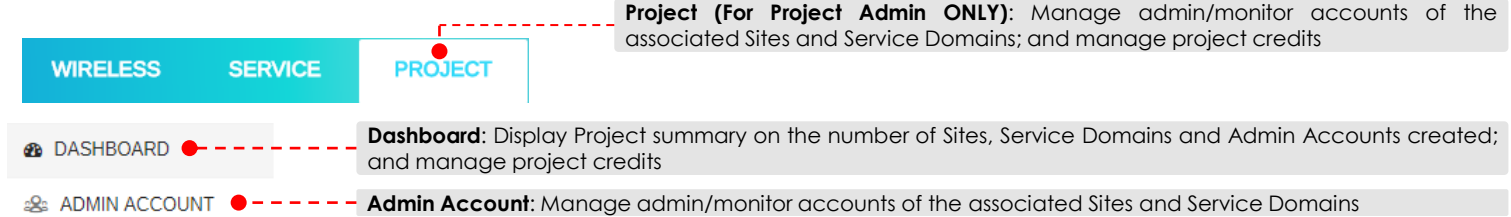


# Service Management Overview



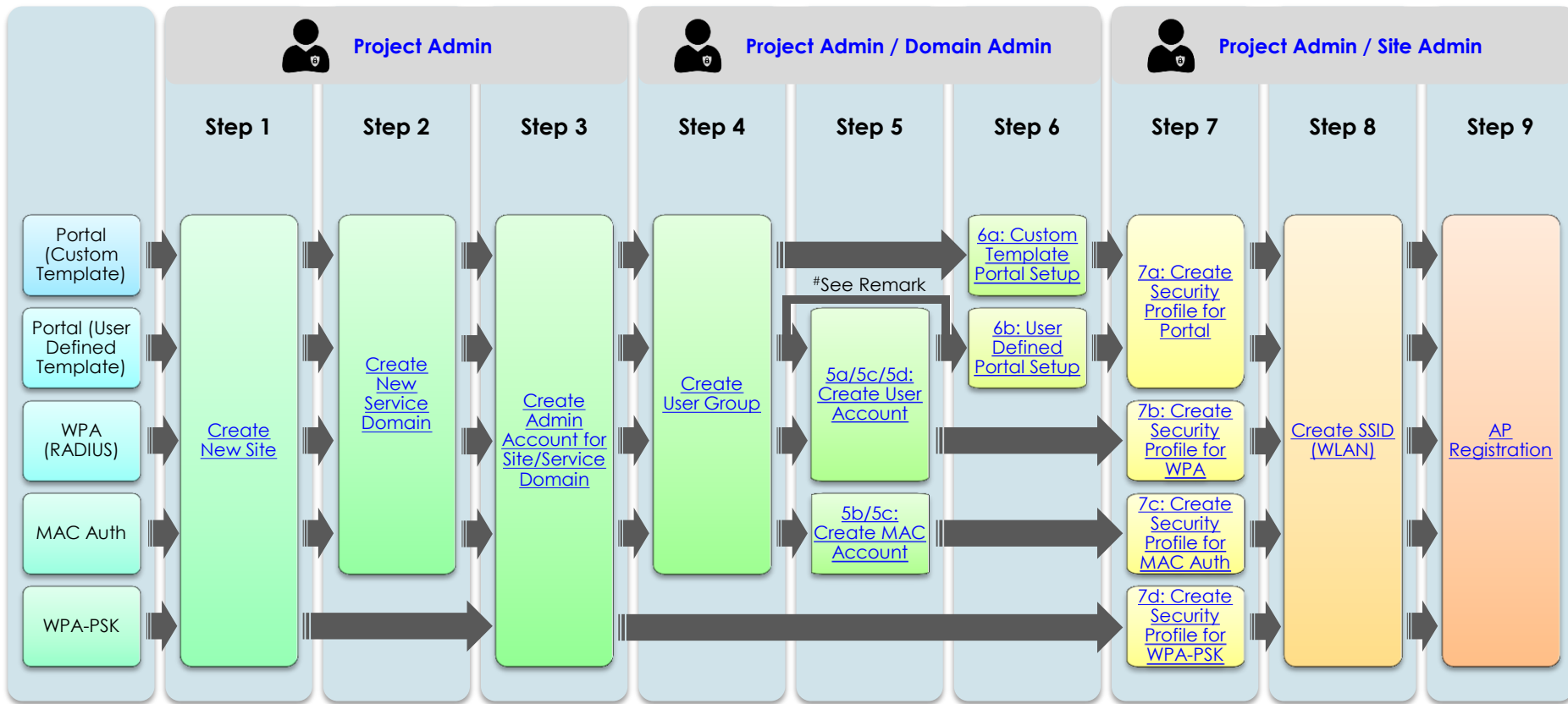
# Project Management Overview

---



## Basic Configuration

# Configuration Procedures



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

## Step 1: Create New Site

# Step 1: Create New Site – Basic Setting

WIRELESS SERVICE PROJECT

Default Site > Site List

SITE SEARCH

### Site List

NAME ^	AP(ONLINE / OFFLINE)	TOTAL TRAFFIC	THROUGHPUT(2.4G / 5G)	STATION	AVG SNR/RSSI	ALERT
<a href="#">Default Site</a>	0 [0/0]	2.4G: 0 MB 5G: 0 MB	Total: 0 Mbps / 0 Mbps Avg: 0 Mbps / 0 Mbps	0	0dB / 0dBm	0

Showing 1-1 of 1 entries 10 >

### NEW SITE

2 NAME:

3 TIME ZONE:

4 DAYLIGHT SAVING:

5


#### 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  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.

# Step 1: Create New Site - Default Radio Setting

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

## Site List

NAME ^	AP(OFFLINE / OFFLINE)	TOTAL TRAFFIC	THROUGHPUT(2.4G / 5G)	STATION	AVG SNR/RSSI	ALERT	
<a href="#">Altai Office</a>	0 [0/0]	2.4G: 0 MB 5G: 0 MB	Total: 0 Mbps / 0 Mbps Avg: 0 Mbps / 0 Mbps	0	0dB / 0dBm	0	  
<a href="#">Default Site</a>	0 [0/0]	2.4G: 0 MB 5G: 0 MB	Total: 0 Mbps / 0 Mbps Avg: 0 Mbps / 0 Mbps	0	0dB / 0dBm	0	  

Showing 1-2 of 2 entries 10 ▾

< 1 >

# 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.

DEFAULT RADIO SETTING

SITE NAME: Altai Office

COUNTRY CODE: HONG KONG

WIRELESS MODE: Auto

TX POWER: Max

CHANNEL: Auto

AUTO CHANNEL SELECTION INTERVAL (Mins): 60

**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:** 1/2 of 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

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

**DEFAULT RADIO SETTING**

SITE NAME:	<input type="text" value="Altai Office"/>
COUNTRY CODE:	<input type="text" value="HONG KONG"/>
WIRELESS MODE:	<input type="text" value="Auto"/>
TX POWER:	<input type="text" value="Max"/>
CHANNEL:	<input type="text" value="Auto"/>
AUTO CHANNEL SELECTION INTERVAL (Mins):	<input type="text" value="60"/>

**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.



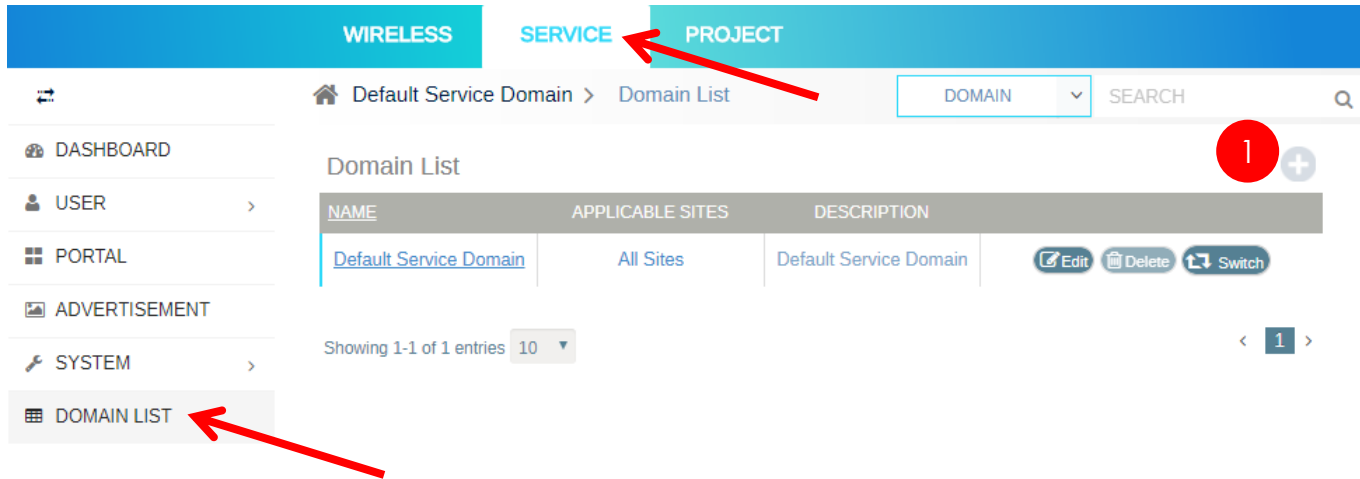
Note: Remember to click **SAVE** button at the page bottom to make all changes take effect.

## Step 2: Create New Service Domain

## Step 2: Create New Service Domain – Basic Setup

### Procedures:

1. Click  to create a new service domain



The screenshot displays the Altai Super WiFi management interface. The top navigation bar includes tabs for WIRELESS, SERVICE, and PROJECT. The SERVICE tab is selected, and the breadcrumb path is Default Service Domain > Domain List. A search bar is present with a dropdown menu set to DOMAIN and a search icon. The left sidebar contains a menu with items: DASHBOARD, USER, PORTAL, ADVERTISEMENT, SYSTEM, and DOMAIN LIST. The DOMAIN LIST item is highlighted, and a red arrow points to it. The main content area shows a table titled 'Domain List' with columns: NAME, APPLICABLE SITES, and DESCRIPTION. The table contains one entry: 'Default Service Domain' with 'All Sites' as applicable sites and 'Default Service Domain' as the description. Action buttons for Edit, Delete, and Switch are visible for this entry. A red circle with the number '1' and a plus sign icon is overlaid on the table header, with a red arrow pointing to it. The table footer indicates 'Showing 1-1 of 1 entries' and a page number '1'.

NAME	APPLICABLE SITES	DESCRIPTION
<a href="#">Default Service Domain</a>	All Sites	Default Service Domain

## 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.

The screenshot shows a 'NEW DOMAIN' configuration window with the following fields and callouts:

- 2** NAME: Altai WiFi Service
- 3** APPLICABLE SITES: Custom Mode (dropdown), Altai Office (selected site)
- 4** TIME ZONE: UTC+08:00 (dropdown)
- 5** DAYLIGHT SAVING: 00:00 (dropdown)
- 6** DESCRIPTION: For Altai WiFi Service
- 7** CREATE and CANCEL buttons




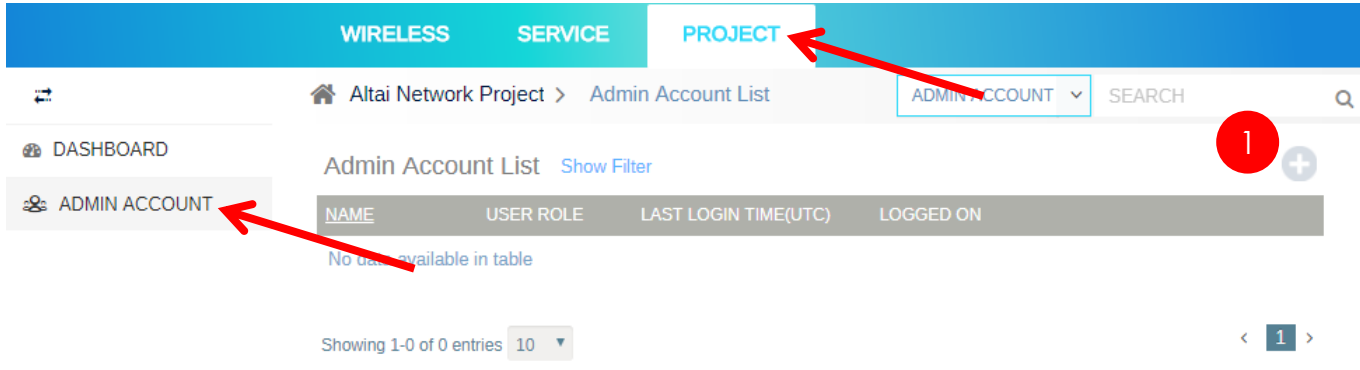
Note: Remember to click **SAVE** button at the page bottom to make all changes take effect.

### 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 account



WIRELESS SERVICE **PROJECT**

Altai Network Project > Admin Account List ADMIN ACCOUNT SEARCH

DASHBOARD

ADMIN ACCOUNT

Admin Account List [Show Filter](#)

NAME	USER ROLE	LAST LOGIN TIME(UTC)	LOGGED ON
No data available in table			

Showing 1-0 of 0 entries 10 < 1 >

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

### NEW ACCOUNT

2 USERNAME: tpsadmin

3 PASSWORD: .....

4 CONFIRM PASSWORD: .....

5 SITE ROLE: Site Admin

6 SITES: Altai Office X

7a DOMAIN ROLE: Derive From Site Role Setting

9 EMAIL ADDRESS: support@altaitechnologies.com

10 CREATE CANCEL

OR

7b DOMAIN ROLE: Domain Admin

8 SERVICES DOMAINS: Altai WiFi Service X  
Altai WiFi Service 2 X

This Service Domain is mapped and applied to the Site "Altai Office" ONLY

This one is applied to ALL sites

### 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.

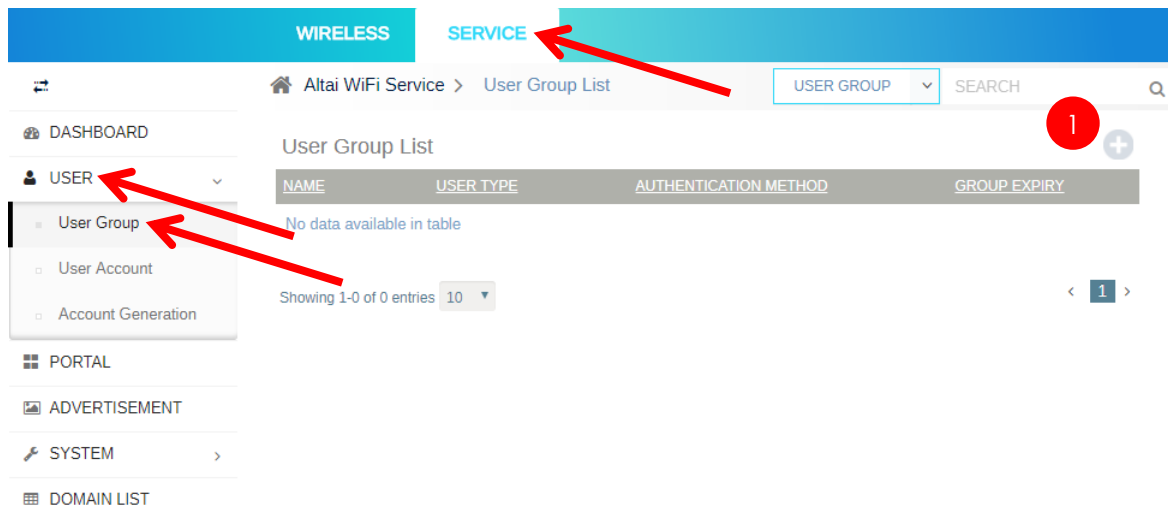
8. Select the existing service domains to be managed for the account. The pool contains the service domains which are applicable to the sites selected in item #6 and those which apply to ALL sites.
9. Enter the user's email address of account registration.
10. Click **CREATE** button to open and confirm the account.

## Step 4: Create User Group

## Step 4: Create User Group

### Procedures:

1. Click  to create a new User Group



The screenshot shows the 'User Group List' page in the Altai WiFi Service interface. The page has a blue header with 'WIRELESS' and 'SERVICE' tabs. The 'SERVICE' tab is selected and highlighted with a red arrow. Below the header, the breadcrumb path is 'Altai WiFi Service > User Group List'. There is a search bar with a dropdown menu set to 'USER GROUP' and a search icon. A red circle with the number '1' is placed over a plus icon in the top right corner of the main content area. On the left side, there is a navigation menu with 'USER' selected and highlighted with a red arrow. Under 'USER', 'User Group' is also highlighted with a red arrow. The main content area shows a table titled 'User Group List' with columns: NAME, USER TYPE, AUTHENTICATION METHOD, and GROUP EXPIRY. The table is empty, displaying 'No data available in table'. Below the table, it says 'Showing 1-0 of 0 entries' and '10' with a dropdown arrow. On the right side of the table, there are navigation arrows and a page number '1'.

## 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.

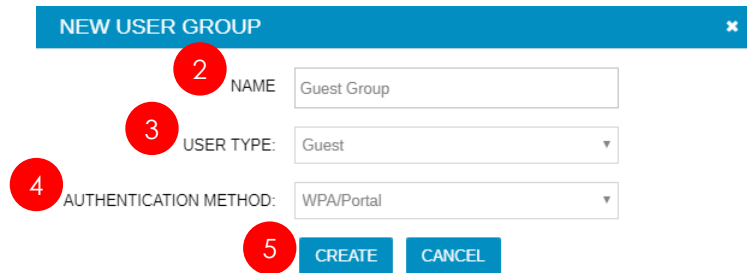
4. Choose one of the following Authentication Method which is to define user account type for different authentication purposes:

**(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.



The screenshot shows a web form titled "NEW USER GROUP" with a close button (X) in the top right corner. The form contains three input fields and two buttons. Red circles with numbers 2, 3, 4, and 5 are overlaid on the form to indicate the steps:

- 2: Points to the "NAME" input field containing "Guest Group".
- 3: Points to the "USER TYPE" dropdown menu, which is currently set to "Guest".
- 4: Points to the "AUTHENTICATION METHOD" dropdown menu, which is currently set to "WPA/Portal".
- 5: Points to the "CREATE" button.











The "CANCEL" button is also visible to the right of the "CREATE" button.

## 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

### User Group List

NAME ^	USER TYPE	AUTHENTICATION METHOD	GROUP EXPIRY	
<a href="#">Guest Group</a>	Guest	WPA/Portal	No Limit	 
<a href="#">PP MAC Group</a>	Prepaid	MAC	No Limit	 
<a href="#">PP User Group</a>	Prepaid	WPA/Portal	No Limit	 
<a href="#">SC MAC Group</a>	Subscription	MAC	No Limit	 
<a href="#">SC User Group</a>	Subscription	WPA/Portal	No Limit	 

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

## Step 4: Create User Group – Group Setting

SETTING

AUTHENTICATION METHOD: WPA/Portal

GROUP EXPIRY: No Limit

AUTO REMOVE EXPIRED USER:

AFTER(Day(s)): 1

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.

ACCOUNT DEFAULT	
VALIDITY:	Custom Mode  <input type="text" value="2"/> Hour(s)
DATA QUOTA (MB):	Custom Mode  <input type="text" value="500"/>
BANDWIDTH UPLOAD LIMIT (Kbps):	Custom Mode  <input type="text" value="10000"/>
BANDWIDTH DOWNLOAD LIMIT (Kbps):	Custom Mode  <input type="text" value="10000"/>
SESSION TIMEOUT (Mins):	<input type="text" value="120"/>
IDLE TIMEOUT (Mins):	<input type="text" value="15"/>
MAX CONCURRENT USER NUMBER:	Custom Mode  <input type="text" value="1"/>

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”.

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

ACCOUNT DEFAULT	
RECURRENT DATA QUOTA PERIOD:	Monthly
RECURRENT DATA QUOTA (MB):	Custom Mode 5000
BANDWIDTH UPLOAD LIMIT (Kbps):	Custom Mode 10000
BANDWIDTH DOWNLOAD LIMIT (Kbps):	Custom Mode 10000
SESSION TIMEOUT (Mins):	120
IDLE TIMEOUT (Mins):	15
MAX CONCURRENT USER NUMBER:	No Limit

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.

