

HIRSCHMANN IT

A **BELDEN** BRAND

DAC User Manual

User manual

Technical Support

Release 01 08/2022

<http://www.belden.com>

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2022, Belden Singapore Pte Ltd

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Belden according to the best of the company's knowledge. Belden reserves the right to change the contents of this document without prior notice. Belden can give no guarantee in respect of the correctness or accuracy of the information in this document.

Belden can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann IT product site (www.belden.com).

Safety Agreement

Safety location

By default, device should be placed in certain location that is safe, stable and reliable; all physical operators should be authorized; the operation CLI scripts should be properly kept, updated and reviewed.

Safety Channel

Hirschmann IT devices support multiple managing methods, including SSH, HTTPS. All un-encrypted management protocols are not recommended. We highly recommend that our user only use SSH and HTTPS as the way to operate the devices, in order to ensure all management traffic is encrypted.

Safety Storage

The login credentials, device configuration and status data should be kept in an appropriate place and be updated regularly and this information can only be accessed and managed by authorized people.

Table of Contents

SAFETY AGREEMENT	2
1. ABOUT THIS MANUAL	1
1.1. ABOUT DAP	1
1.2. ABOUT DAC.....	1
2. SET UP A DAC.....	3
2.1. SYSTEM REQUIREMENT	3
2.2. DAC INSTALLATION.....	4
2.3. DAC UPGRADE	4
3. SET UP A DAP	5
3.1. CLASSIC NETWORK TOPOLOGY	5
3.2. CONNECTING TO NETWORK	6
3.3. ASSIGN IP ADDRESS.....	6
3.4. REGISTER DAP TO DAC	7
3.4.1. DISCOVER DAC BY DHCP OPTIONS.....	7
3.4.2. CONFIGURING DAC IP ADDRESS FROM DAP WEBSITE	7
4. GETTING START WITH DAC	8
4.1. LOGIN WITH DEFAULT ACCOUNT ADMIN.....	8
4.1.1. CHANGE DEFAULT PASSWORD FOR ACCOUNT ADMIN	9
4.2. START WITH WIZARD.....	9
4.2.1. FIRST STEP	9
4.2.2. SECOND STEP	10
4.2.3. THIRD STEP	11
4.2.4. FOURTH STEP	12
4.2.5. LAST STEP	13
4.3. NETWORK STRUCTURE	14
4.3.1. CREATE A NEW SITE.....	14
4.3.2. CREATE A NEW GROUP	15
4.3.3. CREATE A NEW CORPORATE	15
4.3.4. JOIN A SITE TO A CORPORATE.....	16
4.4. ACCOUNT MANAGEMENT	17
4.4.1. ADD SMTP SERVER	18
4.4.2. CREATE ACCOUNT.....	19

4.4.3. CHANGE PASSWORD	20
4.4.4. FORGET PASSWORD	21
4.5. ADMINISTRATOR PRIVILEGES	21
4.5.1. ADD AUTHORIZATION FOR SITE	23
4.5.2. REMOVE AUTHORIZATION FOR SITE	23
5. DAC USER INTERFACE INTRODUCTION	24
5.1. BANNER TOOLS	24
5.2. CONFIGURATION/DISPLAY ICONS	25
5.3. WORKING WITH TABLES	27
5.4. USER HOME PAGE	28
5.4.1. HOME	29
5.4.2. MY DEVICE	29
5.4.3. AP DEVICE	30
5.4.4. ASSIGN DAPS TO A SITE/GROUP	30
5.4.5. AP LOCAL FIRMWARE MANAGEMENT	31
5.4.6. AP CONNECTIVITY HISTORY	31
5.5. SITE VIEW	32
5.5.1. DASHBOARD	33
5.5.2. WLAN	35
5.5.3. AP	35
5.5.4. CLIENTS	35
5.5.5. AUTHENTICATION	35
5.5.6. RF	35
5.5.7. LOG	36
5.5.8. SECURITY	36
5.5.9. GROUP	36
5.5.10. SETTING	37
5.6. GROUP VIEW	38
5.6.1. DASHBOARD	38
5.6.2. WLAN	40
5.6.3. AP	40
5.6.4. CLIENTS	40
5.6.5. AUTHENTICATION	40
5.6.6. RF	41
5.6.7. LOG	41
5.6.8. SECURITY	41
5.6.9. SETTING	41

6. LICENSE	43
6.1. LICENSE ACTIVATION	44
6.2. LICENSE MANAGEMENT	46
6.3. LICENSE RECORD	46
6.4. DEVICE CODE.....	47
7. WLAN.....	48
7.1. SECURITY LEVEL	49
7.2. MAC AUTHENTICATION	49
7.3. CREATE WLAN.....	49
7.3.1. SSID SETTING.....	50
7.3.2. QOS SETTINGS.....	54
7.3.3. BROADCAST/MULTICAST OPTIMIZATION SETTINGS	56
7.4. EDIT WLAN.....	57
7.5. DELETE WLAN	57
8. AP.....	58
8.1. DEVICE LIST	59
8.2. CONFIGURATIONS FOR AP	60
8.2.1. DATAGRAM FRAGMENTATION.....	60
8.2.2. TURN ON/OFF IGMP SNOOPING	60
8.2.3. TURN ON/OFF TELNET	61
8.2.4. TURN ON/OFF LED	61
8.2.5. TURN ON/OFF USB.....	61
8.2.6. FIRMWARE MANAGEMENT	61
8.2.7. DEVICE SYSLOG CONFIG	63
8.2.8. CONFIGURE NTP OF DEVICE	63
8.2.9. ACCESS TO AP WEB UI.....	63
8.2.10. ASSIGN APS TO GROUP	64
8.2.11. PMD	64
8.2.12. REVERSE SSH	65
8.3. CONFIGURE BLUETOOTH.....	66
8.3.1. BLUETOOTH CONFIGURATIONS	66
8.3.2. CONFIG BLUETOOTH WLAN UPLINK.....	67
8.4. REPORTING CONFIG	68
8.5. OPERATION TOOLS	69
8.5.1. CONNECTIVITY TEST.....	69

8.5.2. REBOOT A DEVICE	69
8.5.3. LOG SNAPSHOT	69
8.5.4. EXPORT ALL DEVICE	70
8.6. DO ACTIONS FROM AP	70
8.6.1. SHOW SYSTEM INFO	70
8.6.2. SHOW WIFI INFO	71
8.6.3. SHOW HISTORY SYSLOG INFO	71
8.6.4. TCPDUMP	72
8.6.5. TRACEROUTE	72
8.6.6. PING	73
8.6.7. SHOW HISTORY RESET REASON	73
8.7. DEVICE CONNECTION RECORD	74
9. CLIENTS	75
9.1. ONLINE CLIENTS	75
9.1.1. ADD CLIENT TO BLOCKLIST FROM ONLINE CLIENTS	77
9.2. HISTORY CLIENTS	77
9.3. CLIENT LIST	78
9.4. WIRELESS BLOCKLIST	78
9.4.1. ADDING A CLIENT TO THE BLOCKLIST MANUAL	79
9.4.2. DELETING A CLIENT FROM THE BLOCKLIST	79
10. AUTHENTICATION	80
10.1. CONCEPTS OF AUTHENTICATION	80
10.2. NETWORK CONTROL	86
10.2.1. ACCESS ROLE PROFILE	86
10.2.2. POLICIES	87
10.2.3. POLICY LIST	94
10.2.4. LOCATION POLICY	95
10.2.5. PERIOD POLICY	96
10.3. AUTHENTICATION	96
10.3.1. DASHBOARD	97
10.3.2. ACCESS POLICY	97
10.3.3. AUTHENTICATION STRATEGY	99
10.3.4. ROLE MAPPING FOR LDAP	100
10.3.5. AUTHENTICATION RECORD	102
10.3.6. PORTAL ACCESS RECORD	103
10.4. GUEST ACCESS	104

10.4.1. DASHBOARD	104
10.4.2. GUEST ACCESS STRATEGY	104
10.4.3. GUEST ACCOUNT	106
10.4.4. GUEST DEVICE	108
10.5. EMPLOYEE ACCESS	110
10.5.1. DASHBOARD	110
10.5.2. EMPLOYEE ACCESS STRATEGY	110
10.5.3. EMPLOYEE ACCOUNT	111
10.5.4. EMPLOYEE DEVICE	113
10.6. SETTING	115
10.6.1. COMPANY DEVICE	115
10.6.2. LDAP/AD CONFIGURATION	116
10.6.3. EXTERNAL RADIUS	117
10.6.4. ALLOWED IP	118
10.6.5. MAC GROUPS	118
10.6.6. IP GROUPS	119
10.6.7. SERVICE PORT	120
10.6.8. SERVICES	121
10.6.9. SERVICE GROUPS	121
10.7. DEFAULT CONFIG AND QUICK ENTRANCE	122
10.8. CONFIGURATION INSTANCES FOR AUTHENTICATION	124
10.8.1. CONFIGURE 802.1X AUTHENTICATION IN DEFAULT(SIMPLE MODEL)	124
10.8.2. CONFIGURE PORTAL AUTHENTICATION IN SIMPLE MODEL	125
10.8.3. CONFIGURE 802.1X AUTHENTICATION IN CUSTOMIZATION	126
10.8.4. CONFIGURE WEB PORTAL AUTHENTICATION	127
11. RF	130
11.1. RF OVERVIEW	130
11.2. SET RF CONFIGURATIONS OF SITE	132
11.2.1. GENERAL INFORMATION	132
11.2.2. BACKGROUND SCANNING	133
11.2.3. SMART LOAD BALANCE	133
11.2.4. PER BAND INFO	134
11.3. SET RF CONFIGURATIONS FOR A SELECTED DAP	136
11.3.1. SINGLE AP RF CONFIGURATION	136
11.3.2. FALLBACK TO SITE RF CONFIGURATION	136
11.3.3. AP FULL SCAN MODE	137

12. LOG	138
12.1. SYSTEM LOG	138
12.1.1. LOG LIST.....	138
12.1.2. LOG TYPES	139
12.1.3. SEVERITY	139
12.1.4. CONFIG OF AP EVENT LOG	139
12.2. DEVICE LOG	141
13. SECURITY	142
13.1. SECURITY CONFIG	143
13.1.1. ROGUE AP POLICY.....	143
13.1.2. WIRELESS ATTACK DETECTION POLICY	144
13.2. AP RECORD	151
13.3. CLIENT RECORD	151
13.4. BLOCKLIST.....	152
13.4.1. ADDING A CLIENT TO THE BLOCKLIST	152
13.4.2. DELETING A CLIENT FROM THE BLOCKLIST.....	153
13.5. ATTACK RANKING.....	153
14. CAPTIVE PORTAL	154
14.1. ENTRY TO PORTAL PAGE EDITOR.....	154
14.2. PORTAL EDITOR VIEW	155
14.3. SELECT TEMPLATE	156
14.4. PAGE SELECTOR	157
14.5. PAGE VIEW	157
14.6. COMPONENT ATTRIBUTES	157
14.6.1. IMAGE COMPONENT	157
14.6.2. TEXT COMPONENT	157
14.6.3. FORM COMPONENT	158
15. GLOSSARY	159

Revision History

The following table lists the revisions of this document.

Table: Revision history.

Revision	Date	Change Description

1. About This Manual

This User Manual describes the features supported by DAC and provides detailed instructions for setting up and configuring the wireless network.

This chapter contains the following topics:

- [About DAP](#)
- [About DAC](#)

1.1. About DAP

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

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

Please refer to 《DAP User Manual》 for detailed information of DAP.

1.2. About DAC

DAC is a simple, easy to deploy turnkey WLAN solution consisting of one or more DAPs. An Ethernet port with routable connectivity to the DAC or a self-enclosed network is used for deploying a Wireless Network. A DAP can be installed at a single site or deployed across multiple geographically dispersed locations.

The DAC UI provides a standard web-based interface that allows you to configure and monitor a Wi-Fi network. It is accessible through a standard web browser from a remote management console or workstation and can be launched using the following browsers:

- Microsoft Internet Explorer 11 or later

- Apple Safari 6.0 or later
- Google Chrome 23.0.1271.95 or later
- Mozilla Firefox 17.0 or later

If the DAC UI is launched through an unsupported browser, a warning message is displayed along with a list of recommended browsers. However, the users are allowed to log in using the Continue login link on the login page.

2. Set Up a DAC

This section describes how to install a DAC instance.

This chapter contains the following topics:

- [System Requirement](#)
- [DAC Installation](#)
- [DAC Upgrade](#)

2.1. System Requirement

Listed below are the minimum Hypervisor host system requirements for DAC to run as a guest VM and the resources required for the VM to be functional:

Host Requirements	50 DAP 1000 Client	256 DAP 5000 Client	500 DAP 10000 Client	1000 DAP 20000 Client
Quad-core Core E5 2.2 GHz CPUs or Faster (hyper-threading enabled)	4core	8core	12core	24core
Memory	16G	16G	32G	32G
Disk Space	1T	1T	1T	1T
Disk IO Performance	Read: 1.7 GB / s write: 134 MB / S			

Table 2-1-1

For detailed system requirement, please refer to 《DAC Installation Guide》 .

2.2. DAC Installation

Please refer to 《DAC Installation Guide》 for detailed installation process. After Installation, you can login to DAC by use default account 'admin' with default password 'Admin@01' . You should **MUST** change the default password at you first login to DAC.

2.3. DAC Upgrade

Please refer to 《DAC Installation Guide》 for detailed upgrade process.

3. Set Up a DAP

This chapter describes how to register the DAP to the DAC.

This chapter contains the following topics:

- [Classic Network Topology](#)
- [Connecting to Network](#)
- [Assign IP Address](#)
- [Register DAP to DAC](#)