## Step 4: Create User Group – Account Registration Configuration

ACCOUNT REGISTRATION CONFIGURATION

UNIQUE ITEMS: EMAIL x MOBILE x PHONE x  
SOCIALACCOUNT x

USER RENOVATE ENABLE:

RENOVATE PERIOD: 1 Day(s)

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


## Step 5: Create User Account

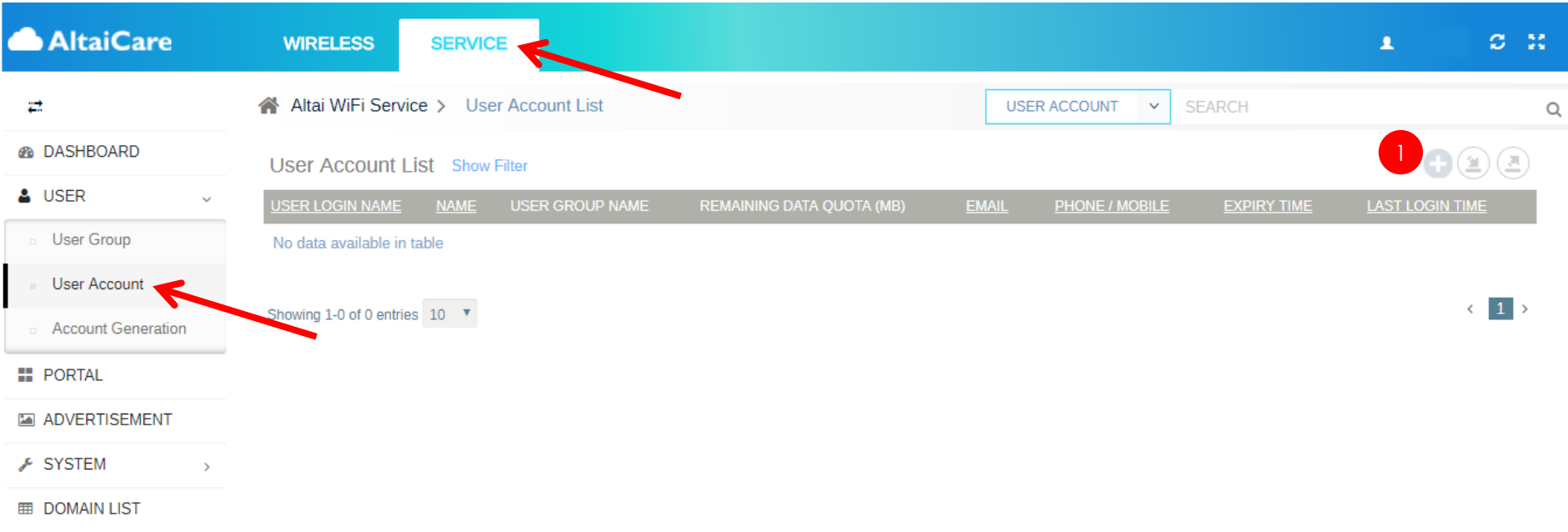
We provide the following three ways of user account generation.

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

# 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](#).



The screenshot displays the AltaiCare management interface. The top navigation bar includes 'AltaiCare', 'WIRELESS', and 'SERVICE' (highlighted with a red arrow). Below the navigation bar, the breadcrumb path is 'Altai WiFi Service > User Account List'. A search bar contains 'USER ACCOUNT' and a search icon. The main content area shows the 'User Account List' page with a table header and a message 'No data available in table'. The table header includes columns: USER LOGIN NAME, NAME, USER GROUP NAME, REMAINING DATA QUOTA (MB), EMAIL, PHONE / MOBILE, EXPIRY TIME, and LAST LOGIN TIME. A red circle with the number '1' is placed over the '+', '-', and refresh icons in the top right of the table area. The left sidebar contains a menu with 'USER' selected, and 'User Account' highlighted with a red arrow. Other menu items include 'DASHBOARD', 'PORTAL', 'ADVERTISEMENT', 'SYSTEM', and 'DOMAIN LIST'. The bottom of the page shows 'Showing 1-0 of 0 entries' and a pagination control with '1' in a box.

## 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](#).

The screenshot shows a web form titled "NEW USER ACCOUNT" with a close button (X) in the top right corner. The form contains the following fields and controls, each with a red circle and number indicating a step:

- 2** NAME: ppuser01
- 3** USER TYPE: Prepaid (dropdown menu)
- 4** ACTIVATION STATUS:
- 5** USER GROUP: PP User Group (dropdown menu)
- 6** USER LOGIN NAME: ppuser01
- 7** USER PASSWORD: \*\*\*\*\*
- 8** DEVICE MAC:
- 9** VALIDITY: Use Group Default Setting (dropdown menu)
- 10** DATA QUOTA (MB): Use Group Default Setting (dropdown menu)
- 11** CREATE CANCEL (two buttons)

## 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](#).

The screenshot shows a web form titled "NEW USER ACCOUNT" with a close button (X) in the top right corner. The form contains the following fields and options, each with a red circular number indicating a step:

- 2** NAME: scuser01
- 3** USER TYPE: Subscription
- 4** ACTIVATION STATUS:
- 5** USER GROUP: SC User Group
- 6** ACCOUNT START TIME: 07/16/2017
- 7** USER LOGIN NAME: scuser01
- 8** USER PASSWORD: .....
- 9** DEVICE MAC:
- 10** RECURRENT DATA QUOTA (MB): Use Group Default Setting
- 11** CREATE CANCEL

## 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](#).

The screenshot shows a web form titled "NEW USER ACCOUNT" with a close button (X) in the top right corner. The form contains the following fields and controls, each with a red circular callout number:

- 2**: NAME: Input field containing "ppmac01".
- 3**: USER TYPE: Dropdown menu with "Prepaid" selected.
- 4**: ACTIVATION STATUS: Checkmark icon.
- 5**: USER GROUP: Dropdown menu with "PP MAC Group" selected.
- 6**: USER LOGIN MAC: Input field containing "44:85:00:99:23:d4".
- 7**: VALIDITY: Dropdown menu with "Use Group Default Setting" selected.
- 8**: DATA QUOTA (MB): Dropdown menu with "Use Group Default Setting" selected.
- 9**: Two buttons labeled "CREATE" and "CANCEL".

## 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](#).

The screenshot shows a web form titled "NEW USER ACCOUNT" with a close button in the top right corner. The form contains the following fields and options, each with a red circular callout number:

- 2. NAME: scmac01
- 3. USER TYPE: Subscription (dropdown menu)
- 4. ACTIVATION STATUS:
- 5. USER GROUP: SC MAC Group (dropdown menu)
- 6. ACCOUNT START TIME: 07/22/2017 (calendar icon)
- 7. USER LOGIN MAC: 9c:4e:36:8c:c9:e0
- 8. RECURRENT DATA QUOTA (MB): Use Group Default Setting (dropdown menu)
- 9. CREATE and CANCEL buttons

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

User Account List [Show Filter](#)

Batch Actions: [Remove All](#)

USER LOGIN NAME ^	NAME	USER GROUP NAME	REMAINING DATA QUOTA (MB)	EMAIL	PHONE / MOBILE	EXPIRY TIME	LAST LOGIN TIME	
<a href="#">44:85:00:99:23:d4</a>	ppmac01	PP MAC Group	500	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">9c:4e:36:8c:c9:e0</a>	scmac01	SC MAC Group	No Limit	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">ppuser01</a>	ppuser01	PP User Group	500	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">scuser01</a>	scuser01	SC User Group	No Limit	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>

Showing 1-4 of 4 entries [10](#)

< [1](#) >

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

Account Name	Username	Password	User Group	Purpose
<b>ppuser01</b>	ppuser01	ppuser01	PP User Group	Used for portal username/password login via SSID: "Care_UDT_Portal"
<b>scuser01</b>	scuser01	scuser01	SC User Group	Used for WPA authentication via SSID: "Care_WPA"
<b>ppmac01</b>	44:85:00:99:23:d4	N/A	PP MAC Group	Used for MAC authentication via SSID: "Care_MAC_Auth"
<b>scmac01</b>	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

The screenshot shows the AltaiCare SERVICE interface. The 'SERVICE' tab is selected, and the 'User Account List' is displayed. A red arrow points to the 'SERVICE' tab, and another red arrow points to the 'User Account' option in the left sidebar. A red circle with the number '1' is positioned above the 'Import Users' icon in the top right corner of the table. Below the table, an 'IMPORT USERS' modal is open, showing a 'USER LIST FILE:' field with a 'Choose File' button and a 'USERS SAMPLE' link. A red circle with the number '2' is positioned above the 'CANCEL' button in the modal.

AltaiCare WIRELESS SERVICE

Altai WiFi Service > User Account List

USER ACCOUNT SEARCH

User Account List Show Filter

Batch Actions: Remove All

USER LOGIN NAME	NAME	USER GROUP NAME	REMAINING DATA QUOTA (MB)	EMAIL	PHONE / MOBILE	EXPIRY TIME	LAST LOGIN TIME	
<a href="#">44:85:00:99:23:d4</a>	ppmac01	PP MAC Group	500	--	-- / --	No Limit	--	Dashboard Edit Delete
<a href="#">4a:36:8c:c9:e0</a>	scmac01	SC MAC Group	No Limit	--	-- / --	No Limit	--	Dashboard Edit Delete
<a href="#">ppuser01</a>	ppuser01	PP User Group	500	--	-- / --	No Limit	--	Dashboard Edit Delete
<a href="#">scuser01</a>	scuser01	SC User Group	No Limit	--	-- / --	No Limit	--	Dashboard Edit Delete

Showing 1-4 of 4 entries 10


IMPORT USERS

USER LIST FILE: Choose File No file chosen

USERS SAMPLE

IMPORT CANCEL

### Procedures:

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

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

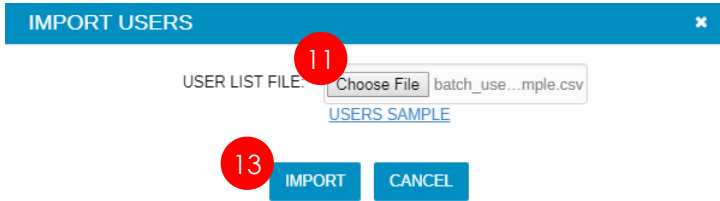
The Explorer window shows the file 'batch\_user\_sample.csv' being saved as a 'Microsoft Excel Comma Separated Values File'. The Excel window shows the file open with a table of user account data. Red circles with numbers 3 through 10 highlight specific steps in the process.

1	2	3	4	5	6
name	profile name	login name	password	data quota(in mb)	validity(in minutes)
ppuser02	PP User Group	ppuser02	ppuser02		
ppuser03	PP User Group	ppuser03	ppuser03	1000	180
scuser02	SC User Group	scuser02	scuser02		
scuser03	SC User Group	scuser03	scuser03	5000	
ppmac02	PP MAC Group	C4-85-08-90-1E-47			
scmac02	SC MAC Group	dc:37:14:2c:ae:C8		512	1440

### Procedures:

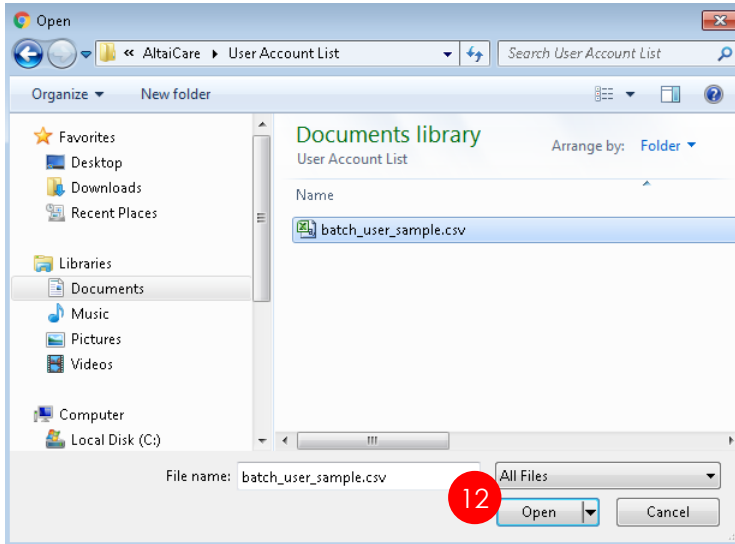
- Click "Save" button.
- Open the file "batch\_user\_sample.csv".
- Give a name for the account. This name is not used for login.
- Assign the user account to one of the User Groups which have been created in Step 4, e.g. PP User Group and SC User Group for WPA/Portal Authentication; and PP MAC Group and SC MAC Group for MAC Authentication in our example.
- 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**
- Enter Password for user login. For MAC Authentication, this item is not applicable and you can keep it blank.
- 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.
- 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.

## 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.

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

User Account List [Show Filter](#)

Batch Actions: [Remove All](#)



USER LOGIN NAME ^	NAME	USER GROUP NAME	REMAINING DATA QUOTA (MB)	EMAIL	PHONE / MOBILE	EXPIRY TIME	LAST LOGIN TIME	
<a href="#">44:85:00:99:23:d4</a>	ppmac01	PP MAC Group	500	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">9c:4e:36:8c:c9:e0</a>	scmac01	SC MAC Group	No Limit	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">c4:85:08:90:1e:47</a>	ppmac02	PP MAC Group	500	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">dc:37:14:2c:ae:c8</a>	scmac02	SC MAC Group	512	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">ppuser01</a>	ppuser01	PP User Group	500	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">ppuser02</a>	ppuser02	PP User Group	500	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">ppuser03</a>	ppuser03	PP User Group	1000	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">scuser01</a>	scuser01	SC User Group	No Limit	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">scuser02</a>	scuser02	SC User Group	No Limit	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">scuser03</a>	scuser03	SC User Group	5000	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>

Showing 1-10 of 10 entries [10](#)

< [1](#) >

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

Account Name	Username	Password	User Group	Purpose
<b>ppuser02</b>	ppuser02	ppuser02	PP User Group	Used for portal username/password login via SSID: "Care_UDT_Portal"
<b>ppuser03</b>	ppuser03	ppuser03	PP User Group	Used for portal username/password login via SSID: "Care_UDT_Portal"
<b>scuser02</b>	scuser02	scuser02	SC User Group	Used for WPA authentication via SSID: "Care_WPA"
<b>scuser03</b>	scuser03	scuser03	SC User Group	Used for WPA authentication via SSID: "Care_WPA"
<b>ppmac02</b>	c4:85:08:90:1e:47	N/A	PP MAC Group	Used for MAC authentication via SSID: "Care_MAC_Auth"
<b>scmac02</b>	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.

User Account List [Show Filter](#)

Batch Actions: [Remove All](#)



USER LOGIN NAME ^	NAME	USER GROUP NAME	REMAINING DATA QUOTA (MB)	EMAIL	PHONE / MOBILE	EXPIRY TIME	LAST LOGIN TIME	
<a href="#">44:85:00:99:23:d4</a>	ppmac01	PP MAC Group	500	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">9c:4e:36:8c:c9:e0</a>	scmac01	SC MAC Group	No Limit	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">ppuser01</a>	ppuser01	PP User Group	500	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">scuser01</a>	scuser01	SC User Group	No Limit	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>

Showing 1-4 of 4 entries [10](#)

< [1](#) >

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

The screenshot shows the AltaiCare interface with the 'SERVICE' tab selected. The breadcrumb path is 'Altai WiFi Service > Alert List'. The 'Alert List' section is active, showing a table with one entry. The table has columns for NAME, ALERT RAISE TIME, ALERT TYPE, ALERT SEVERITY, and ALERT CATEGORY. The entry is for a 'User Account Import Failure' on '2017-07-25 12:17:38' with a 'Major' severity and 'User Account' category. A red arrow points to the 'SERVICE' tab, and another red arrow points to the 'Alert' menu item in the left sidebar. A red arrow points to the 'Detail' button for the alert entry. A dashed red arrow points from the 'Detail' button to the 'Alert [353488] Detail Info' section below.

NAME	ALERT RAISE TIME	ALERT TYPE	ALERT SEVERITY	ALERT CATEGORY
=	2017-07-25 12:17:38	User Account Import Failure	Major	User Account

Alert [353488] Detail Info

The 'GENERAL' section of the alert details provides the following information:

- RAISE TIME : 2017-07-25 10:22:07
- ALERT TYPE : User Account Import Failure
- ALERT SEVERITY : Major
- ALERT CATEGORY : User Account
- ALERT DETAILS : User account import success count: 4  
User account import failure count: 2

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

BACK TO THE LIST

# Step 5d: Voucher-based user account batch generation

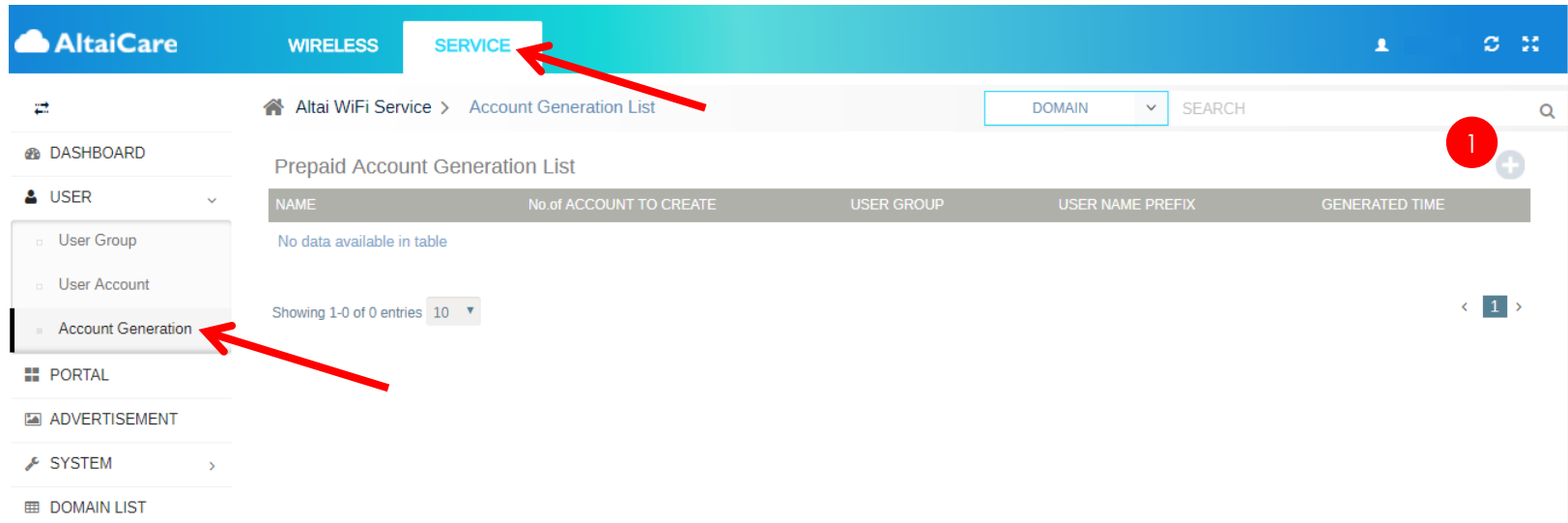
(For WPA/Portal Prepaid Account ONLY)



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.



The screenshot displays the AltaiCare web interface. The top navigation bar includes 'AltaiCare', 'WIRELESS', and 'SERVICE'. A red arrow points to the 'SERVICE' tab. Below the navigation bar, the breadcrumb path is 'Altai WiFi Service > Account Generation List'. A search bar with a 'DOMAIN' dropdown and a 'SEARCH' button is visible. The main content area is titled 'Prepaid Account Generation List' and contains a table with columns: 'NAME', 'No. of ACCOUNT TO CREATE', 'USER GROUP', 'USER NAME PREFIX', and 'GENERATED TIME'. The table is currently empty, displaying 'No data available in table'. A red circle with the number '1' is placed over a plus icon in the top right corner of the table area. The left sidebar contains a menu with options: 'DASHBOARD', 'USER', 'PORTAL', 'ADVERTISEMENT', 'SYSTEM', and 'DOMAIN LIST'. The 'USER' menu is expanded, and a red arrow points to the 'Account Generation' option.