3.1. Classic Network Topology

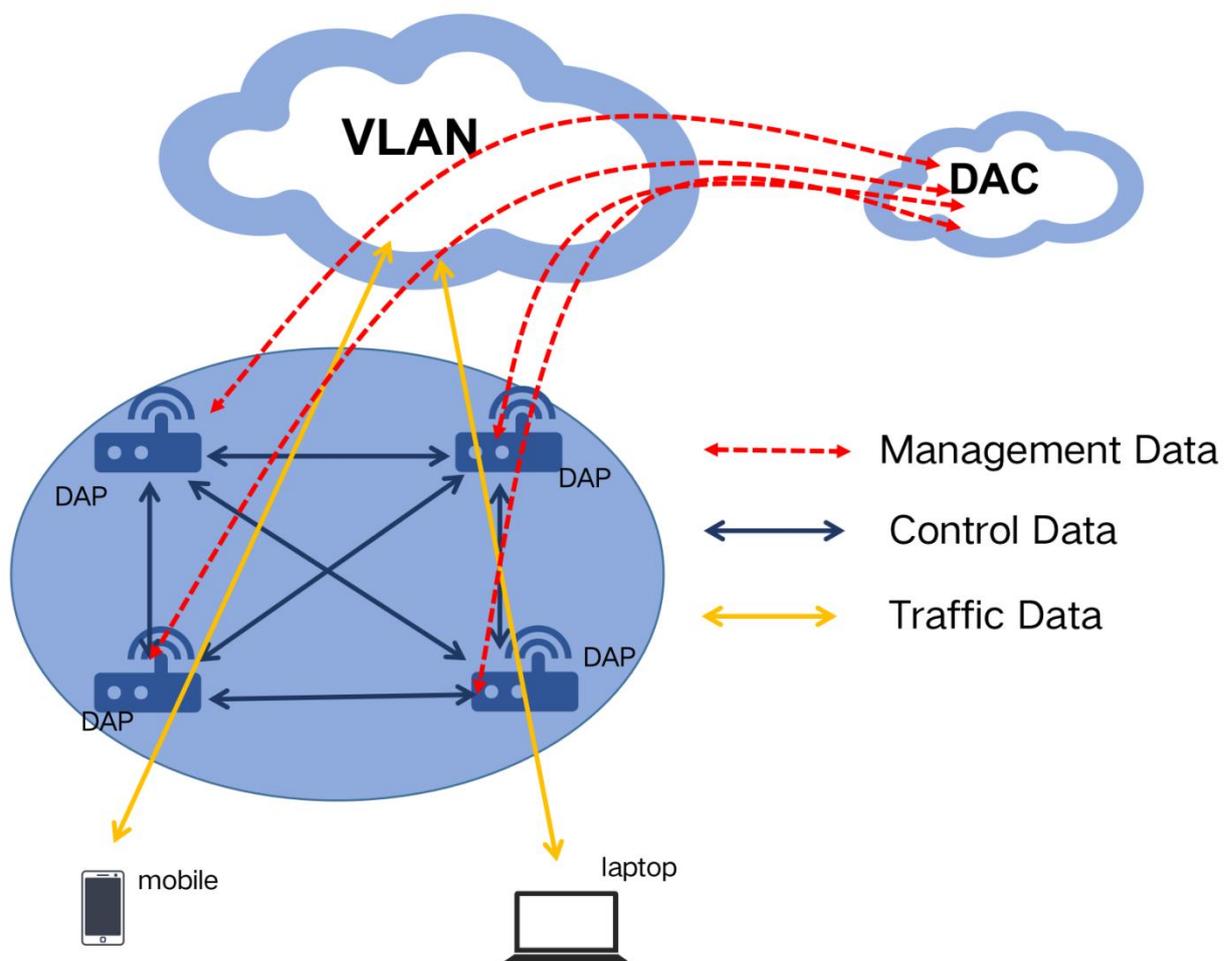


Figure 3-1-1

Fully Distributed cluster architecture separates Management Data, Control Data and Traffic Data.

Distributed Edge Computing within APs replaces the central control of traditional ACs, avoiding platform or link failure, providing higher reliability and saving cost.

- **Management Data** - Management data is transmitted through MQTT protocol; TLS is used to ensure data security. It mainly includes configuration data (such as WLAN configuration, RF configuration, etc.) and service data (such as AP performance monitoring, terminal basic information, etc.).
- **Control Data** - Control data mainly refers to data transmission between DAP devices. The neighboring DAPs will synchronize the terminal, radio and other information, which will be used for load balancing, terminal roaming, dynamic power and so on.
- **Traffic Data** - Traffic data refers to the data that users access the network.

3.2. Connecting to Network

Based on the type of the power source used, perform one of the following steps to connect a DAP to the power source:

- **PoE Switch** - Connect the Ethernet port of DAP to the appropriate port on the PoE switch.
- **PoE Injector** - Connect the Ethernet port of DAP to the appropriate port on the PoE injector.
- **AC to DC power adapter** - Connect the DC power jack socket to the AC to DC power adapter.

3.3. Assign IP Address

The DAP needs an IP address for network connectivity. When you connect an DAP to a network, it receives an IP address from a DHCP server.

To obtain an IP address for a DAP:

1. Ensure that the DHCP service is enabled on the network.
2. Connect the Ethernet port of DAP to a switch or router using an Ethernet cable.

If there is no DHCP service on the network, DAP will use the IP address 192.168.1.254 by default.

3.4. Register DAP to DAC

When the DAP is connected to the wired network, it needs to register to the DAC to be managed by the DAC. There are two ways to register DAPs with DAC.

3.4.1. Discover DAC by DHCP Options

If the AP receives Option 43, Sub-Option 1 from the DHCP server, the AP will boot up and connect to DAC for management. When configuring your DHCP Server, set Option 43 and Sub-Option 1 (01:0C:31:39:32:2E:31:36:38:2E:32:32:2E:31) means 192.168.22.1.

01	0C	31	39	32	2E	31	36	38	2E	32	32	2E	31
Sub-Option1	Length of IP address, 0C = 12	1	9	2	.	1	6	8	.	2	2	.	1

Table 3-4-1-1

3.4.2. Configuring DAC IP Address from DAP Website

At the DAP setup wizard, you can select management mode of DAP, Cluster or DAC. Select DAC, then you can set the DAC IP address. Please refer to 《DAP User Manual》 section **Setup Wizard** to find more information.

4. Getting Start with DAC

The sections below provide an overview of the DAC.

This chapter contains the following topics:

- [Login with default account admin](#)
- [Start with Wizard](#)
- [Network Structure](#)
- [Account Management](#)
- [Administrator Privileges](#)

4.1. Login with default account admin

DAC has a default account "admin" with default password "Admin@01". You should **MUST** change the default password at you first login to DAC.