# 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.

The screenshot shows a web form titled "PREPAID ACCOUNT GENERATION WIZARD" with the following fields and callouts:

- 2. NUMBER OF ACCOUNT TO CREATE: 100
- 3. USER GROUP: PP Voucher User Group
- 4. ACTIVATION STATUS:
- 5. USER NAME PREFIX: Jul2017
- 6. USER LOGIN NAME COMBINATION: Prefix & Random
- 7. USER LOGIN NAME PREFIX: hi
- 8. USER LOGIN NAME LENGTH: 6
- 9. USER LOGIN PASSWORD COMBINATION: Random
- 10. USER LOGIN PASSWORD LENGTH: 6
- 11. CREATE CANCEL

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**

# Step 5d: Voucher-based user account batch generation (Cont.)

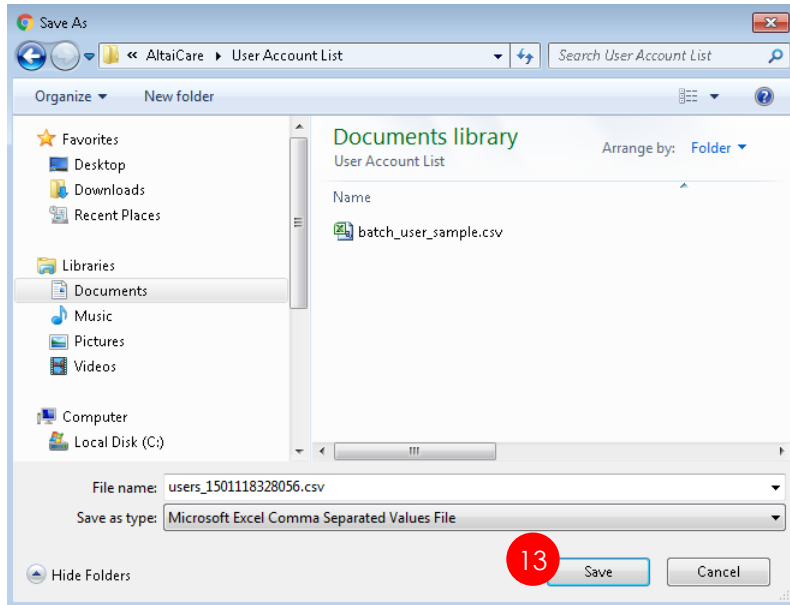
(For WPA/Portal Prepaid Account ONLY)

## Prepaid Account Generation List

NAME	No.of ACCOUNT TO CREATE	USER GROUP	USER NAME PREFIX	GENERATED TIME	
users_1501118328056.csv	100	PP Voucher User Grou...	Jul2017	2017-07-27 09:18:48	<span>12</span> <a href="#">Download</a> <a href="#">Delete</a>

Showing 1-1 of 1 entries 10 ▾

< 1 >



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.

# Step 5d: Voucher-based user account batch generation (Cont.)

(For WPA/Portal Prepaid Account ONLY)

14

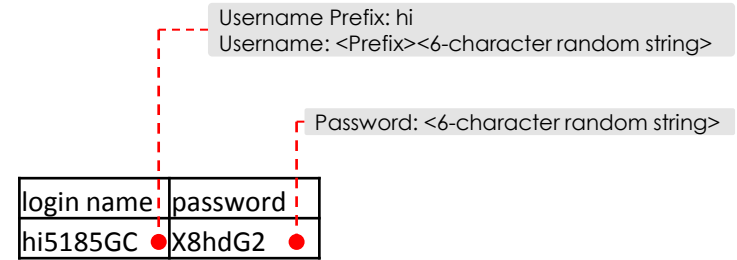
users\_1501118328056.csv - Microsoft Excel

15

login name	password
hi5185GC	X8hdG2
hi60t0Z7	3T8fx7
hiOe63My	1j51D1
hiF43832	n25df1
hiZ0e00l	n36LU6
hi816VCf	V5jr7Z
hib7852g	1S3H07
hi77211i	WoGp72
hiYTajv4	k485Hm
hiFO2k4R	0Kvoz3
hi15T21M	h0Z3FQ
hi08q366	4KA1dL
hiOG216C	8R6X6X
hiHvqcZf	800y44
hi6nuH7	116nuH7

## Procedures:

- 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.
- In our example, we have 100 pairs of different username/password combination for demo purpose.



# 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

USER LOGIN NAME	NAME ^	USER GROUP NAME	REMAINING DATA QUOTA (MB)	EMAIL	PHONE / MOBILE	EXPIRY TIME	LAST LOGIN TIME	
<a href="#">hi5185GC</a>	Jul2017_1	PP Voucher User Grou...	No Limit	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">hiFO2k4R</a>	Jul2017_10	PP Voucher User Grou...	No Limit	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">hiM25r80</a>	Jul2017_100	PP Voucher User Grou...	No Limit	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">hi15T21M</a>	Jul2017_11	PP Voucher User Grou...	No Limit	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">hi08q366</a>	Jul2017_12	PP Voucher User Grou...	No Limit	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">hiOG216C</a>	Jul2017_13	PP Voucher User Grou...	No Limit	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">hiHvacZf</a>	Jul2017_14	PP Voucher User Grou...	No Limit	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">higrdpuk</a>	Jul2017_15	PP Voucher User Grou...	No Limit	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">hib8x7C4</a>	Jul2017_16	PP Voucher User Grou...	No Limit	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<a href="#">hiwHnOR3</a>	Jul2017_17	PP Voucher User Grou...	No Limit	--	-- / --	No Limit	--	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>

## Step 6a: Custom Template Portal Setup

## Step 6a: Custom Template Portal Setup – Create Portal


The screenshot shows the 'Altai WiFi Service > Portal List' page. The 'SERVICE' tab is active. A search bar with a 'DOMAIN' dropdown and a 'SEARCH' button is at the top right. A table with columns 'NAME', 'TEMPLATE TYPE', and 'LAST UPDATE TIME' is shown, but it is empty with the message 'No data available in table'. A red circle with the number '1' highlights a '+' icon in the top right of the table area. The left sidebar contains menu items: DASHBOARD, USER, PORTAL, ADVERTISEMENT, SYSTEM, and DOMAIN LIST. A red arrow points to the 'PORTAL' menu item, which is labeled with a red circle containing the number '2'.

The 'NEW PORTAL CONFIG' dialog box is shown. It has a blue header with a close button. The form contains the following fields:

- NAME:** A text input field containing 'Custom Template Portal', labeled with a red circle containing the number 2.
- TEMPLATE TYPE:** A dropdown menu with 'Custom Template' selected, labeled with a red circle containing the number 3.
- CUSTOM TEMPLATE STYLE:** A dropdown menu with 'Simple' selected, labeled with a red circle containing the number 4.

At the bottom, there are two buttons: 'CREATE' and 'CLOSE'.

### 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.

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

**GENERAL**

PORTEL NAME:

TEMPLATE TYPE:

SUPPORTED LANGUAGES:

LANDING URL:

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

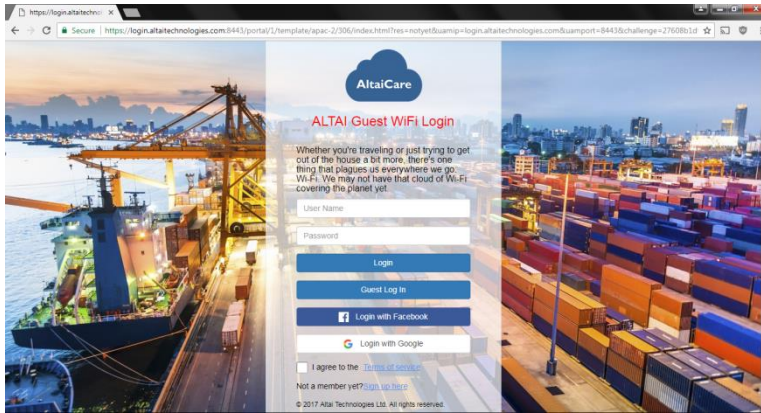
Assign User Groups for those auto-generated accounts for different login methods

**LOGIN / SIGN-UP METHODS**

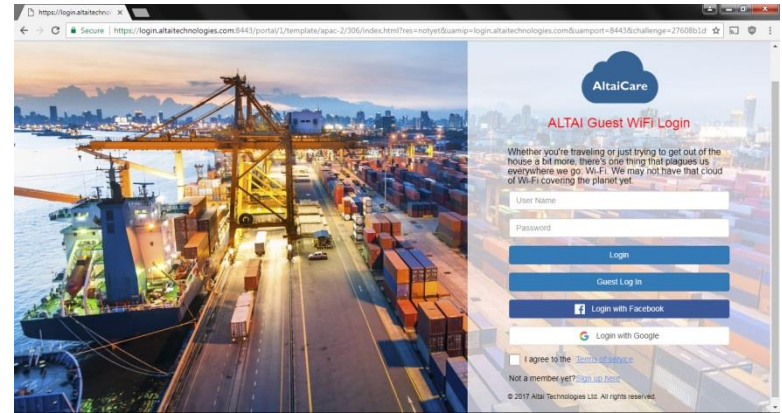
LOGIN/SIGN-UP METHODS:

GUEST LOGIN:	<input type="text" value="Guest Group"/>	X
EMAIL SIGN-UP:	<input type="text" value="Guest Group X"/>	X
FACEBOOK LOGIN:	<input type="text" value="Guest Group"/>	X
GOOGLE LOGIN:	<input type="text" value="Guest Group"/>	X

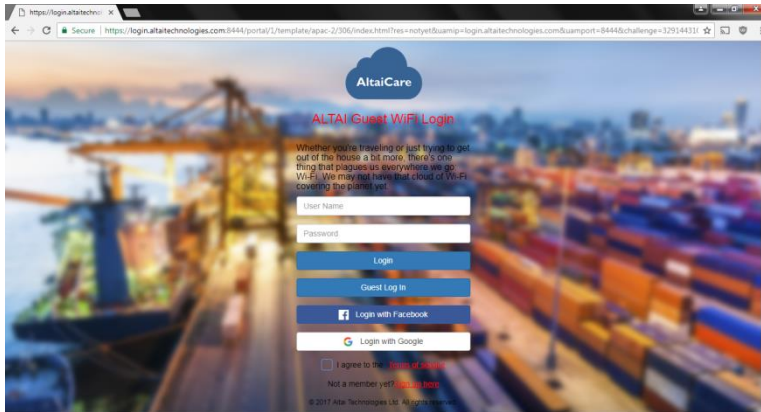
# Step 6a: Custom Template Portal Setup – General & Login/Sign-Up Methods (Cont.)



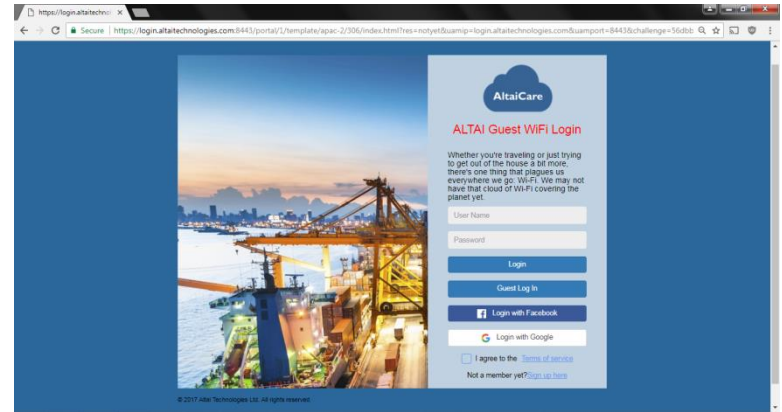
Simple Type Template



Clear Type Template

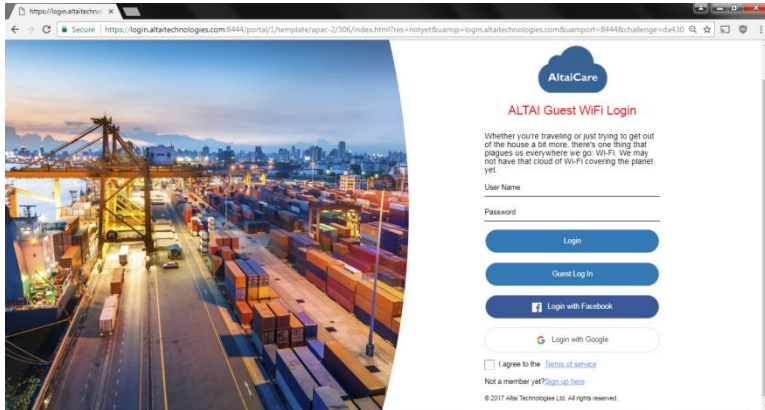


Blur Type Template

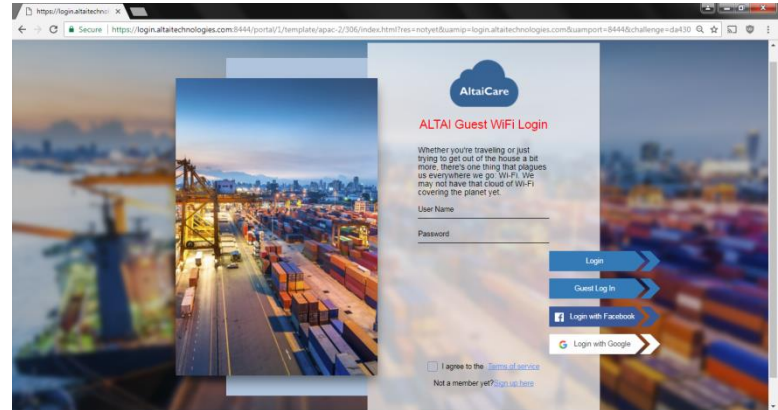


Grid Type Template

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

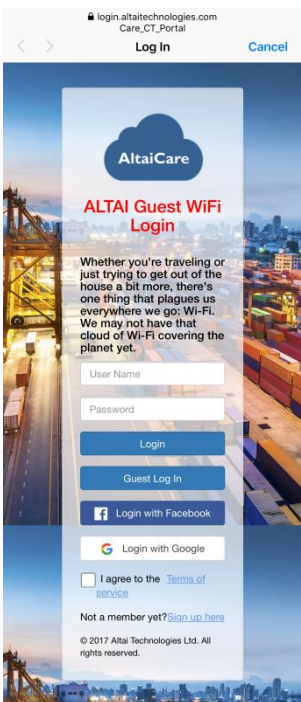


Curvy Type Template

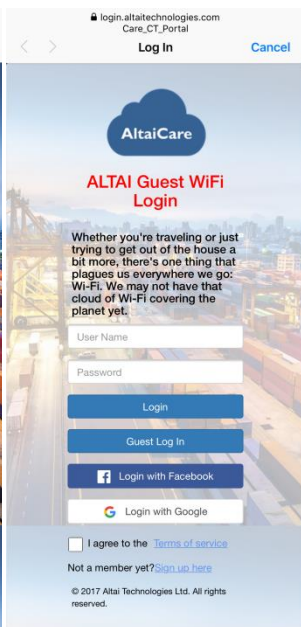


Stylish Type Template

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



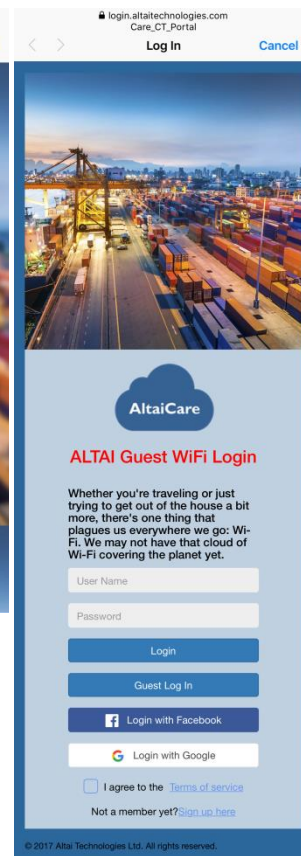
Simple Type Template



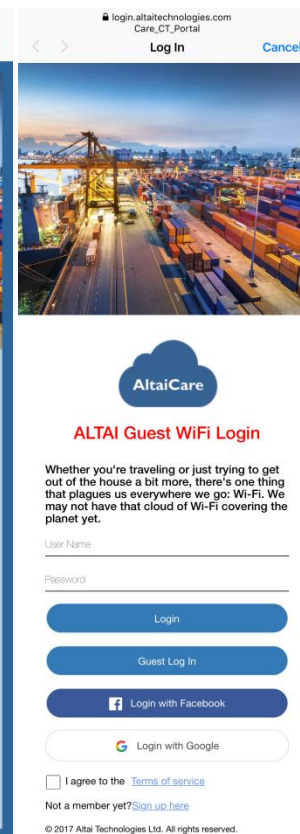
Clear Type Template



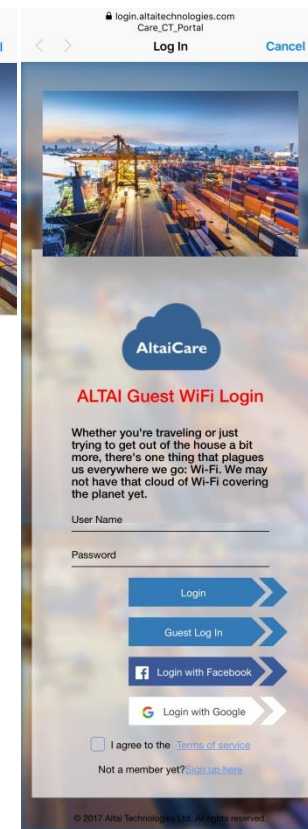
Blur Type Template



Grid Type Template



Curvy Type Template



Stylish Type Template



Note: Screenshots from iOS



# 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: \*

SENDER NAME: \*

EMAIL HEADER: \*

SIGNATURE: \*

Note: Screenshots from outlook app (iOS version)

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

## CAPTIVE NETWORK ASSISTANT(CNA)

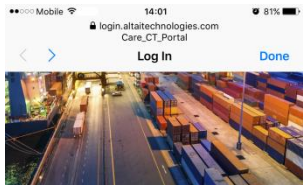
CNA DETECTION ENABLED:

CNA INSTRUCTION ANDROID:

Welcome to our Wi-Fi network. Please open your web browser to complete the login procedure.

CNA INSTRUCTION IOS:

Welcome to our Wi-Fi network. Please follow below instruction to complete the login:<u><li>Press "Cancel" button at the top right corner.</li><li>Choose "Use Without Internet" option to maintain the connection to our WiFi network.</li></u>



### ALTAI Guest WiFi Login

Welcome to our Wi-Fi network. Please follow below instruction to complete the login:

- Press "Cancel" button at the top right corner.
- Choose "Use Without Internet" option to maintain the connection to our WiFi network.
- Open your device web browser on an non-HTTPS to complete the login procedure.

© 2017 Altai Technologies Ltd. All rights reserved.

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.

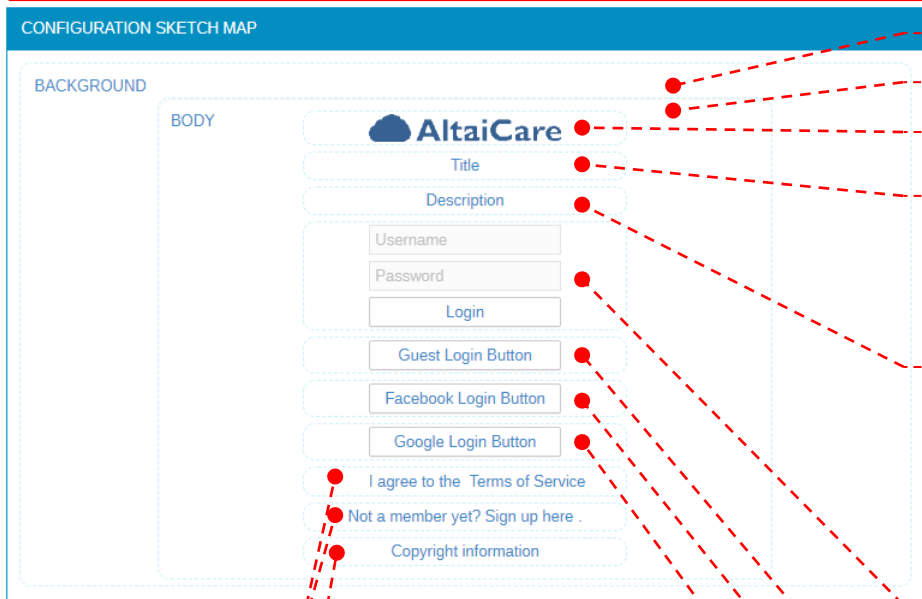
However, the app is not like other web browsers such as Safari, Chrome, ... It supports very limited functions and may even not be desirable when it comes to particular login methods. For this case, we may need a way to guide the users how to bypass the CNA and use the standard web browsers to proceed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

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

**TERMS OF SERVICE(TOS) SETTING**

**MAIN PAGE**

TOS LABEL:

TOS REMINDER TEXT:

**POP UP PAGE**

TOS DETAIL:  **B**

TOS DETAIL COLOR:

**Terms of Service ("this TOS")**

**1. Access to this Service**

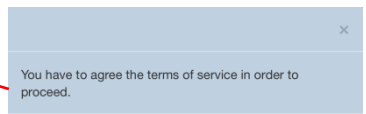
1



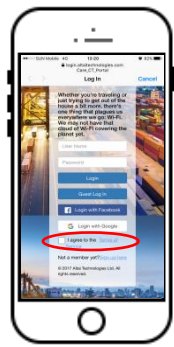
Attempt to sign in without checking the box of the "Terms of Service"

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



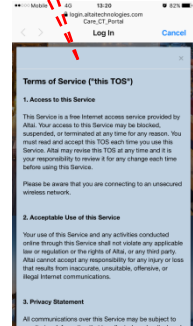
3



I agree to the [Terms of Service](#)

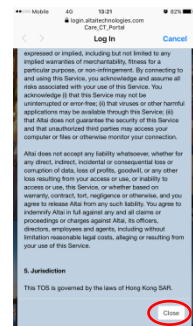
Click TOS Label

4



A TOS page pops up

5



Close

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.