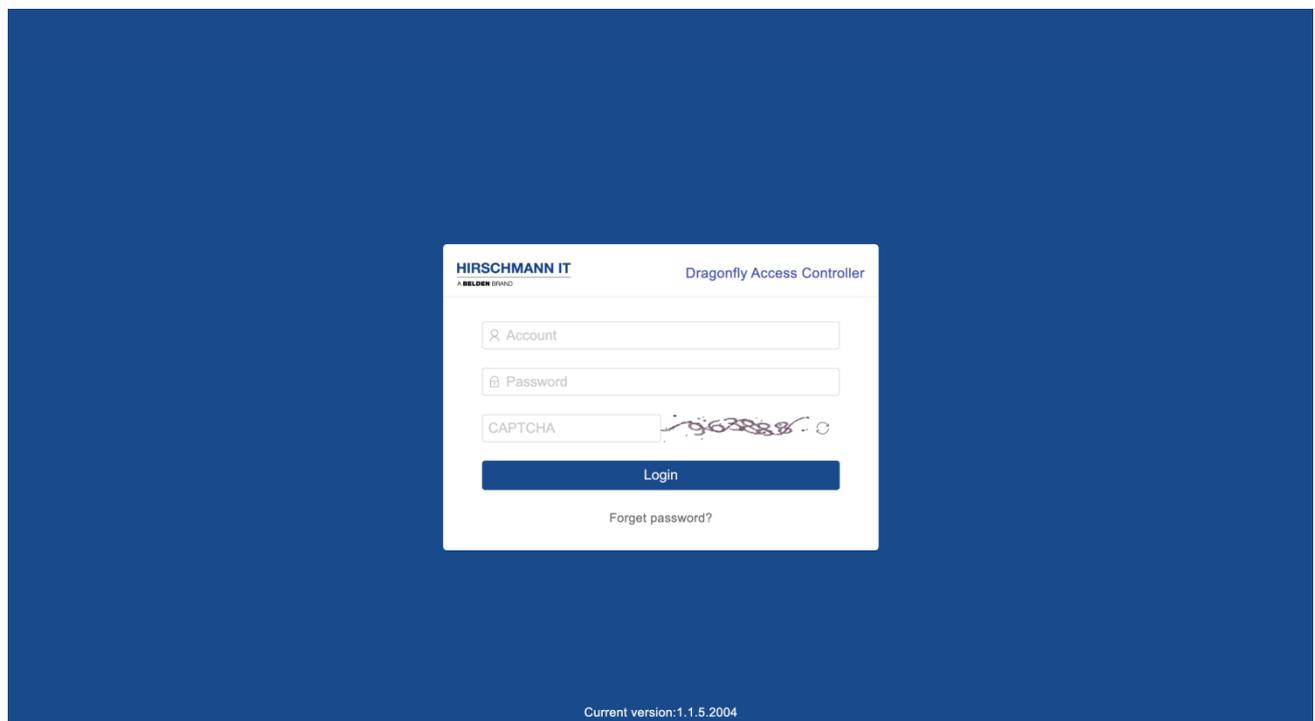


Figure 4-1-1

4.1.1. Change default Password for Account admin

Login to DAC with the admin. Click the personal icon on navigation bar and click Personal Settings item to enter the personal setting page, and then click **Change password**.

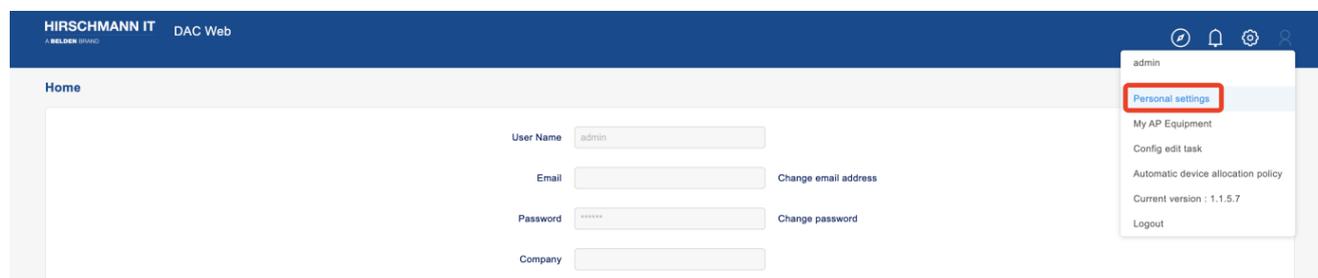


Figure 4-1-1-1

You can change your password in the **Change password** dialog.

- **Old password:** The password that you current use.
- **New password:** The password that you want to change to.
- **Confirm password:** Confirm the new password.

4.2. Start with Wizard

When login to DAC for the first time with the "admin" account, it will ask you whether to do configuration with wizard. You can choose yes to enter wizard or cancel to skip it. You can also click the icon of **wizard** (🧙) in the navigation bar to enter wizard. In the wizard, you will be able to complete

4.2.1. First Step

To create wireless network structure according to your company's organizational structure.

DAC provides three-level structure of network architecture management: Site(required), Group(optional), Corporate(optional). Site is the basic structure, which provides the most abundant network configuration. At the same time, you can assign partially DAPs from the site to groups. While inheriting most of the configuration of the site, groups provide you with the ability of special configuration. Adding sites to Corporate can help you manage multiple sites and allocate unified permissions. You can map the site to the building of the park according to the business needs; Or use

the site to map to the company's office network and use the group to use a special configuration for a specific department (such as the financial office which need more security) to provide security isolation. For more details, please refer to Network Structure and Administrator.

Create site(required) - The DAC defines that customer should create a site at first. Site is one of the distribution units of configuration. It is an organizational structure concept larger than Group and smaller than Corporate. The wireless configuration created in the site not only takes effect on the AP directly under the site, but also can be distributed to the AP in each group to which it belongs. First, it is necessary to create the customer's own site. If there are necessary organizational structure segmentation requirements, you can continue to create groups in the existing site;

Create a Group (optional) - Group is the smallest unit distributed by wireless configuration. The Group must have a home site structure, which can meet the needs of most users. According to the design, the Group can have its own wireless configuration and inherit the wireless configuration of the home Site, with high flexibility;

Create a Corporate (optional) - Corporate is the largest unit. Only when the customer's actual organizational structure has more than one site coverage, the unified management of multiple sites can be realized through the concept of Corporate;

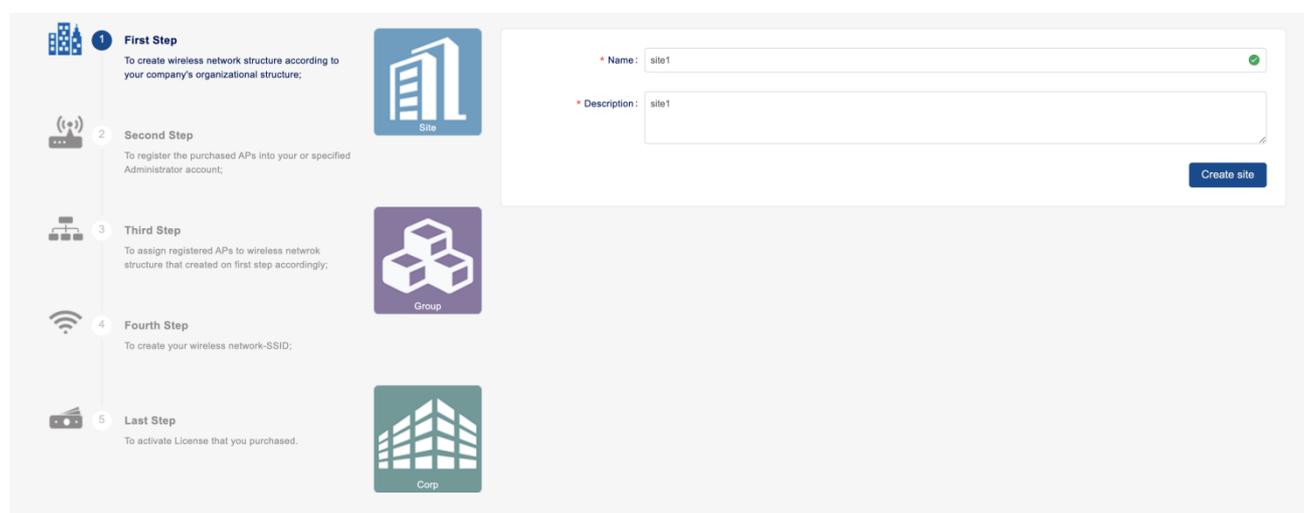


Figure 4-2-1-1

4.2.2. Second Step

To register the purchased APs into your or specified Administrator account;

This step is not necessary. When DAP register to DAC at the first time, it will be bind to the admin account automatically.

Select the AP that needs to be registered under the account and fill in the MAC and SN of the AP to add the AP to the account (Note: the AP and DAC network can reach); in addition to manual entry one by one, we provide more convenient functions of "automatic entry of AP with gateway" and "addition with cluster". The former is the outgoing condition of the latter function.

"Same gateway AP automatic entry" function: when customers deploy AP wireless networks in batches in their own network (with fixed gateway), the AP equipment behind the fixed gateway can use the "same gateway AP automatic entry" function to complete the entry in batches at one time, and all will be displayed in the AP list under the entry box;

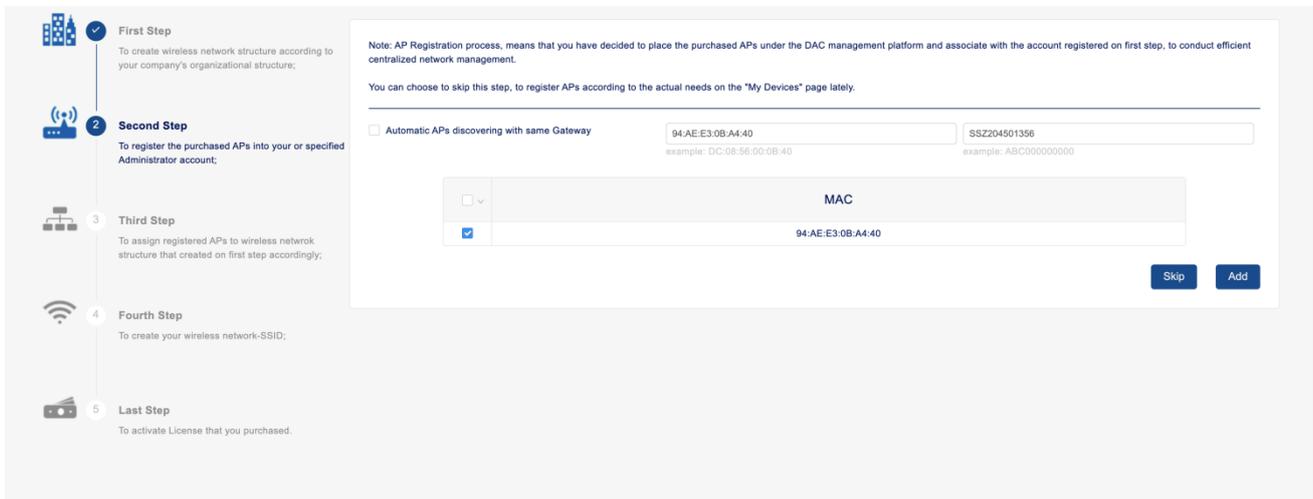


Figure 4-2-2-1

4.2.3. Third Step

To assign registered APs to wireless network structure that created on first step accordingly;

In third step of the setup wizard, select to assign APs to sites or to groups under sites;

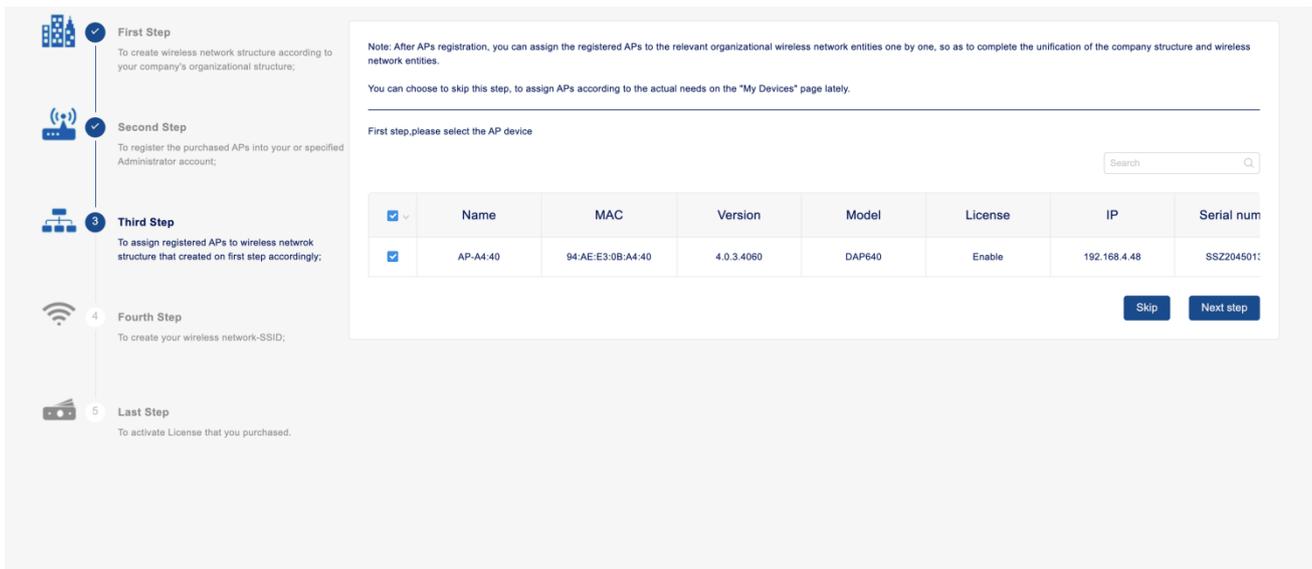


Figure 4-2-3-1

Click the Next step button, select Site that you want these APs assign to.

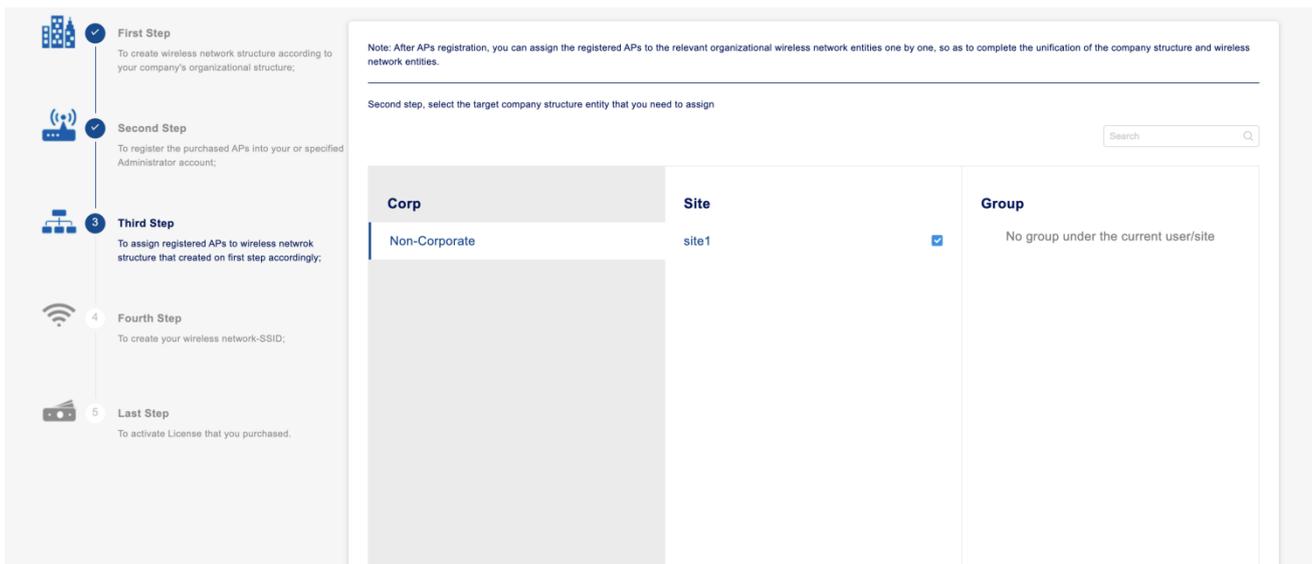


Figure 4-2-3-2

4.2.4. Fourth Step

To create your wireless network - SSID.

Create WLAN. WLAN is under the Site or Group. When creating WLAN, you need to select the Site or Group where WLAN needs to be created; Please refer to [WLAN](#) for more information.