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

**SIGNUP SETTING**

**MAIN PAGE**

SIGN UP LINK PREFIX:

SIGN UP LINK:

**POP UP PAGE**

SIGN UP EMAIL PLACEHOLDER:

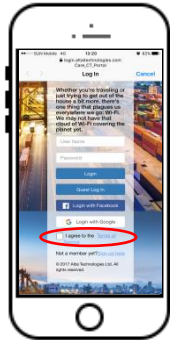
SIGN UP PASSWORD PLACEHOLDER:

SUBMIT BUTTON TEXT:



**Note:** This setting is for Email sign up ONLY

1

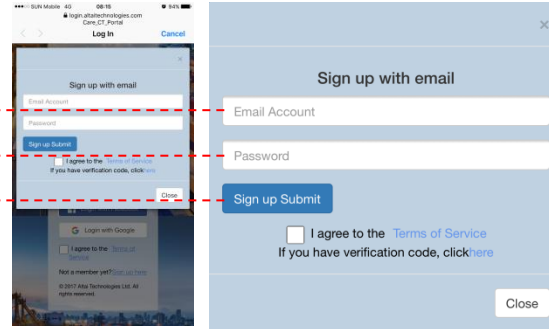


Not a member yet? [Sign up here](#)

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

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

Template Preview

Desktop Mobile

**AltaiCare**

**ALTAI Guest WiFi Login**

Whether you're traveling or just trying to get out of the house a bit more, there's one thing that plagues us everywhere we go: Wi-Fi. We may not have that cloud of Wi-Fi covering the planet yet.

User Name

Password

Login

Guest Log In

Login with Facebook

Login with Google

I agree to the [Terms of Service](#)

Not a member yet? [Sign up here](#)

© 2017 Altai Technologies Ltd. All rights reserved.

**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):**

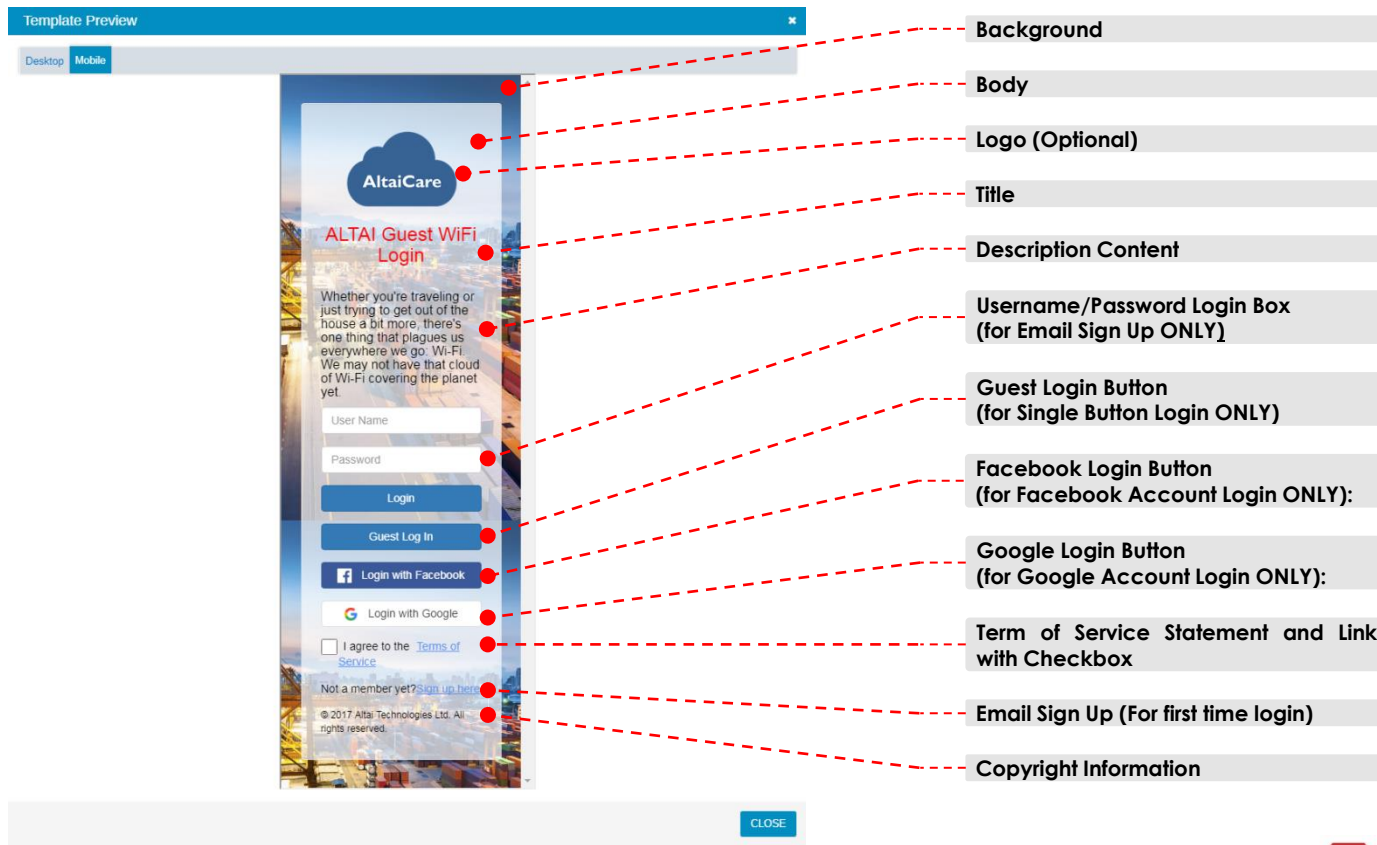
**Term of Service Statement and Link with Checkbox**

**Email Sign Up (For first time login)**

**Copyright Information**

CLOSE

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



The image shows a mobile preview of the AltaiCare login portal. The interface includes a header with the AltaiCare logo, a title 'ALTAI Guest WiFi Login', a descriptive paragraph, a login form with fields for 'User Name' and 'Password', and buttons for 'Login', 'Guest Log In', 'Login with Facebook', and 'Login with Google'. There is also a checkbox for 'I agree to the Terms of Service' and a link for 'Not a member yet? Sign up here'. A copyright notice is at the bottom. Red dashed lines connect various parts of the interface to a list of customizable elements on the right.

- 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

## Step 6b: User Defined Template Portal Setup

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

WIRELESS SERVICE

Altai WiFi Service > Portal List

DOMAIN SEARCH

Portal List

NAME	TEMPLATE TYPE	LAST UPDATE TIME	
<a href="#">Custom Template Portal</a>	Simple Template	2017-07-07 13:28:02	<a href="#">Edit</a> <a href="#">Preview</a> <a href="#">Delete</a>

Showing 1-1 of 1 entries 10 < 1 >

DASHBOARD

USER >

PORTAL

ADVERTISEMENT

SYSTEM >

DOMAIN LIST

NEW PORTAL CONFIG

2 NAME: User Defined Template Portal

3 TEMPLATE TYPE: User Defined Template

4 CREATE CLOSE

### 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.

# Step 6b: User Defined Template Portal Setup – General

**GENERAL**

PORTAL NAME:

TEMPLATE TYPE:

LANDING URL:

THEME COLOR:

BACKGROUND COLOR: \*

BUTTON COLOR: \*

BUTTON FONT COLOR: \*

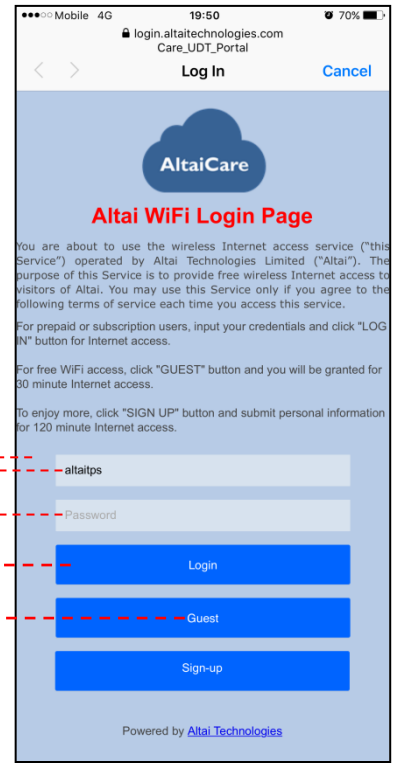
INPUT FONT COLOR: \*

INPUT PLACEHOLDER FONT COLOR: \*

For User Defined color

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



## 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

LOGIN / SIGN-UP METHODS

LOGIN/SIGN-UP METHODS: User & Password Guest Simple

GUEST LOGIN: Guest Group x

SIMPLE SIGN-UP: Guest Group x



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](#)).

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

PORTAL SIGN IN/GUEST IN TEMPLATE

CUSTOMIZATION MODE:

Image Element for Logo

IMAGE FILE:  No file chosen  
(Maximum size: 500 KB)




IMAGE SIZE: Original image size

IMAGE EXTERNAL LINK: <http://www.altaittechnologies.com>

Text Element for Title

TEXT: x-large

Altai WiFi 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.

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

**Text Element for Description Content**

**Text Element for Description Content**

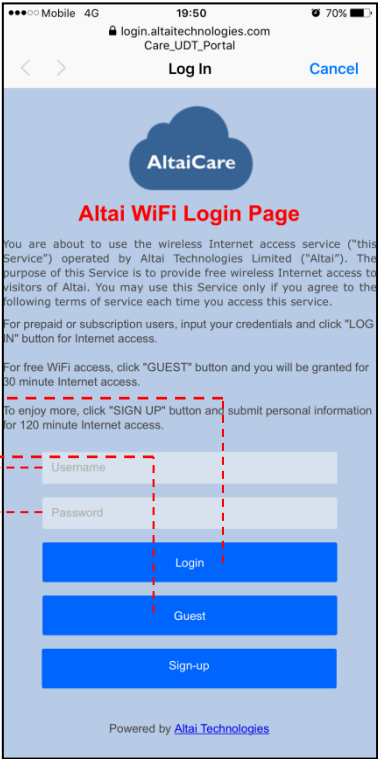
**Login Element (Default)**

- LOGIN BUTTON TEXT: Login
- GUEST LOGIN BUTTON TEXT: Guest
- LOGIN NAME PLACEHOLDER: Username
- LOGIN PASSWORD PLACEHOLDER: Password

**Text Element for Copyright Info**

care.altatechnologies.com says:  
Please enter the URL  
  
OK Cancel

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



Highlight the text and click "🔗" button. Enter the URL in the pop up box. Then click "OK" to confirm it

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

Image Element for Separation Line

Image Element for Terms of Service

IMAGE FILE:  Separation Line.png  
(Maximum size: 500 KB)

IMAGE SIZE: Original image size

IMAGE EXTERNAL LINK: http(s):/www.domain.com

TEXT: x-large **Terms of Service ("this TOS")**

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

Mobile 4G 11:24 99%

login.altaittechnologies.com  
Care\_UDT\_Portal

Log In Cancel

Username

Password

Login

Guest

Sign-up

Powered by [Altai Technologies](#)

Terms of Service ("this TOS")

1. Access to this Service

This Service is a free Internet access service provided by Altai. Your access to this Service may be blocked, suspended, or terminated at any time for any reason. You must read and accept this TOS each time you use this Service. Altai may revise this TOS at any time and it is your responsibility to review it for any change each time before using this Service.

Please be aware that you are connecting to an unsecured wireless network.

2. Acceptable Use of this Service

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

PORTAL SIGN UP TEMPLATE

CUSTOMIZATION MODE:

IMAGE FILE:  No file chosen  
(Maximum size: 500 KB)




IMAGE SIZE: Original image size

IMAGE EXTERNAL LINK:


TEXT: medium

sign up for free WiFi access here

By clicking "Confirm", you accept our Terms of Service

**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



# 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.

**AltaiCare**

### Altai WiFi Login Page

You are about to use the wireless Internet access service ("this Service") operated by Altai Technologies Limited ("Altai"). The purpose of this Service is to provide free wireless Internet access to visitors of Altai. You may use this Service only if you agree to the following terms of service each time you access this service.

For prepaid or subscription users, input your credentials and click "LOG IN" button for Internet access.

For free WiFi access, click "GUEST" button and you will be granted for 30 minute Internet access.

To enjoy more, click "SIGN UP" button and submit personal information for 120 minute Internet access.

Username:

Password:

**Login**

**Guest**

**Sign-up**

Powered by Altai Technologies

#### Terms of Service ("this TOS")

- 1. Access to this Service**

This Service is a free Internet access service provided by Altai. Your access to this Service may be blocked, suspended, or terminated at any time for any reason. You must read and accept this TOS each time you use the Service. Altai may revise this TOS at any time and it is your responsibility to review it for any change each time before using this Service. Please be aware that you are connecting to an unsecured wireless network.
- 2. Acceptable Use of this Service**

Your use of this Service and any activities conducted online through this Service shall not violate any applicable law or regulation or the rights of Altai, or any third party. Altai cannot accept any responsibility for any injury or loss that results from malicious, unlawful, offensive, or illegal Internet communications.
- 3. Privacy Statement**

All communications over this Service may be subject to monitoring. Information that is collected can be disclosed under authorized investigations, for capacity planning purposes, or any other required activities for Altai to manage this Service. Information that is collected may also include "personal data" as defined in the Personal Data (Privacy) Ordinance. You have certain rights in the personal data. By using the Service you grant us the consent to use your personal data in accordance with Altai's Privacy Policy.

**3. Jurisdiction**

This TOS is governed by the laws of Hong Kong SAR.

Sign In/Guest Login Page

**AltaiCare**

### Sign up for free WiFi access here

By clicking "Confirm", you accept our Terms of Service

Username:

Email:

Mobile:

Country:

**Confirm**

**Back**

Powered by Altai Technologies

**CLOSE**

Sign Up Page

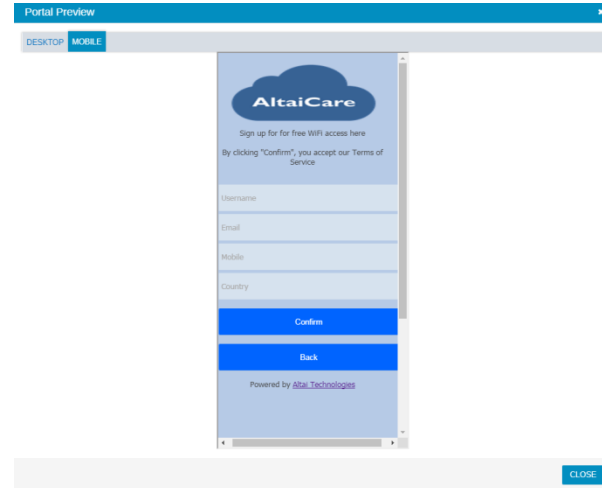
# Step 6b: User Defined Template Portal Setup – Template Preview (Mobile)



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

## Step 7a: Create Portal Security Profile

## Step 7a: Create Portal Security Profile

The screenshot shows the AltaiCare interface. The top navigation bar has tabs for 'WIRELESS', 'SERVICE', and 'PROJECT'. The left sidebar shows a menu with 'Security' selected. The main content area displays a 'Security Profile List' table. A 'NEW SECURITY PROFILE' dialog box is open, showing the 'NAME' field filled with 'Care\_CT\_Portal' and 'CREATE' and 'CANCEL' buttons. Red circles and arrows highlight the steps: 1. Clicking the '+' button to add a new profile, 2. Entering the name 'Care\_CT\_Portal', 3. Clicking the 'CREATE' button, and 4. Clicking the 'Edit' button on the newly created profile in the list below.

NAME	AUTHENTICATION MODE	PORTAL MODE	SERVICE DOMIN / PORTAL NAME	RADIUS SERVER
No data available in table				

Showing 1-0 of 0 entries 10

NEW SECURITY PROFILE

NAME: Care\_CT\_Portal

CREATE CANCEL

NAME	AUTHENTICATION MODE	PORTAL MODE	SERVICE DOMIN / PORTAL NAME	RADIUS SERVER
<a href="#">Care_CT_Portal</a>	Open	--	--/--	--

Showing 1-1 of 1 entries 10

### 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.

## Step 7a: Create Portal Security Profile – Portal Setting

**GENERAL**

SECURITY PROFILE NAME: Care\_CT\_Portal

5 AUTHENTICATION MODE: PORTAL

- Open
- WPA
- WPA-PSK
- MAC
- PORTAL

**PORTAL DETAIL**

PORTAL

6 PORTAL MODE: Built-in

- Built-in
- External

7 SERVICE DOMAIN: Altai WiFi Service

8 PORTAL: Custom Template Portal

PORTAL DHCP LEASE TIME (Seconds): 7200

PORTAL ACL MODE:  DISABLE  ENABLE

### 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.

## Step 7a: Create Portal Security Profile – RADIUS Setting

RADIUS

**9** RADIUS SERVER:  Built-in  
 External

**10** ALLOWED USER GROUPS:

RADIUS RETRY TIMEOUT (Seconds):

NAS IDENTIFIER:

### 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](#).

MAC ACCESS CONTROL LIST

ACL MODE:

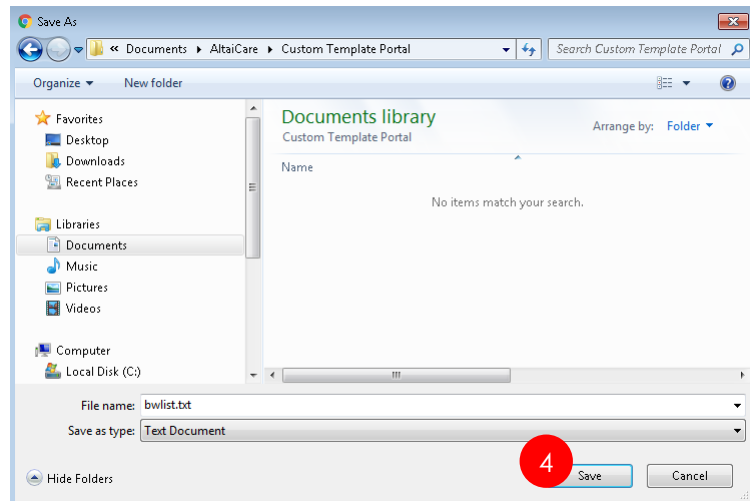
# Step 7a: Create Portal Security Profile – Portal ACL Configuration

- 1 PORTAL ACL MODE:  DISABLE  ENABLE
- 2 PORTAL ACL FILE: [UPLOAD](#) (\* Portal ACL file is not uploaded yet.)

## IMPORT PORTAL ACL FILE

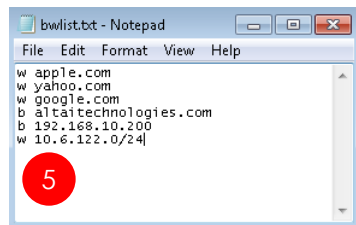
ACL FILE:  No file chosen

[ACL\\_SAMPLE](#)



### 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

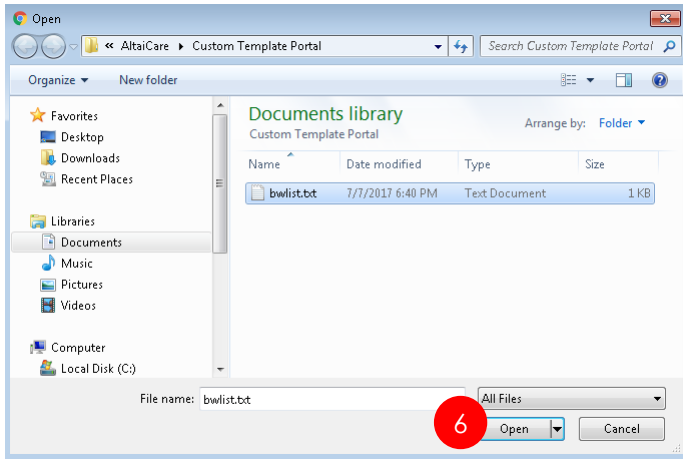


Note: The list can consist of domain, single IP or even IP subnet



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.