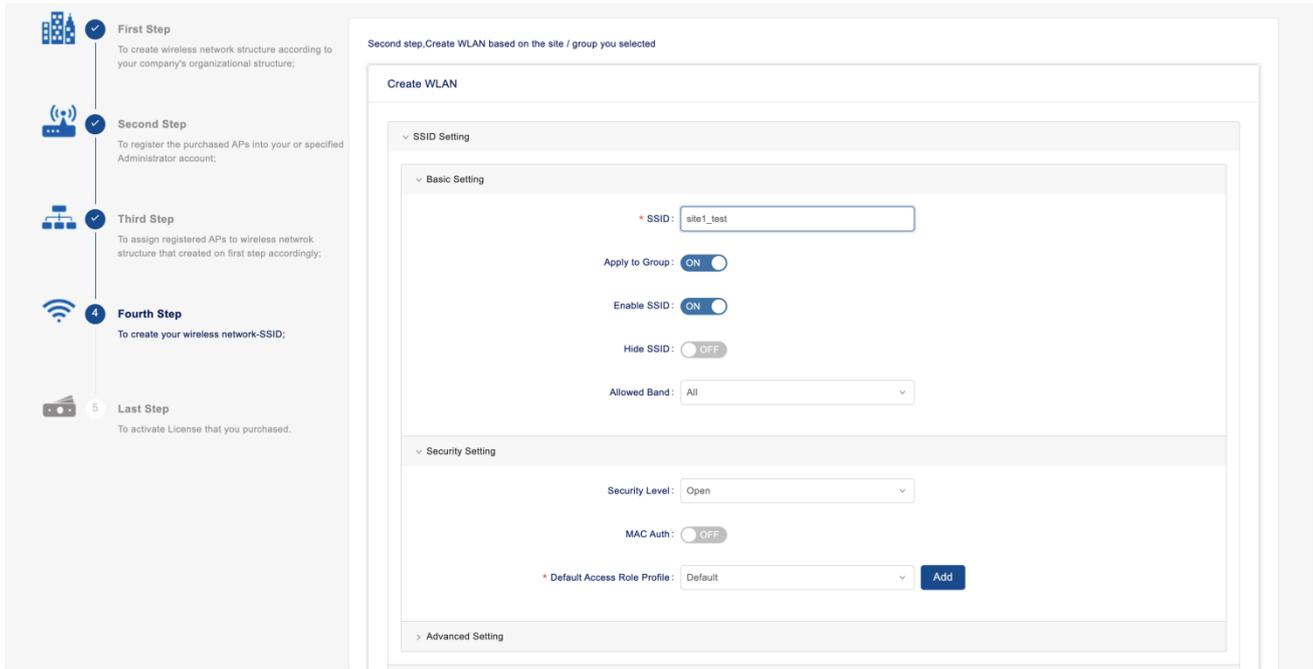


Figure 4-2-4-1

4.2.5. Last Step

To activate License that you purchased.

In last step of the setup wizard, activate the license, fill in the license serial number applied for, and click the **Active** button to activate the license.

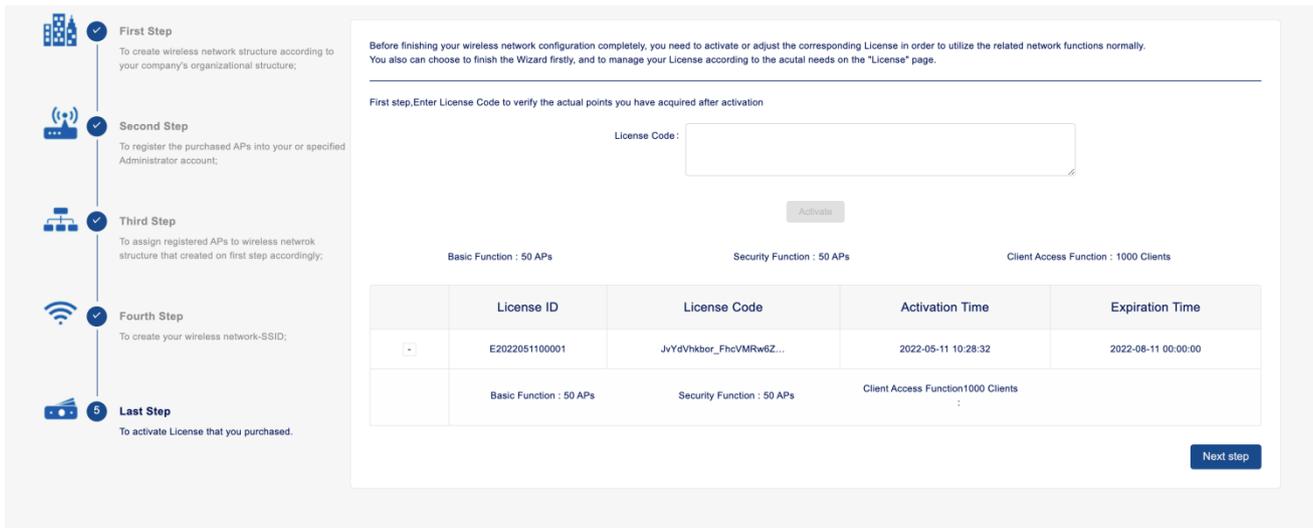


Figure 4-2-5-1

4.3. Network Structure

The internal organization of an enterprise is often not completely flat and needs to be divided into different regions or sub-nets. For enterprises with many branches or chain stores, it is more necessary to manage the network separately. At the same time, administrators with different permissions may be assigned to branches or stores to facilitate their maintenance of the network. DAC provides a mechanism to deal with these situations.

DAC manages the enterprise network structure through the relationship at the Corporate(optional)-Site(required)-Group(optional) level. In the wizard, we already establish the corresponding network structure. This section describes how to create corresponding management objects from the user dashboard.

Only the "admin" account can create and maintain these network structures.

- **Site** - Site is the basic structure, which provides the most abundant network configuration.
- **Group** - A Group belongs to a Site and can only be created from site. While inheriting most of the configuration of the site, groups provide you with the ability of special configuration.
- **Corporate** - Corporate is a set of sites. Adding sites to corporate can help you manage multiple sites and allocate unified permissions.

4.3.1. Create a New Site

On the user dashboard page, click "+" of "Site" tab, you will see the "Create Site" window.

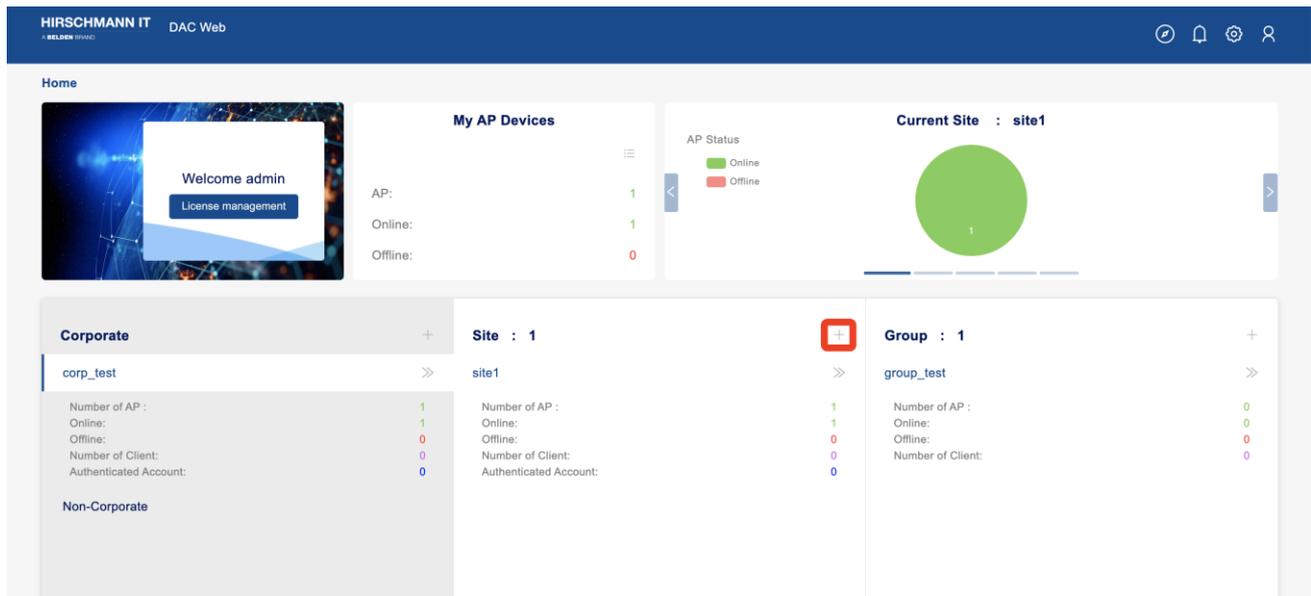


Figure 4-3-1-1

- Fill in the name and description.
- Click **Save** to complete, you can see the newly created site on the site tab of the user dashboard.
- If you want to create sites in batch, enable switch of batch creation You need to fill in the number of sites created, up to 64. Each user can create 64 sites. If you already have other sites, the total number of batch creation is 64 minus the number of sites already created.

4.3.2. Create a New Group

- On the user dashboard page, select the site that you want to add Group. Click "+" of "Group" tab.
- Click **"add group"** and the create group window will be displayed.
- Fill in the name and description fields and click **Save**.
- You will see the newly created group appear in the list.

4.3.3. Create a New Corporate

- On the user dashboard page, click "+" of "Corporate" tab, you will see the "Create Corporate" window.
- Fill in the Name and Description.
- Click "Save" to complete, you can see the newly created Corporate on the Corporate tab of the

user dashboard.

4.3.4. Join a Site to a Corporate

A site can only join one corporate. If a site is already join into a corporate, you should quit it at first.

- Open "Setting" tab in the view of Site.
- Click **Join Corp** button, you will see the **Corp information** window.

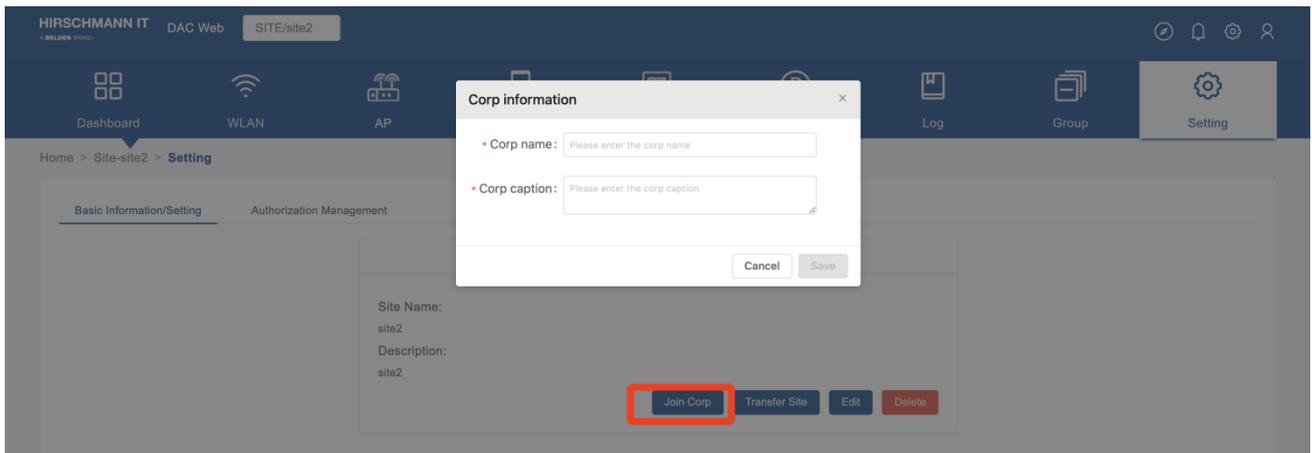


Figure 4-3-4-1

- Fill in the Corp name and Corp caption. You need to make sure that the Corp exists.
- Click **Save** button, if success, you will see **Corp Operation** in the "Setting" view of Site. And the Join Status is "In Progress".

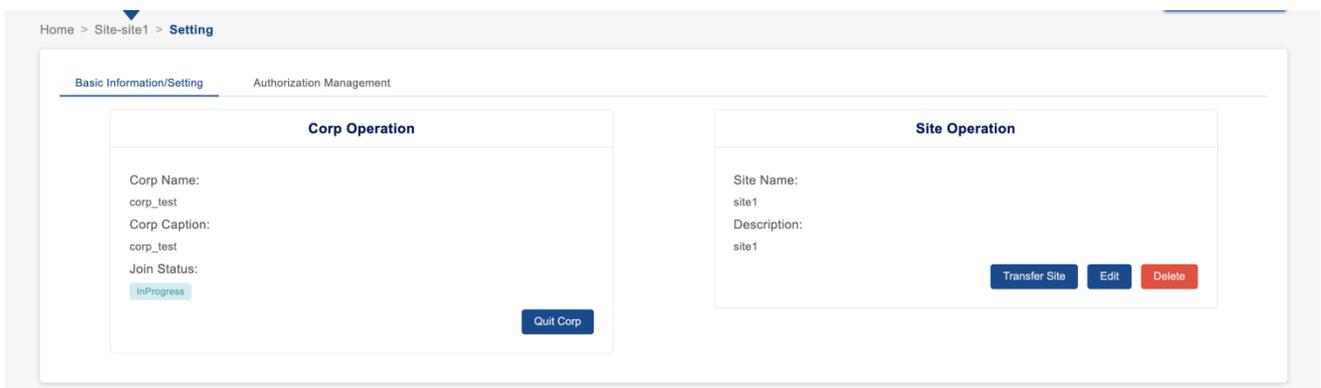


Figure 4-3-4-2

- Then you should go to Corp dashboard.

- You can see the join request on the Monitoring Panel. Click **Accept** button to accept the join request or click **Reject** button to reject the join request.