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

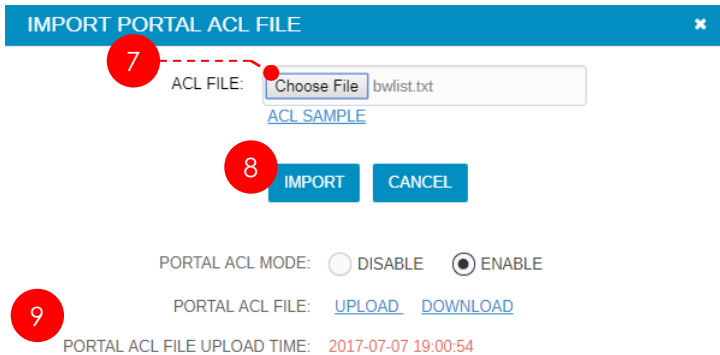


### Procedures:

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.





## Step 7b: Create WPA Security Profile

## Step 7b: Create WPA Security Profile

The screenshot shows the AltaiCare web interface. The top navigation bar has tabs for 'WIRELESS', 'SERVICE', and 'PROJECT'. The left sidebar contains a menu with 'Security' selected. The main area displays a 'Security Profile List' table with columns: NAME, AUTHENTICATION MODE, PORTAL MODE, SERVICE DOMIN / PORTAL NAME, and RADIUS SERVER. A modal window titled 'NEW SECURITY PROFILE' is open, showing a 'NAME' field with 'Care\_WPA' and 'CREATE' and 'CANCEL' buttons. Below the modal, the 'Security Profile List' table shows one entry: 'Care\_WPA' with 'Open' authentication mode. Red annotations (1-4) and arrows indicate the steps: 1. Clicking the '+' button in the top right of the table. 2. Entering 'Care\_WPA' in the 'NAME' field. 3. Clicking the 'CREATE' button. 4. Clicking the 'Edit' button on the 'Care\_WPA' entry in the table.

### 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  to further configure it.

## Step 7b: Create WPA Security Profile – RADIUS Setting

**GENERAL**

SECURITY PROFILE NAME: Care\_WPA

5 AUTHENTICATION MODE: WPA

- Open
- WPA
- WPA-PSK
- MAC
- PORTAL

**WPA DETAIL**

GROUP KEY INTERVAL (Seconds): 86400

**RADIUS**

6 RADIUS SERVER:  Built-in  External

7 SERVICE DOMAIN: Altai WiFi Service

8 ALLOWED USER GROUPS: SC User Group x

RADIUS RETRY TIMEOUT (Seconds): 300

NAS IDENTIFIER: 0-32 characters

### 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.

## 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](#).

MAC ACCESS CONTROL LIST

ACL MODE:

- Disable
- Black List
- White List

## Step 7c: Create MAC Auth Security Profile

## Step 7c: Create MAC Auth Security Profile

The screenshot shows the AltaiCare web interface. The top navigation bar has tabs for 'WIRELESS', 'SERVICE', and 'PROJECT'. The left sidebar contains a menu with 'Security' selected. The main content area displays a 'Security Profile List' table with columns: NAME, AUTHENTICATION MODE, PORTAL MODE, SERVICE DOMAIN / PORTAL NAME, and RADIUS SERVER. A 'NEW SECURITY PROFILE' modal is open, showing a 'NAME' field with the value 'Care\_MAC\_Auth' and 'CREATE' and 'CANCEL' buttons. Below the modal, the 'Security Profile List' table shows one entry: 'Care\_MAC\_Auth' with 'Open' authentication mode. The table has 'Edit' and 'Delete' buttons for each entry.

NAME	AUTHENTICATION MODE	PORTAL MODE	SERVICE DOMAIN / PORTAL NAME	RADIUS SERVER
Care_MAC_Auth	Open	--	-- / --	--

### 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 to further configure it.

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

**GENERAL**

SECURITY PROFILE NAME: Care\_MAC\_Auth

5 AUTHENTICATION MODE: MAC

- Open
- WPA
- WPA-PSK
- MAC
- PORTAL

**MAC DETAIL**

RADIUS

6 RADIUS SERVER:  Built-in  External

7 SERVICE DOMAIN: Altai WiFi Service

8 ALLOWED USER GROUPS: PP MAC Group × SC MAC Group ×

RADIUS RETRY TIMEOUT (Seconds): 300

NAS IDENTIFIER: 0-32 characters

### 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

MAC ACCESS CONTROL LIST

ACL MODE:

- Disable
- Black List
- White List

### 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

The screenshot shows the AltaiCare interface. The top navigation bar has tabs for 'WIRELESS', 'SERVICE', and 'PROJECT'. The left sidebar has a 'Security' menu item highlighted. The main content area shows a 'Security Profile List' table with a '+' button in the top right corner. A 'NEW SECURITY PROFILE' modal is open, showing a 'NAME' field with the value 'Care\_WPA\_PSK' and 'CREATE' and 'CANCEL' buttons. Below the modal, the 'Security Profile List' table is updated with one entry: 'Care\_WPA\_PSK' with 'Open' authentication mode. The 'Edit' button for this entry is highlighted.

NAME	AUTHENTICATION MODE	PORTAL MODE	SERVICE DOMAIN / PORTAL NAME	RADIUS SERVER
Care_WPA_PSK	Open	--	--/--	--

### 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  to further configure it.

## Step 7d: Create WPA-PSK Security Profile

**GENERAL**

SECURITY PROFILE NAME: Care\_WPA\_PSK

5 AUTHENTICATION MODE: WPA-PSK

- Open
- WPA
- WPA-PSK
- MAC
- PORTAL

**WPA-PSK DETAIL**

GROUP KEY INTERVAL (Seconds): 86400

6 PASSPHRASE: altaitps

**MAC ACCESS CONTROL LIST**

ACL MODE: Disable

- Disable
- Black List
- White List

### 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](#).

## Step 8: Create SSID (WLAN)

## Step 8: Create New WLAN – Basic Setting

The screenshot shows the AltaiCare interface with the 'WIRELESS' tab selected. The 'WLAN List' table is empty, and the 'NEW WLAN' form is open. The form fields are: NAME: Care\_CT\_Portal, SSID: Care\_CT\_Portal, SCOPE: Site, TARGET RADIO: Both, and SECURITY PROFILE: Care\_CT\_Portal. The 'CREATE' button is highlighted with a red circle and arrow.

**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.

## Step 8: Create New WLAN – WLAN Scheduler

### SCHEDULE

ENABLE SCHEDULE:  + Schedule

DAYS OF WEEK: MONDAY x FRIDAY x

SCHEDULE WORK TIME: 9:00 AM - 6:00 PM

DAYS OF WEEK: SATURDAY x

SCHEDULE WORK TIME: 9:00 AM - 1:00 PM

### Optional Items:

**Enable Schedule:** Check the box to enable the scheduler. It controls the periods for the WLAN service by enabling/disabling 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.

## Step 8: Create New WLAN – Advanced Setting

ADVANCED

HIDE SSID:

INTRA-WLAN USER ISOLATION:

VLAN PASS THROUGH:

VLAN ID:

ACCESS TRAFFIC RIGHT:

**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.

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

ALLOW DHCP SNOOPING TRUSTED PORT:

MAX STATION:

WLAN MAXIMUM UPLINK (Kbps):

WLAN MAXIMUM DOWNLINK (Kbps):

STATION MAXIMUM UPLINK (Kbps):

STATION MAXIMUM DOWNLINK (Kbps):

**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):   
(0-100dB, 0:Disable)

DISASSOCIATE STATION IF SNR DROPS MORE THAN (dB):

FOR CONSECUTIVE  PACKETS

**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.

## 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

AltaiCare WIRELESS SERVICE PROJECT [altaitps]

Altai Office > AP List

AP List Show Filter

No data available in table

Showing 1-0 of 0 entries 10

NEW AP

NAME: HKO\_A3w

ETHERNET MAC: 00:19:be:a3:09:20

CREATE CANCEL

## 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.

Status Configuration Administration Tools About

Overview Radio0(2.4G) Radio1(5G) Ethernet Logs

**System**

System Name: NA  
Product Name: A3w  
CPU Usage: 40%  
Memory Usage: 36/236 MB (15%)  
Time of Day: Thu Jul 13 15:38:00 2017  
Uptime: 23h 59min 12s

**Network(Switch Mode)**

Ethernet  
IPv4 DHCP Client: Disabled  
IPv4 Address: 192.168.100.30  
IPv4 Subnet Mask: 255.255.255.0  
IPv4 Default Gateway: 192.168.100.1  
IPv4 DNS Server: 10.6.127.4, 8.8.8.8

**Interfaces(4)**

Ethernet (eth0)  
MAC: 00:19:be:a3:09:20  
Link: Auto (Full 100Mb/s)

**Remote Management**

Remote Management: OFF

AP WebUI

## Step 9a: Single AP Registration (Cont.)

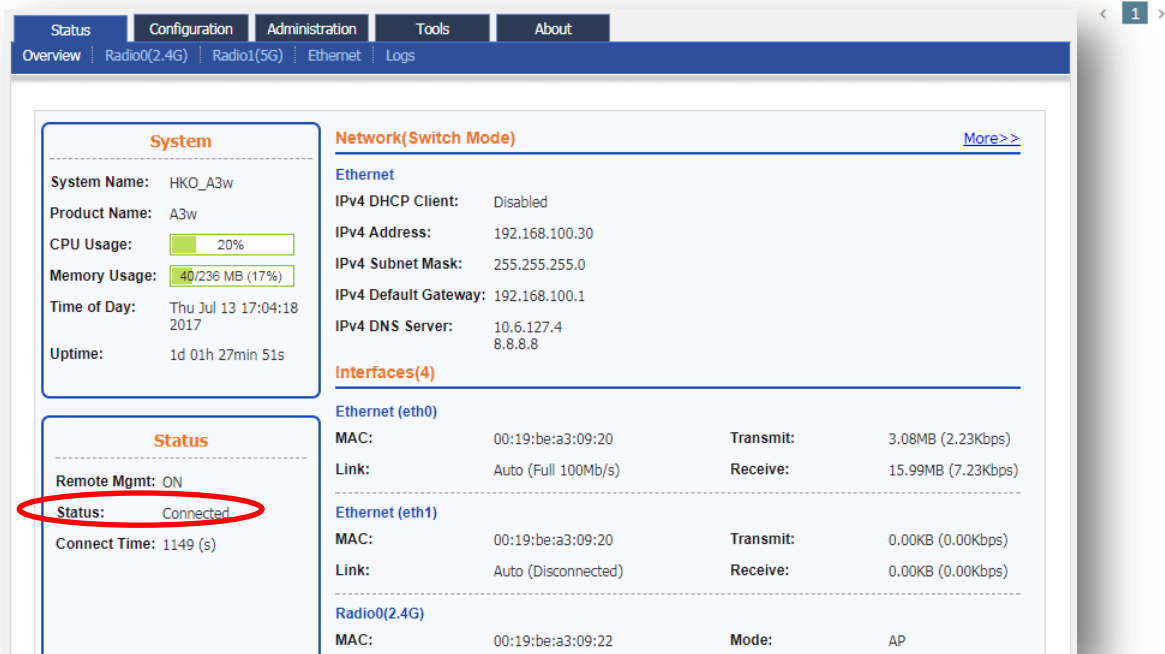
AP List [Show Filter](#)

STATUS	NAME ^	BRANCH	MODEL	ETHERNET MAC	SERIAL	IP ADDRESS	CHANNEL	ALERT	STATION	AVG RSSI	LAST CONNECTED TIME	
	<a href="#">HKO_A3w</a>	--	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".



The screenshot shows the AP WebUI configuration page for HKO\_A3w. The 'Status' tab is selected, displaying system and network information. The 'Status' section at the bottom shows 'Remote Mgmt: ON' and 'Status: Connected', with 'Connected' circled in red.


System	Network(Switch Mode)
<b>System Name:</b> HKO_A3w	<b>Ethernet</b>
<b>Product Name:</b> A3w	IPv4 DHCP Client: Disabled
<b>CPU Usage:</b> 20%	IPv4 Address: 192.168.100.30
<b>Memory Usage:</b> 40/236 MB (17%)	IPv4 Subnet Mask: 255.255.255.0
<b>Time of Day:</b> Thu Jul 13 17:04:18 2017	IPv4 Default Gateway: 192.168.100.1
<b>Uptime:</b> 1d 01h 27min 51s	IPv4 DNS Server: 10.6.127.4 8.8.8.8
	<b>Interfaces(4)</b>
	<b>Ethernet (eth0)</b>
	MAC: 00:19:be:a3:09:20
	Link: Auto (Full 100Mb/s)
	Transmit: 3.08MB (2.23Kbps)
	Receive: 15.99MB (7.23Kbps)
	<b>Ethernet (eth1)</b>
	MAC: 00:19:be:a3:09:20
	Link: Auto (Disconnected)
	Transmit: 0.00KB (0.00Kbps)
	Receive: 0.00KB (0.00Kbps)
	<b>Radio0(2.4G)</b>
	MAC: 00:19:be:a3:09:22
	Mode: AP

AP WebUI

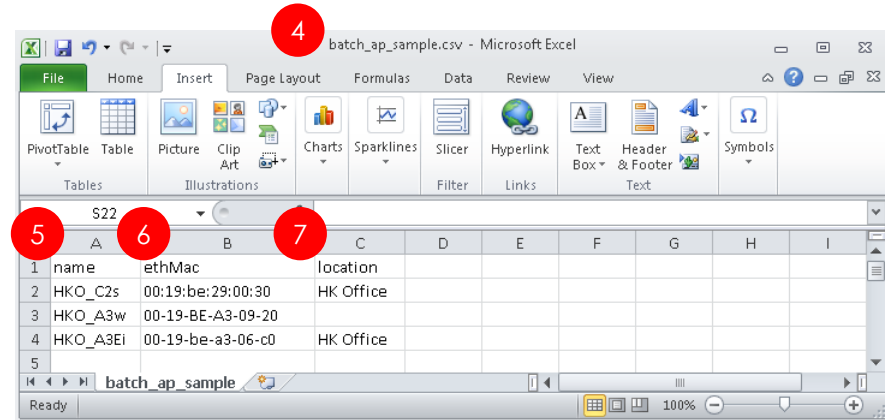
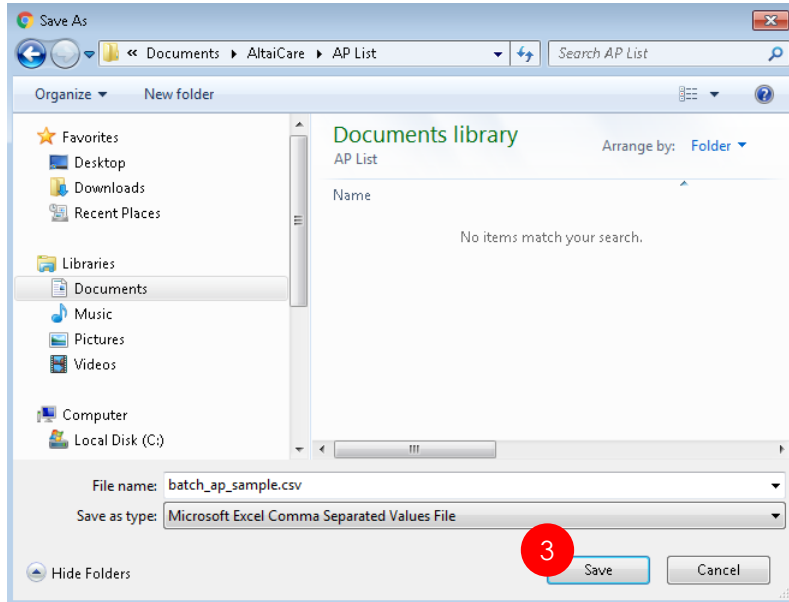
## Step 9b: AP Batch Registration

The screenshot displays the AltaiCare web interface. At the top, there are navigation tabs for WIRELESS, SERVICE, and PROJECT. The WIRELESS tab is selected. Below the navigation, the breadcrumb path is 'Altai Office > AP List'. A search bar contains 'AP' and a search icon. A red circle with the number '1' is positioned over the search bar. On the left sidebar, the 'NETWORK' menu is expanded, and 'Access Point' is selected, indicated by a red arrow. The main content area shows 'AP List' with a 'Show Filter' link. Below this, there is a table header with columns: STATUS, NAME, BRANCH, MODEL, ETHERNET MAC, SERIAL, IP ADDRESS, CHANNEL, ALERT, STATION, AVG RSSI, and LAST CONNECTED TIME. The table is currently empty, displaying 'No data available in table'. Below the table, it says 'Showing 1-0 of 0 entries' with a dropdown set to '10'. A modal dialog box titled 'IMPORT APS' is open in the center. It contains a label 'AP LIST FILE:' followed by a 'Choose File' button and the text 'No file chosen'. A red circle with the number '2' is positioned over the 'Choose File' button. Below the file selection area, there is a blue link labeled 'APs SAMPLE'. At the bottom of the dialog, there are 'IMPORT' and 'CANCEL' buttons.

### Procedures:

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

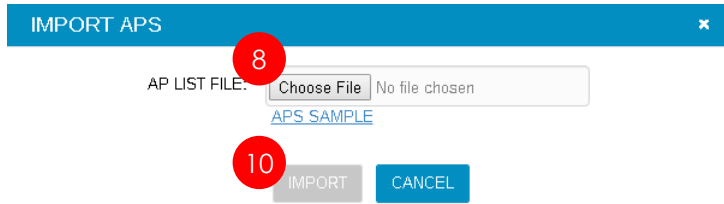
## Step 9b: AP Batch Registration (Cont.)



### Procedures:

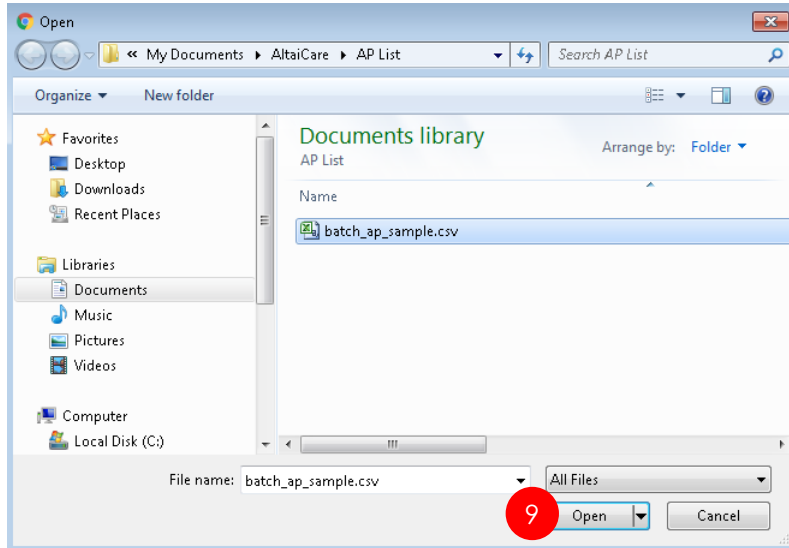
3. Click "Save" button.
4. Open the file "batch\_ap\_sample.csv".
5. Give a name for each AP.
6. Input the AP Ethernet MAC address in **colon-separated** or **hyphen-separated** format with either **uppercase** or **lowercase** alphabets, e.g. **XX:XX:XX:XX:XX:XX** or **xx-xx-xx-xx-xx-xx**
7. Enter AP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

## 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.



## 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	
	<a href="#">HKO_A3Ei</a>	..	..	00:19:be:a3:06:c0	..	..	..	0	2.4G: 0 5G: 0	2.4G: .. 5G: ..	..	
	<a href="#">HKO_A3w</a>	..	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	
	<a href="#">HKO_C2s</a>	..	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 >

System Configuration Administration Tools About

Overview Radio0(2.4G) Radio1(5G) Ethernet Logs

### System

System Name: HKO\_A3w  
Product Name: A3w  
CPU Usage: 20%  
Memory Usage: 40/236 MB (17%)  
Time of Day: Thu Jul 13 17:04:18 2017  
Uptime: 1d 01h 27min 51s

### Network(Switch Mode)

[More>>](#)

Ethernet

IPv4 DHCP Client: Disabled  
IPv4 Address: 192.168.100.30  
IPv4 Subnet Mask: 255.255.255.0  
IPv4 Default Gateway: 192.168.100.1  
IPv4 DNS Server: 10.6.127.4  
8.8.8.8

Interfaces(4)

Ethernet (eth0)

MAC: 00:19:be:a3:09:20 Transmit: 3.08MB (2.23Kbps)  
Link: Auto (Full 100Mb/s) Receive: 15.99MB (7.23Kbps)

Ethernet (eth1)

MAC: 00:19:be:a3:09:20 Transmit: 0.00KB (0.00Kbps)

### Status

Remote Mgmt: ON

Status: **Connected**

Connect Time: 1149 (s)

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 Firmware Update

# AP Firmware Compatibility Check

The screenshot shows the AltaiCare interface with the 'WIRELESS SERVICE' menu selected. The 'AP List' is displayed with one entry: HKO\_A3w. A red arrow points to the 'WIRELESS SERVICE' menu, and another red arrow points to the 'Access Point' option in the left sidebar. A red circle with a white exclamation mark is placed over the status icon of the HKO\_A3w entry. A blue callout box with a white border contains the text: 'Current AP firmware may not be fully compatible with AltaiCare, please upgrade to official AltaiCare version'. A mouse cursor is pointing at the warning icon. A note box on the right contains the text: '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.'

STATUS	NAME ^	BRANCH	MODEL	ETHERNET MAC	SERIAL	IP ADDRESS	CHANNEL	ALERT	STATION	AVG RSSI	LAST CONNECTED TIME	
	<a href="#">HKO_A3w</a>	--	A3w	00:19:be:a3:09:20	A3W053300009	223.255.161.226(WAN) 192.168.100.30(LAN)	Radio1: 1 Radio2: 36	6	2.4G: 0 5G: 0	2.4G: -- 5G: --	2017-07-18 00:23:54	

Showing 1-1 of 1 entries 10

# Single AP Firmware Update

The screenshot shows the AltaiCare management interface. At the top, there's a navigation bar with 'AltaiCare' logo, 'WIRELESS' tab, and 'SERVICE' sub-tab. Below this, the breadcrumb path is 'Altai Office > AP List'. A search bar contains 'AP'. The main content area displays an 'AP List' table with columns: STATUS, NAME, BRANCH, MODEL, ETHERNET MAC, SERIAL, IP ADDRESS, CHANNEL, ALERT, STATION, AVG RSSI, and LAST CONNECTED TIME. One AP entry is visible: HKO\_A3w, Model A3w, Ethernet MAC 00:19:be:a3:09:20, Serial A3W053300009, IP 223.255.161.226(WAN) and 192.168.100.30(LAN), Channel Radio1: 1, Radio2: 36, Alert 6, Station 2.4G: 0, 5G: 0, Avg RSSI 2.4G: --, 5G: --, Last Connected Time 2017-07-18 00:23:54. A red circle '1' highlights the 'Update Firmware' button in the AP's action menu. Below the table, a modal dialog titled 'UPDATE FIRMWARE' is open. It has a dropdown for 'FIRMWARE:' set to 'A3c\_2.1.0.1211 (Official)'. Below that, 'SCHEDULE START TIME:' has two options: 'NOW' (selected) and 'SPECIFIC TIME'. A red circle '2' is next to the firmware dropdown, '3a' is next to the 'NOW' radio button, and '4' is next to the 'UPDATE' button. The 'SPECIFIC TIME' section is also visible with 'SPECIFIC TIME:' set to '07/20/2017' and '03:00'.

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	6	2.4G: 0 5G: 0	2.4G: -- 5G: --	2017-07-18 00:23:54

Showing 1-1 of 1 entries 10

UPDATE FIRMWARE

FIRMWARE: A3c\_2.1.0.1211 (Official)


SCHEDULE START TIME:  NOW  SPECIFIC TIME

UPDATE CANCEL

SCHEDULE START TIME:  NOW  SPECIFIC TIME

SPECIFIC TIME: 07/20/2017 03:00

## 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.

# Single AP Firmware Update (Cont.)

### UPDATE FIRMWARE

FIRMWARE: A3c\_2.1.0.1211 (Official) ▼

SCHEDULE START TIME:  NOW  SPECIFIC TIME

\* Firmware task is scheduled. [Go to detail page.](#)

## 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.

## AltaiCare

WIRELESS SERVICE

Altai Office > Firmware Task List

DEFAULT SEARCH

### Firmware Update List

AP_NAME	FIRMWARE NAME	LAST UPDATE TIME	LAST UPDATE STATUS	NEXT SCHEDULE TIME	
HKO_A3w	A3c_2.1.0.1211	2017-07-18 01:29:48	Pending	--	Delete
--	A2c_2.1.0.1211	2017-07-13 23:45:31	Success	--	Delete
--	A3c_2.1.0.1211	2017-06-27 14:07:38	Success	--	Delete
--	A2c_2.1.0.1211	2017-06-17 17:58:29	Failed	--	Delete
--	A3c_2.1.0.1211	2017-06-08 11:12:18	Success	--	Delete

Showing 1-5 of 5 entries 10

AP_NAME	FIRMWARE NAME	LAST UPDATE TIME	LAST UPDATE STATUS	NEXT SCHEDULE TIME	
HKO_A3w	A3c_2.1.0.1211	2017-07-18 01:29:48	Success	--	Delete

# Single AP Firmware Update (Cont.)

The screenshot shows the AltaiCare WIRELESS SERVICE interface. The top navigation bar includes 'AltaiCare' and 'WIRELESS SERVICE'. The breadcrumb trail is 'Altai Office > AP List'. A search bar is present with 'AP' selected. The left sidebar menu is expanded to 'NETWORK', with 'Access Point' selected. The main content area displays an 'AP List' table with the following data:

STATUS	NAME	BRANCH	MODEL	ETHERNET MAC	SERIAL	IP ADDRESS	CHANNEL	ALERT	STATION	AVG RSSI	LAST CONNECTED TIME	
	<a href="#">HKO_A3w</a>	--	A3w	00:19:be:a3:09:20	A3W053300009	223.255.161.226(WAN) 192.168.100.30(LAN)	Radio2: 36 Radio1: 1	8	2.4G: 0 5G: 0	2.4G: -- 5G: --	2017-07-18 01:56:51	   

Below the table, it says 'Showing 1-1 of 1 entries' and '10'. A red circle with the number '8' points to the 'Access Point' menu item, and a red circle with the number '9' points to the 'HKO\_A3w' link in the table.

## Procedures:

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

# 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.

The screenshot displays the AltaiCare management interface for a specific AP. The interface is divided into several sections:

- Header:** AltaiCare logo, navigation tabs for WIRELESS and SERVICE, user profile [taylor], and search bar.
- Navigation:** DASHBOARD, NETWORK (with sub-items: Access Point, Wireless LAN, Security, Branch, Map, Firmware Update), SYSTEM, and SITE LIST.
- AP [ HKO\_A3w ] Dashboard Info:** Overview cards for STATIONS (2.4G / 5G), ALERTS (8), TODAY TRAFFIC (UL / DL), and CURRENT THROUGHPUT (UL / DL).
- Configuration Status:** A table listing key information:

LOCATION:	--
AP NAME:	HKO_A3w
AP STATUS:	Online
ETHERNET MAC:	00:19:be:a3:09:20
SERIAL NUMBER:	A3W053300009
LAST CONNECTED:	2017-07-18 02:07:34
IP ADDRESS:	223.255.161.226(WAN) / 192.168.100.30(LAN)
MODEL:	A3w
FIRMWARE VERSION:	2.1.0.1211
HARDWARE VERSION:	1.2
- Traffic:** A line graph showing traffic (MB) over the last 1 minute, with tabs for Upload and Download.

# 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.

The screenshot displays the AltaiCare interface for managing wireless services. The 'WIRELESS' tab is selected, and the 'AP List' page is shown. A search bar at the top right contains the text 'AP' and 'A8'. A dropdown menu below the search bar shows search results, with 'A8 aps' highlighted. A table of APs is visible below the search results, with columns for STATUS, NAME, BRANCH, MODEL, ETHERNET MAC, and SERIAL. The table lists several APs, including 'A2 Bridge Core 10.6.80.248', 'A2Ei Core 10.6.80.249', 'A8-Ein Bridge Photonics 10.8.80.242', 'A8-Ein Photonics 10.6.80.241', 'A8-Ein Photonics 10.6.80.243', 'C1an Core 10.6.80.251', and 'C1n Core 10.6.80.250'. Red arrows and numbers 1, 2, and 3 highlight the search process: 1 points to the 'WIRELESS' tab, 2 points to the search input field containing 'AP' and 'A8', and 3 points to the search results dropdown showing 'A8 aps'.

STATUS	NAME	BRANCH	MODEL	ETHERNET MAC	SERIAL
📶	<a href="#">A2 Bridge Core 10.6.80.248</a>	<a href="#">A2 bridge</a>	A2	00:19:be:70:9e:35	1A21550A0111
📶	<a href="#">A2Ei Core 10.6.80.249</a>	--	A2-Ei	00:19:be:70:a3:e3	1A21541C0030
📶	<a href="#">A8-Ein Bridge Photonics 10.8.80.242</a>	<a href="#">A8 bridge</a>	A8-Ein	00:19:be:20:10:d4	1AN13033A013
📶	<a href="#">A8-Ein Photonics 10.6.80.241</a>	--	A8-Ein	00:19:be:20:0c:25	1AN124430087
📶	<a href="#">A8-Ein Photonics 10.6.80.243</a>	--	A8-Ein	00:19:be:20:10:fa	1AN13033A011
📶	<a href="#">C1an Core 10.6.80.251</a>	--	C1an	00:19:be:a2:15:96	C1AN152800394
📶	<a href="#">C1n Core 10.6.80.250</a>	--	C1n	00:19:be:a1:45:42	C1N153000774

# AP Batch Firmware Update (Cont.)

## Procedures:

- In this example, the result shows and filter out the A8n series products only based on the keyword "A8".
- Check the box in the header row and all the boxes will then be checked automatically.
- Hit the button "Firmware Update".
- 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.

Altai Free WiFi > Search Result List

AP SEARCH

### Search Result List (AP)

Batch Actions: [Reboot](#) [Firmware Update](#) [Add To Branch](#)

<input checked="" type="checkbox"/>	STATUS	NAME	LOCATION	ETH MAC	SERIAL	WAN IP	MODEL	
<input checked="" type="checkbox"/>	Online	A8-Ein Photonics 10.6.80.241	--	00:19:be:20:0c:25	1AN124430087	223.255.161.226	A8-Ein	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<input checked="" type="checkbox"/>	Online	A8-Ein Photonics 10.6.80.243	--	00:19:be:20:10:fa	1AN13033A011	223.255.161.226	A8-Ein	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>
<input checked="" type="checkbox"/>	Online	A8-Ein Bridge Photonics 10.8.80.242	--	00:19:be:20:10:d4	1AN13033A013	223.255.161.226	A8-Ein	<a href="#">Dashboard</a> <a href="#">Edit</a> <a href="#">Delete</a>

Showing 1-3 of 3 entries

### 7 UPDATE FIRMWARE

FIRMWARE: A8n\_2.1.0.1211

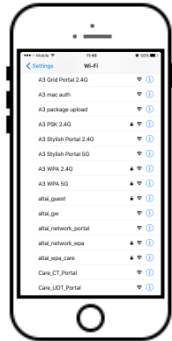
SCHEDULE START TIME:  NOW  SPECIFIC TIME

[UPDATE](#) [CANCEL](#)

## Verification (Custom Template Portal)

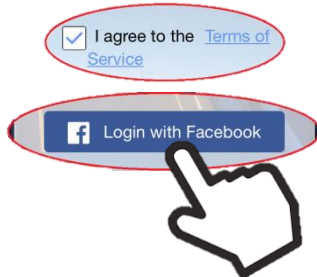
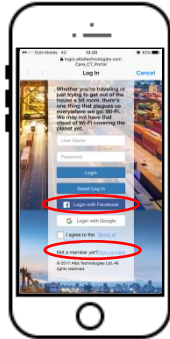
# Verification: Custom Template Portal (Facebook Account Login – iOS Device)


1



Turn on WiFi and Select SSID

2

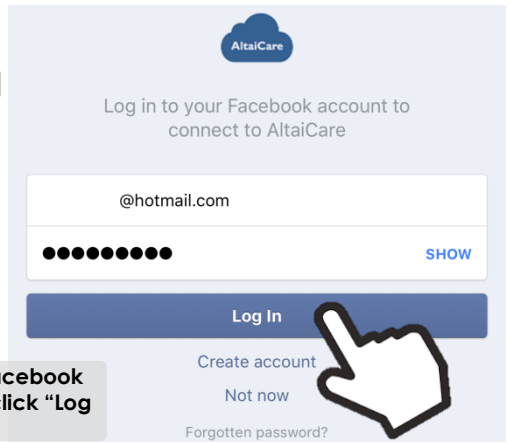


Portal Page pops up. Check the box and agree the Terms of Service. Then click  Facebook Login Button

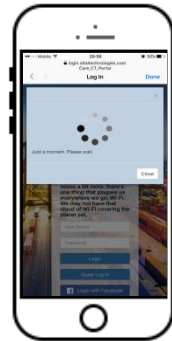
3



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



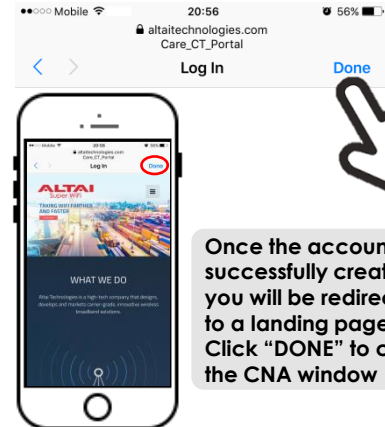
4



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

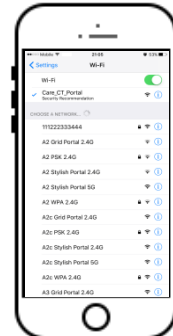
- # Basic personal Information include:
- Facebook Username
  - Email
  - Age Range (i.e. <21 or >21)
  - Gender
  - Locale

5

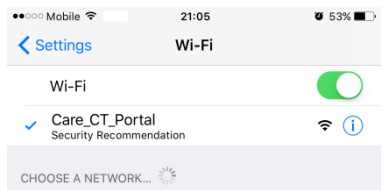


Once the account is successfully created, you will be redirected to a landing page. Click "DONE" to close the CNA window

6



**DONE!** You are now connected with Care WiFi! Enjoy it 😊



# Verification: Custom Template Portal (Facebook Account Login)

AltaiCare WIRELESS SERVICE [taylor]

Altai Hotspot Service > User Account List USER ACCOUNT SEARCH

User Account List Show Filter

Batch Actions: Remove All

USER LOGIN NAME	NAME	USER GROUP NAME	REMAINING DATA QUOTA (MB)	EMAIL	PHONE / MOBILE	EXPIRY TIME	LAST LOGIN TIME
<a href="#">auto_dc37142caec8</a>	Taylor Yiu Ming Wan	Guest Group	500	--	--/--	2017-07-08 18:17:50	2017-07-08 16:17:50

Showing 1-1 of 1 entries 10

Dashboard Edit Delete

- 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**

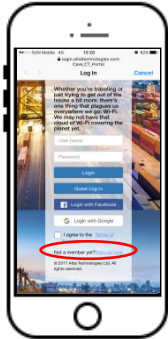
# Verification: Custom Template Portal (Email Sign Up with Passcode Return – iOS Device)

1



Turn on WiFi and Select SSID

2

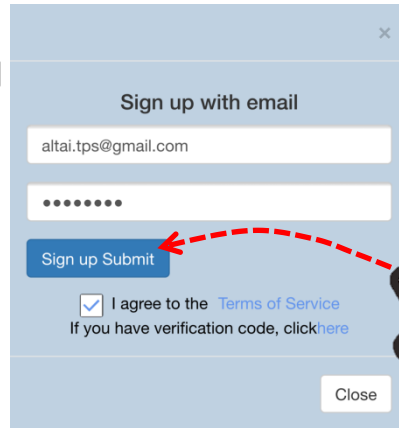
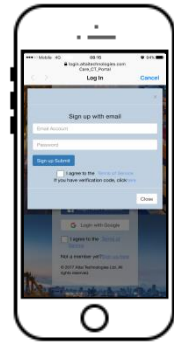


Not a member yet? [Sign up here](#)



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

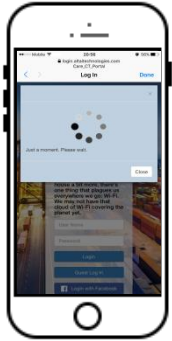
3



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

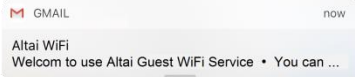
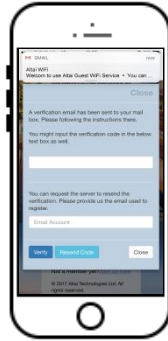


4



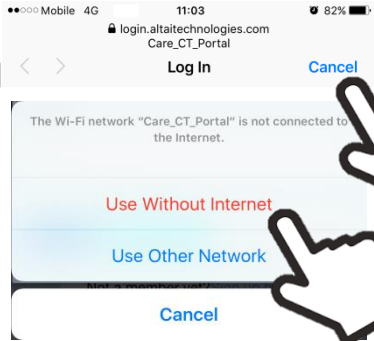
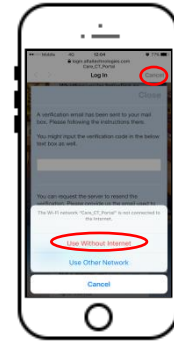
Upon click on "Sign up Submit" button, you will have 2 min for Internet access. In this time window, AltaiCare will generate passcode and send verification Email to your account. You are required to submit the code back in this timeslot for system verification and get Internet access

5

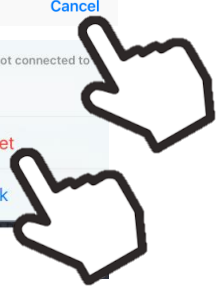


You will receive Email with verification code from AltaiCare System shortly

6

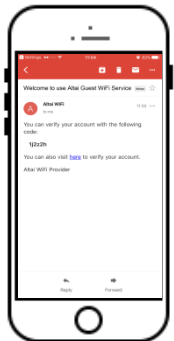


Click "Cancel" to close the CNA window and then click "Use Without Internet"



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

7



Altai WiFi  
to me

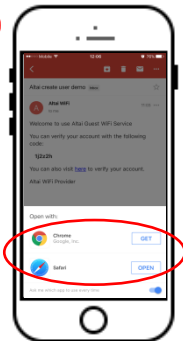
You can verify your account with the following code:  
**1j2z2h**

You can also visit [here](#) to verify your account.  
Altai WiFi Provider



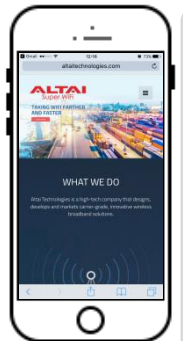
Open the Email and click the URL to send the passcode back to the system for verification

8a



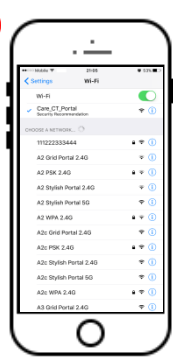
Open a browser and send the URL

9

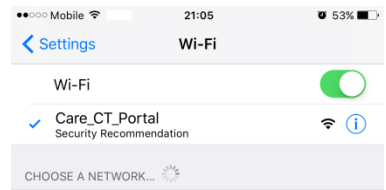


Once the code is verified OK, AltaiCare will automatically generate a user account using your registered email as username for you. In the meanwhile,

10



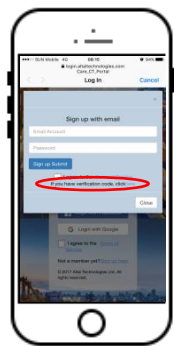
**DONE!** You are now connected with Care WiFi! Enjoy it 😊



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

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

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

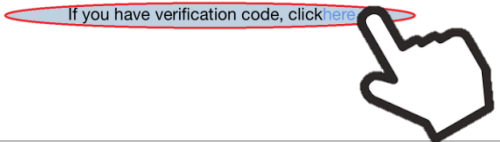
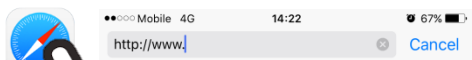
8b



Enter the verification code and click "Verify" button

Please input the verification code in the text box below.

You can request the server to resend the verification. Please provide us the email used to register.



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

The screenshot shows the AltaiCare management interface. The top navigation bar includes 'WIRELESS' and 'SERVICE' (highlighted with a red arrow). The main content area is titled 'User Account List' and contains a table with the following columns: USER LOGIN NAME, NAME, USER GROUP NAME, REMAINING DATA QUOTA (MB), EMAIL, PHONE / MOBILE, EXPIRY TIME, and LAST LOGIN TIME. A 'Batch Actions: Remove All' button is located above the table. The table contains one entry with the following data: USER LOGIN NAME: altai.tps@gmail.com (callout 1), NAME: auto\_dc37142caec8 (callout 2), USER GROUP NAME: Guest Group (callout 3), REMAINING DATA QUOTA (MB): 500 (callout 4), EMAIL: altai.tps@gmail.com (callout 5), PHONE / MOBILE: -- / -- (callout 6), EXPIRY TIME: 2017-07-08 18:26:59 (callout 7), and LAST LOGIN TIME: 2017-07-08 16:26:59 (callout 8). A 'Dashboard' button and 'Edit'/'Delete' icons are visible at the bottom right of the table row. The left sidebar shows a navigation menu with 'User Account' selected (callout 1).

USER LOGIN NAME	NAME	USER GROUP NAME	REMAINING DATA QUOTA (MB)	EMAIL	PHONE / MOBILE	EXPIRY TIME	LAST LOGIN TIME
altai.tps@gmail.com	auto_dc37142caec8	Guest Group	500	altai.tps@gmail.com	-- / --	2017-07-08 18:26:59	2017-07-08 16:26:59

**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

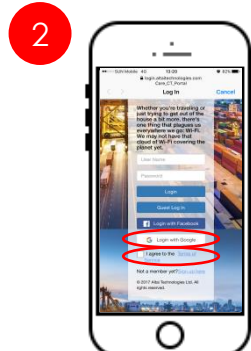
**7. Expiry Time:** Account validity which is counted from the Start at the first login. (See Configuration Step 5 for account validity setting)

**8. Last Login Time**


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




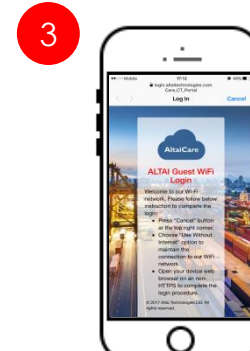
Turn on WiFi and Select SSID



I agree to the [Terms of Service](#)

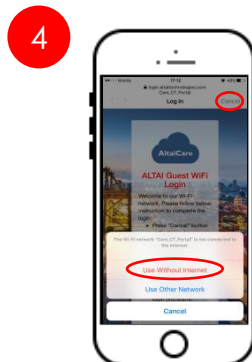
 Login with Google

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



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

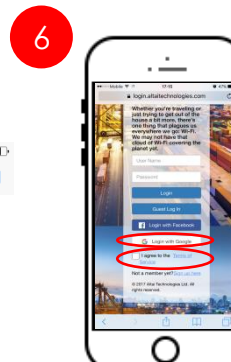
#The system pops up the instruction page for Google login in iOS device by default, no matter whether the CNA detection is enabled or not




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



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

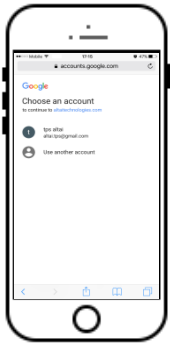


Same as Step #2. Check the box again and agree the Terms of Service. Then click 

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

7

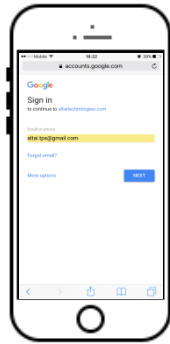
Sign up with Google account



Choose an account to continue to [altaitechnologies.com](#)

t tps altai  
alta.tps@gmail.com

Use another account



Sign in to continue to [altaitechnologies.com](#)

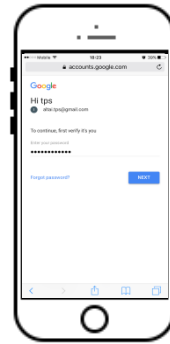
Email or phone

alta.tps@gmail.com

Forgot email?

More options

NEXT



Hi tps  
Hi tps @alta.tps@gmail.com

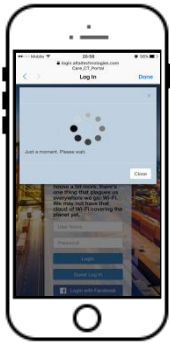
To continue, first verify it's you

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

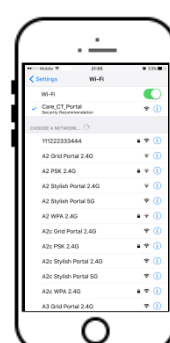
- # Basic personal information include:
- Username
  - Email
  - Gender

9

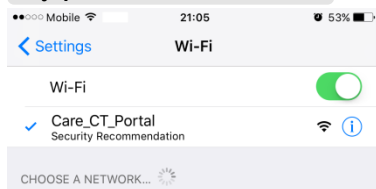


Once the account is successfully created, you will be redirected to a landing page.

10



**DONE! You are now connected with Care WiFi!**  
Enjoy it 😊



# Verification: Custom Template Portal (Google Account Login)

AltaiCare WIRELESS SERVICE

Altai Hotspot Service > User Account List

USER ACCOUNT SEARCH

User Account List Show Filter

Batch Actions: Remove All

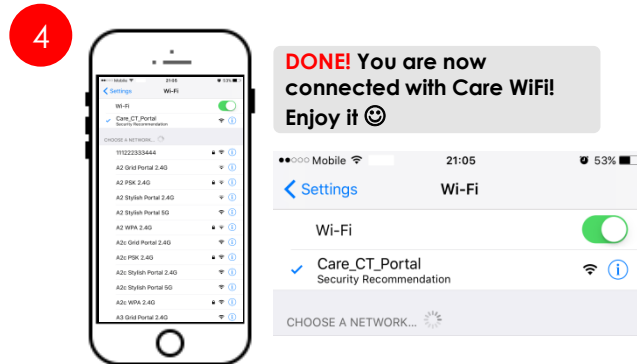
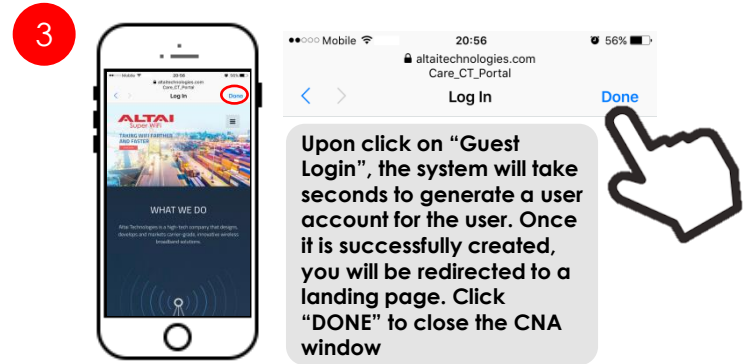
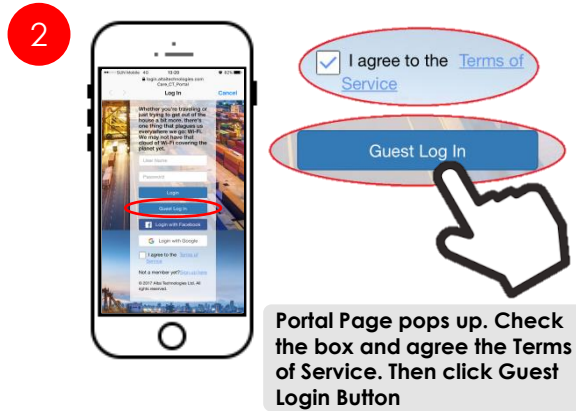
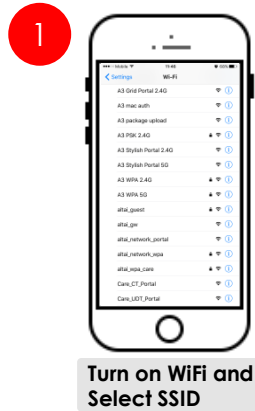
USER LOGIN NAME	NAME	USER GROUP NAME	REMAINING DATA QUOTA (MB)	EMAIL	PHONE / MOBILE	EXPIRY TIME	LAST LOGIN TIME
auto_dc37142caec8	altai_tps	Guest Group	500	altai.tps@gmail.com	--	2017-07-08 19:19:56	2017-07-08 17:19:56

Showing 1-1 of 1 entries 10

1 2 3 4 5 6 7 8

- 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)



## Verification (User Defined Template Portal)

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

1

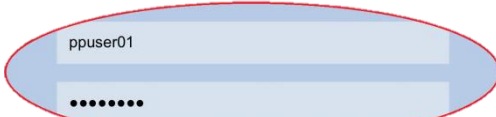


Turn on WiFi and Select SSID

2

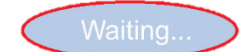


Portal Page pops up. Enter your #account Username/Password. Then click Login Button

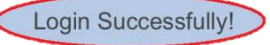


#Note: We only allowed the user group "PP User Group" for user authentication and connection with the SSID "Care\_UDT\_Portal" in our setup, so we use the user account "ppuser01/ppuser01" for portal login

3



...1-2 sec later



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

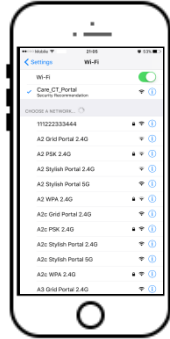
4



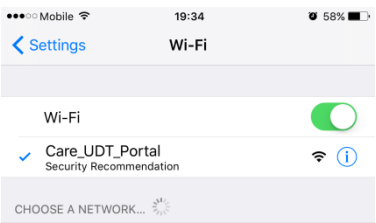
The system will soon redirect you to a landing page. Click "DONE" to close the CNA window



5



**DONE!** You are now connected with Care WiFi! Enjoy it 😊



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

AltaiCare WIRELESS SERVICE PROJECT

Altai WiFi Service > User Account List

USER ACCOUNT SEARCH

User Account List Show Filter

Batch Actions: Remove All

USER LOGIN NAME	NAME	USER GROUP NAME	REMAINING DATA QUOTA (MB)	EMAIL	PHONE / MOBILE	EXPIRY TIME	LAST LOGIN TIME
<a href="#">ppuser01</a>	ppuser01	PP User Group	494	--	-- / --	2017-07-17 21:30:50	2017-07-17 19:31:00

Showing 1-1 of 1 entries 10

- 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!".



Login Successfully!

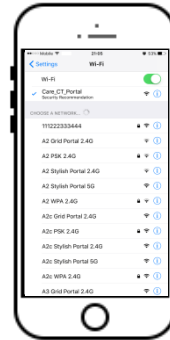
4



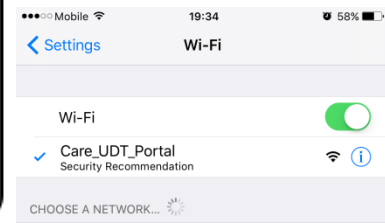
The system will soon redirect you to a landing page. Click "DONE" to close the CNA window



5



**DONE!** You are now connected with Care WiFi! Enjoy it 😊



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

The screenshot shows the AltaiCare interface for the 'User Account List'. The table contains one entry with the following data:

USER LOGIN NAME	NAME	USER GROUP NAME	REMAINING DATA QUOTA (MB)	EMAIL	PHONE / MOBILE	EXPIRY TIME	LAST LOGIN TIME
<a href="#">auto_dc37142caec8</a>	auto_dc37142caec8	Guest Group	500	--	--/--	2017-07-17 22:51:08	2017-07-17 20:51:08

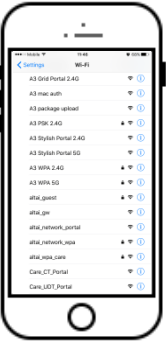
Numbered callouts (1-8) point to the following fields:

- 1. User Login Name
- 2. Name
- 3. User Group Name
- 4. Remaining Data Quota (MB)
- 5. Email
- 6. Phone / Mobile
- 7. Expiry Time
- 8. Last Login Time

The legend on the right provides the following definitions:

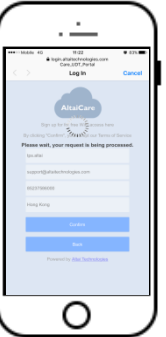
- 1. Auto-generated User Account:** Client MAC address with "auto\_" prefix
- 2. Account Name:** Client MAC address with "auto\_" prefix
- 3. User Group:** The user group to which this auto-generated user account is assigned (See Configuration Step 7b)
- 4. Remaining Data Quota:** See Configuration Step 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**

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


**1**  Turn on WiFi and Select SSID

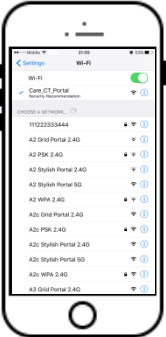
**2**  Portal Page pops up. Then click Sign-Up button

**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 😊**

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

The screenshot shows the AltaiCare management interface. The top navigation bar includes 'AltaiCare', 'WIRELESS', and 'SERVICE'. The main content area is titled 'Altai WiFi Service > User Account List'. A search bar and a 'USER ACCOUNT' dropdown are visible. On the left, a sidebar menu contains 'DASHBOARD', 'USER', 'PORTAL', 'ADVERTISEMENT', 'SYSTEM', and 'DOMAIN LIST'. The 'USER' menu is expanded, showing 'User Group', 'User Account', and 'Account Generation'. The 'User Account List' table has the following columns: USER LOGIN NAME, NAME, USER GROUP NAME, REMAINING DATA QUOTA (MB), EMAIL, PHONE / MOBILE, EXPIRY TIME, and LAST LOGIN TIME. A single entry is shown with the following data: USER LOGIN NAME: auto\_dc37142caec8, NAME: tps.altai, USER GROUP NAME: Guest Group, REMAINING DATA QUOTA (MB): 500, EMAIL: support@altaitechnologies.com, PHONE / MOBILE: Hong Kong / 85237586000, EXPIRY TIME: 2017-07-18 14:51:59, LAST LOGIN TIME: 2017-07-18 12:51:59. Red circles with numbers 1 through 8 are placed over the table cells to indicate key information: 1 (User Login Name), 2 (Name), 3 (User Group Name), 4 (Remaining Data Quota), 5 (Email), 6 (Phone / Mobile), 7 (Expiry Time), and 8 (Last Login Time). Below the table, it says 'Showing 1-1 of 1 entries' and '10' items per page. On the right side of the table, there are 'Dashboard', 'Edit', and 'Delete' buttons.

USER LOGIN NAME	NAME	USER GROUP NAME	REMAINING DATA QUOTA (MB)	EMAIL	PHONE / MOBILE	EXPIRY TIME	LAST LOGIN TIME
1 auto_dc37142caec8	2 tps.altai	3 Guest Group	4 500	5 support@altaitechnologies.com	6 Hong Kong / 85237586000	7 2017-07-18 14:51:59	8 2017-07-18 12:51:59

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)

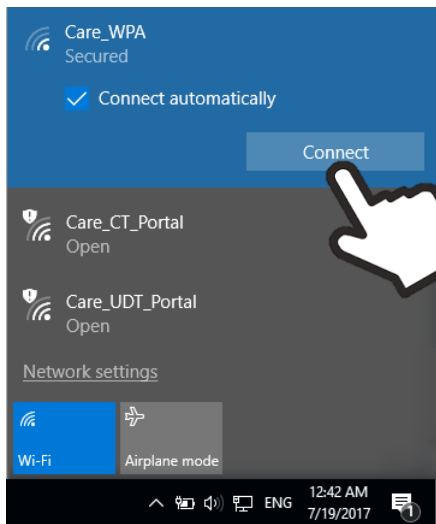
8. **Last Login Time**

## Verification (WPA – PEAP)

# Verification: WPA (PEAP – Windows 10 Client)

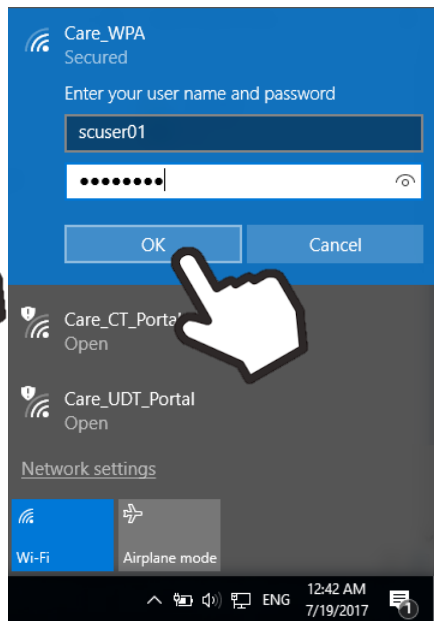
1

Turn on WiFi and Select SSID, i.e. Care\_WPA for our case. Check the box of “Connect automatically” and click “Connect”



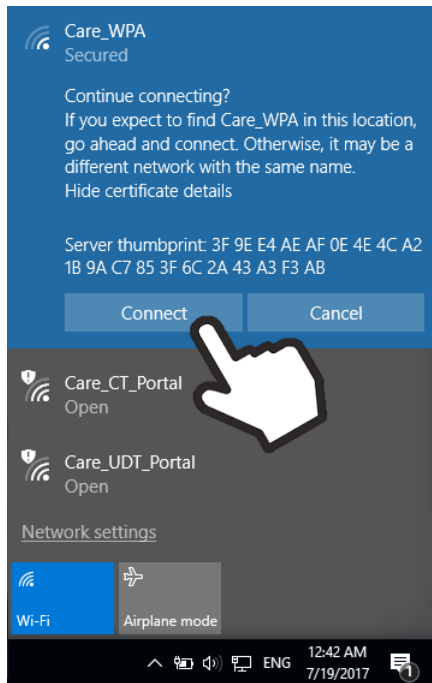
2

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



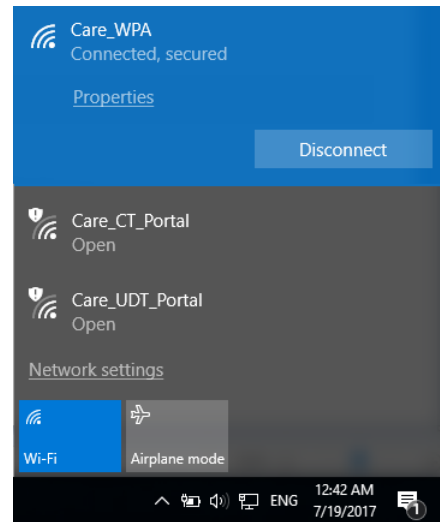
3

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 😊

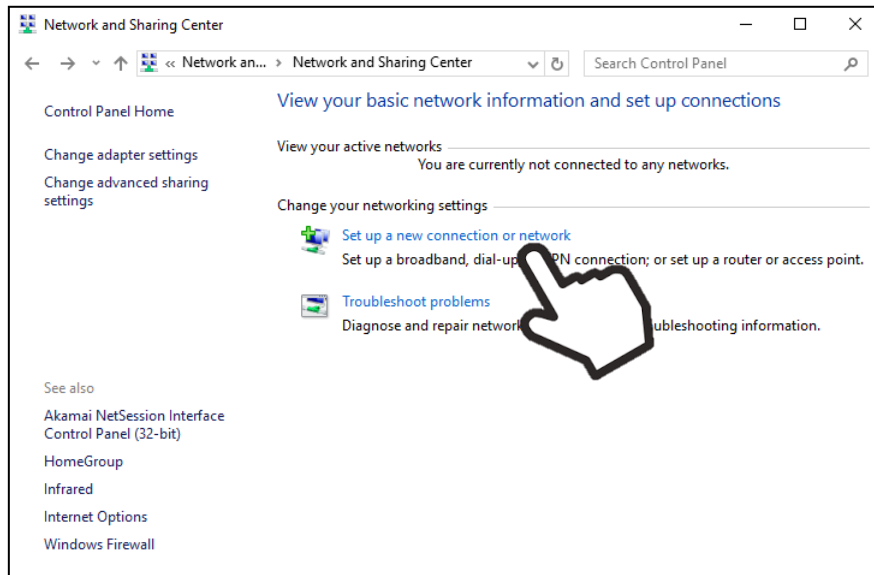


# Verification: WPA (PEAP – Windows 10 Client)



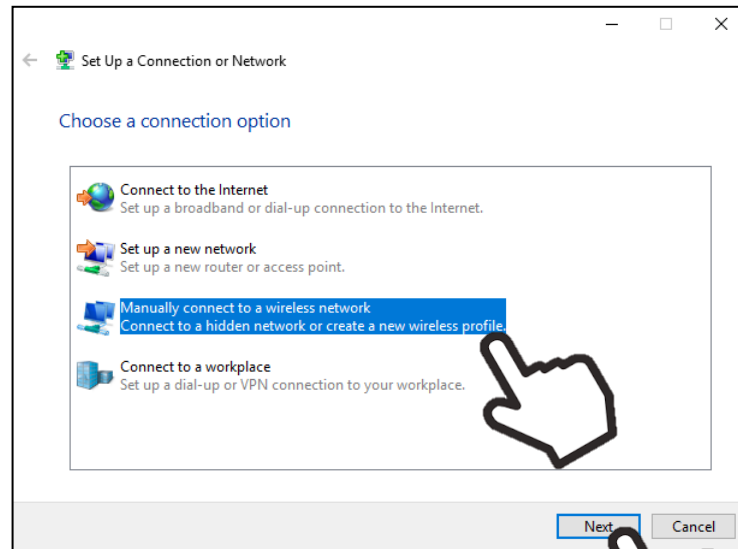
Note: In some of the cases such as hidden network, you may need to manually create wireless profile for connection to the wireless network.

1



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

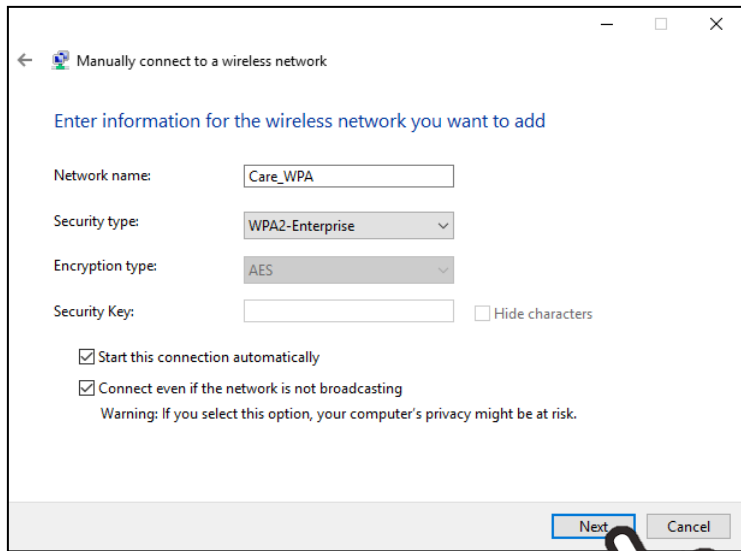
2



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

# Verification: WPA (PEAP – Windows 10 Client)

3



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:

Security type:

Encryption type:

Security Key:   Hide characters

Start this connection automatically

Connect even if the network is not broadcasting

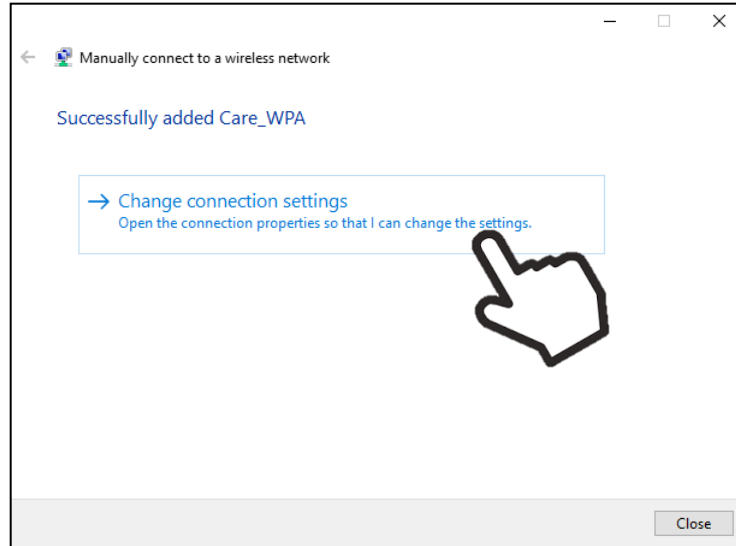
Warning: If you select this option, your computer's privacy might be at risk.

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



Manually connect to a wireless network

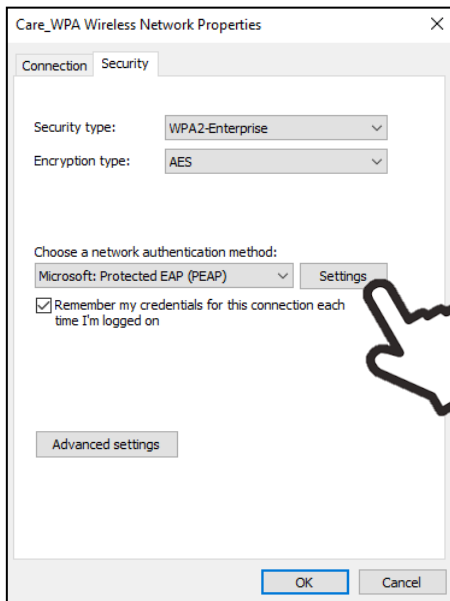
Successfully added Care\_WPA

[→ Change connection settings](#)  
Open the connection properties so that I can change the settings.

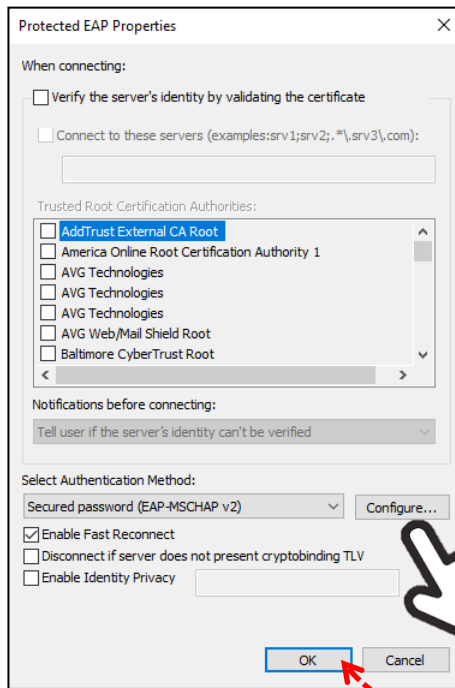
The wireless profile for SSID, i.e. **“Care\_WPA”** has just been created. Click **“Change connection settings”** for further configuration changes

# Verification: WPA (PEAP – Windows 10 Client)

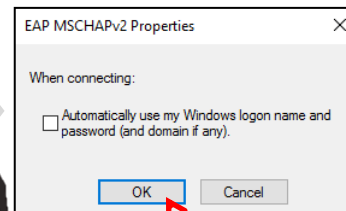
5



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



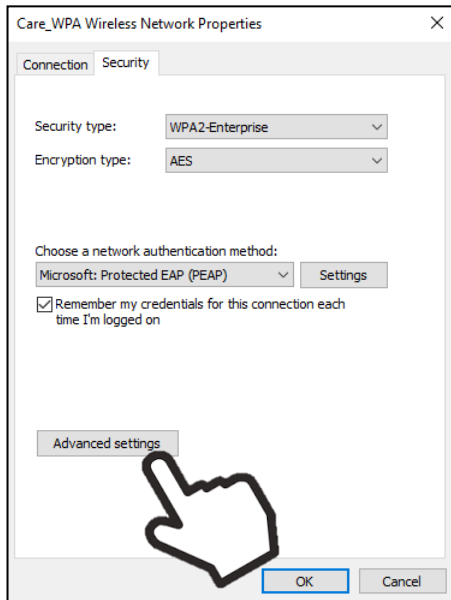
Uncheck the box of “Verify the server’s identity by validating the certificate”. Select “EAP-MSCHAP v2” as Authentication Method and then click “Configure...” for further changes



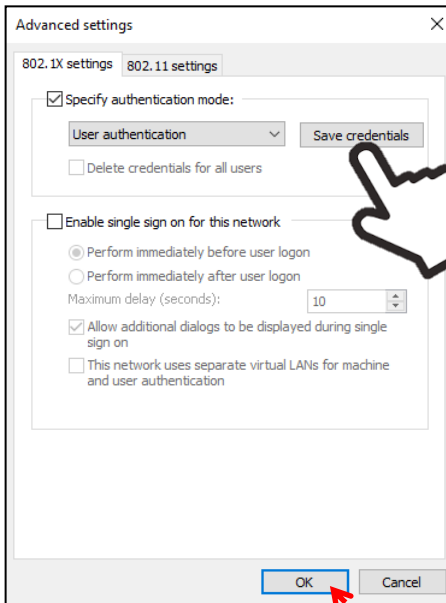
Uncheck the box of “Automatically use my Windows logon name and password (and domain if any).” and then click “OK” to go back to “Protected EAP Properties” Window. Click “OK” again to go back to “Wireless Network Properties” window

# Verification: WPA (PEAP – Windows 10 Client)

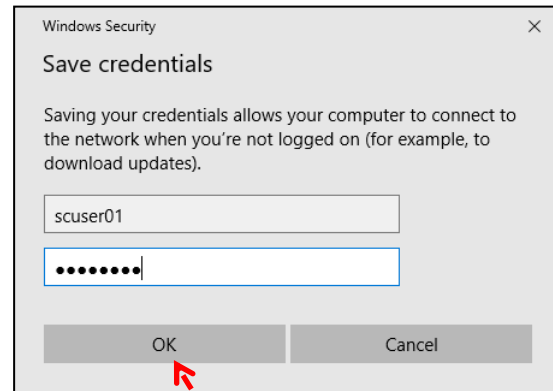
6



Click "Advanced settings"



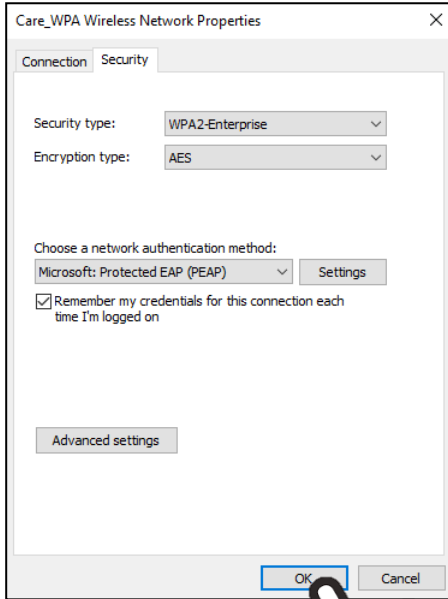
Click the tab "802.1X settings" and choose "User authentication" as authentication mode. Then click "Save credentials"



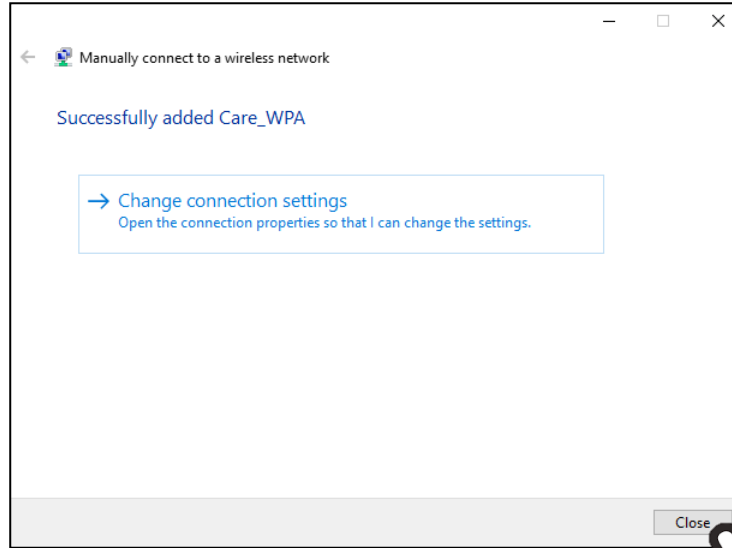
Input username and password. Then click "OK" to go back to "Advanced settings" window. Click "OK" again to go back to "Wireless Network Properties" window.

# Verification: WPA (PEAP – Windows 10 Client)

7

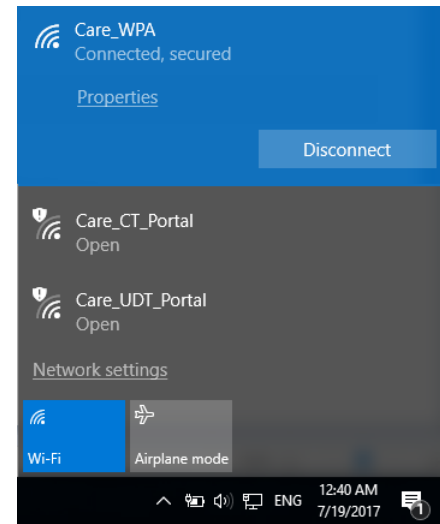


Click "OK" to close "Wireless Network Properties" window



Click "Close" to finish the wireless network profile setting

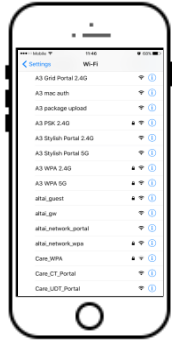
8



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

# Verification: WPA (PEAP – iOS Device)

1



Care\_WPA

Turn on WiFi and Select SSID, i.e. Care\_WPA for our case



2



Enter the password for "Care\_WPA"

Cancel

Enter Password

Join

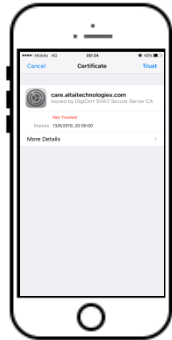
Username scuser01

Password \*\*\*\*\*

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



3



Cancel

Certificate

Trust



care.altatechnologies.com

Issued by DigiCert SHA2 Secure Server CA

Not Trusted

Expires 13/6/2019, 20:00:00

More Details



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

4



Settings

Wi-Fi

Wi-Fi

Care\_WPA

CHOOSE A NETWORK...

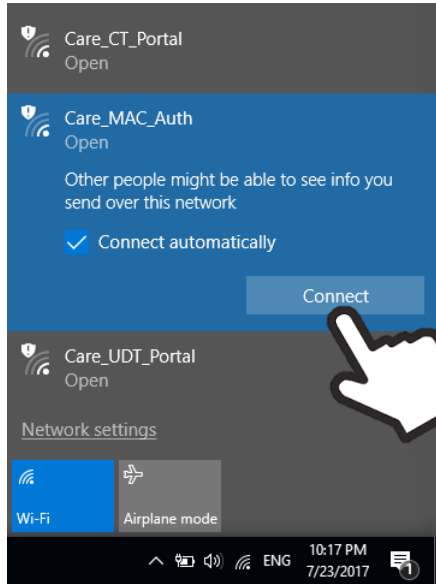
**DONE!** You are now connected with Care WiFi! Enjoy it 😊

## Verification (MAC Authentication)

# Verification: MAC Auth (Windows 10 Client)

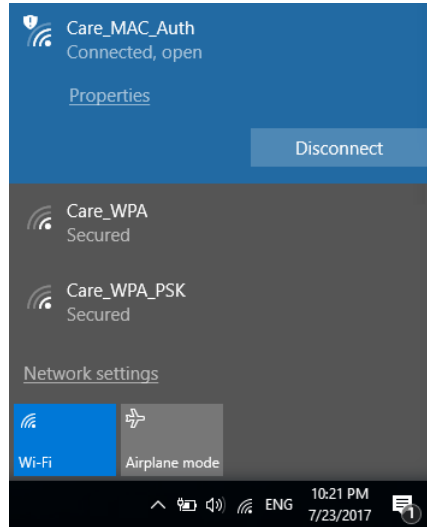
1

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



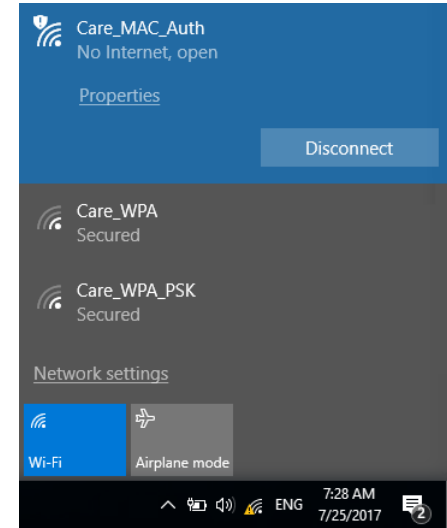
2a

**DONE!** You are now connected with Care WiFi! Enjoy it 😊



2b

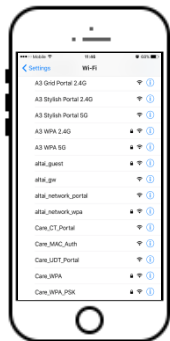
For those clients which are not in the registered MAC addresses list of the allowed user group(s), they will not be allowed to get Internet access



## Verification (WPA-PSK)

# Verification: WPA-PSK (iOS Device)

1



Care\_WPA\_PSK



Turn on WiFi and Select SSID, i.e. Care\_WPA\_PSK for our case

2



Enter the password for "Care\_WPA\_PSK"

Cancel

Enter Password

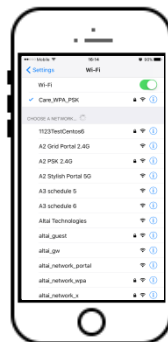
Join

Password ●●●●●●

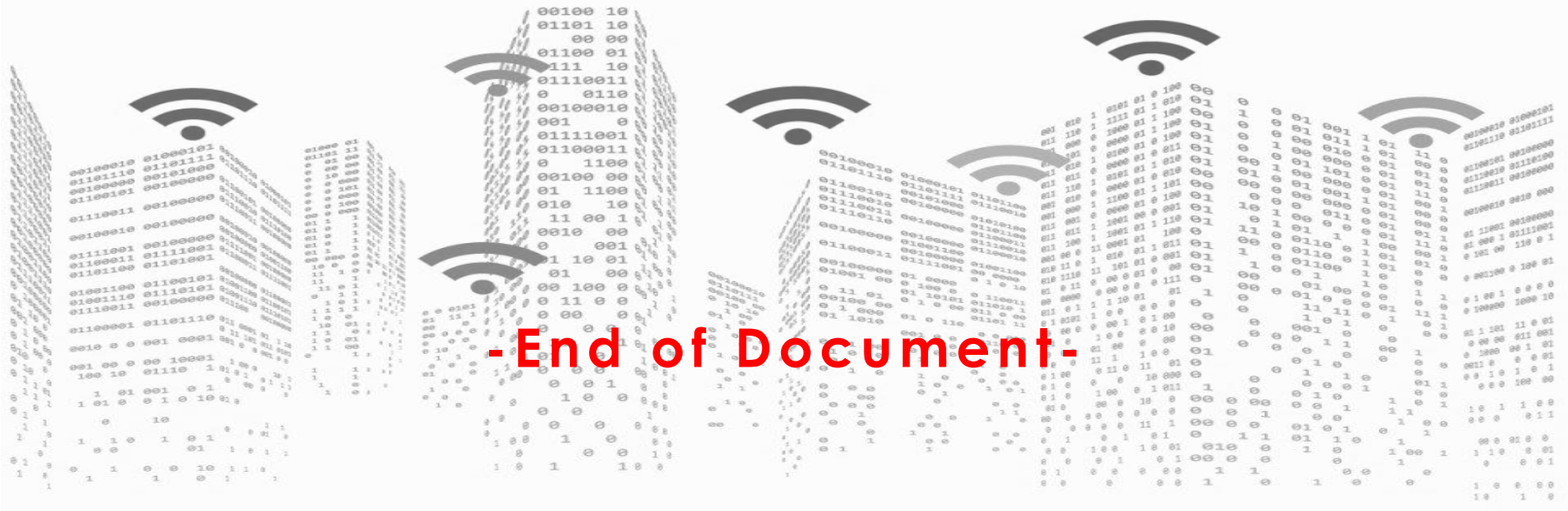


Enter the Password and then click "Join"

3



**DONE!** You are now connected with Care WiFi! Enjoy it 😊



Copyright © 2017 Altai Technologies Limited

ALL RIGHTS RESERVED.

**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.altaittechnologies.com](http://www.altaittechnologies.com)

**Customer Support Centre:**  
Email: [support@altaittechnologies.com](mailto:support@altaittechnologies.com)