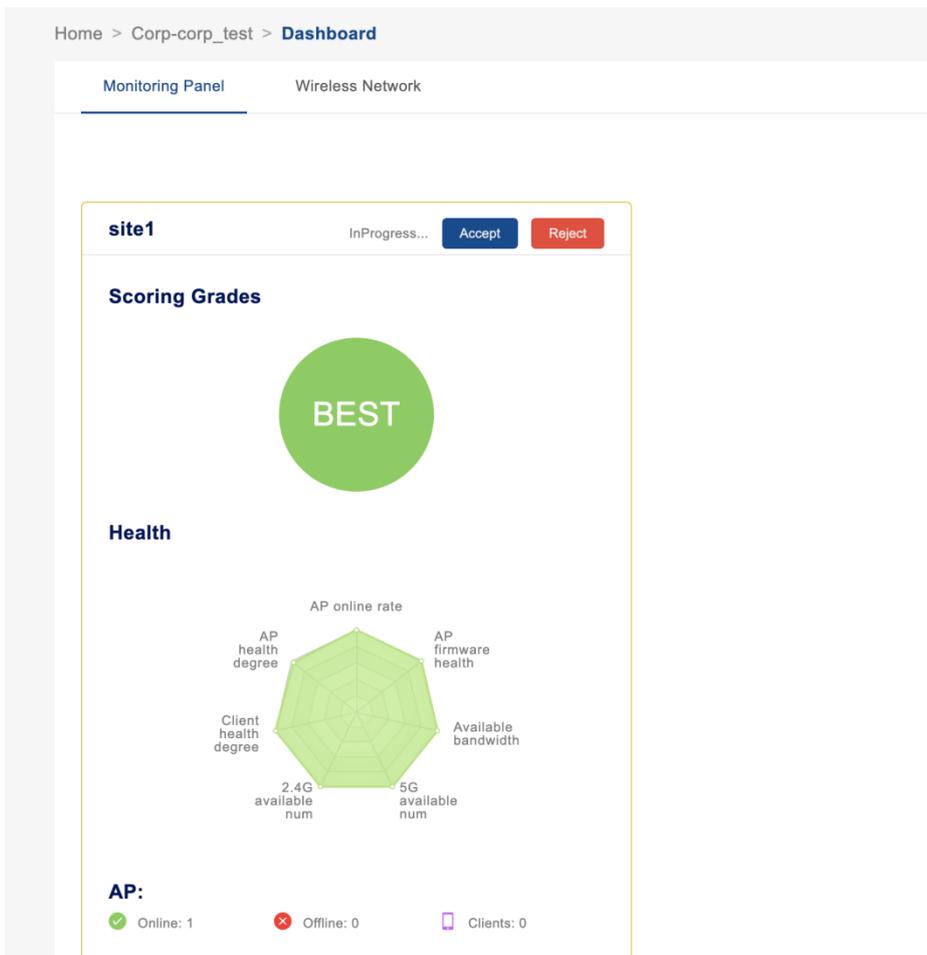


Figure 4-3-4-3

4.4. Account Management

DAC is a multi-tenant system with rich and flexible authorization control. As a network administrator, you can usually use the default account "admin" to manage your wireless network. But in some cases, you need to make network management more flexible by creating new accounts and assigning authorization to those accounts.

DAC guides other administrators to complete account registration by sending an invitation email from the "admin" account.

In order to enable the email notification / account creation and other functions of the DAC (these functions require the system to send emails externally), you need to add at least one **SMTP Server**

that can send emails on the DAC at first.

4.4.1. Add SMTP Server

- Log in with the default account "**admin**".
- Click System Configuration on the navigation bar
- Click **SMTP(Email) Configuration** tab to enter the SMTP mailbox list page;
- Click + icon to add the SMTP Server

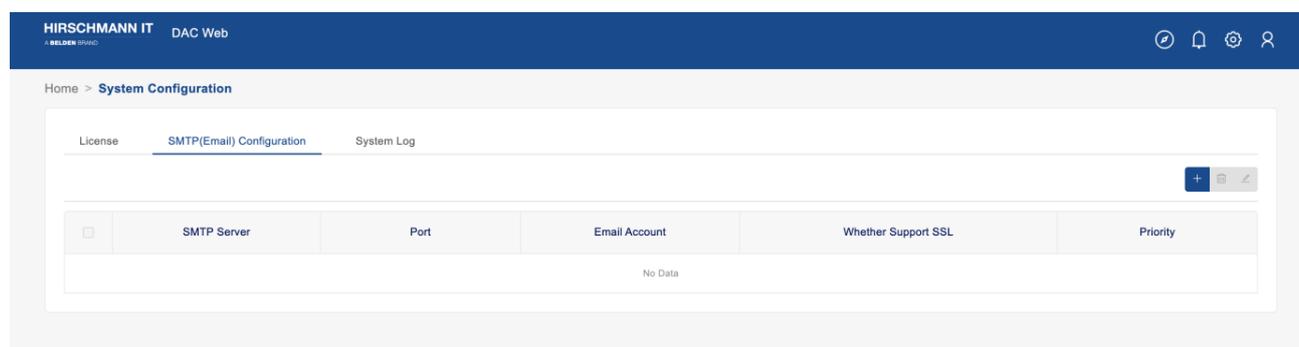


Figure 4-4-1-1

At the **Add SMTP Mailbox Server** Dialog,

- **SMTP Server** - Domain of SMTP Server.
- **Priority** - Priority of SMTP Mail Server. You can add at most 10 SMTP Mail Server. The lower the value of Priority, the higher the priority. If a working mailbox fails to send mail due to failure, the system will try to send mail with a lower priority working mailbox.
- **Port**: Port of SMTP Server
- **Email Account** - Email Account which used to send mail
- **Email Password** - Email Password
- **Whether Support SSL**
 - **Support** - Connect mail server with SSL.
 - **Not Support** - Mail server do not support SSL, connect it normally.
- **Test Email** - An Email Address used to receive the Test email.

Click **Email Server Test** button, DAC will send test email to Test Email and the **Save** button will

available only after sending successfully. Click **Save** button to save the working mailbox.

4.4.2. Create Account

Account creation needs to be completed through the invitation of the **"admin"** account, and the authorization of the account will be completed at the same time.

Initiate email invitation

Enter the setting page of the site view, click authorization management, click +, fill in the e-mail address of the account to be registered in the Add administrator window, and select the permission of the account in the current site.

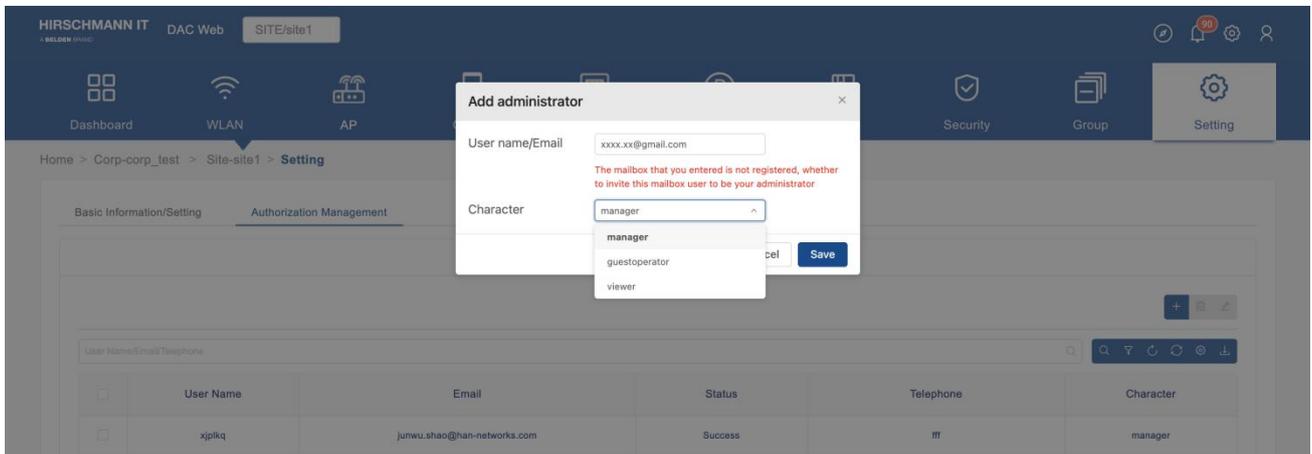


Figure 4-4-2-1

Create Account

Login to the invited mailbox and click the registration connection. Go to the invitation registration page.

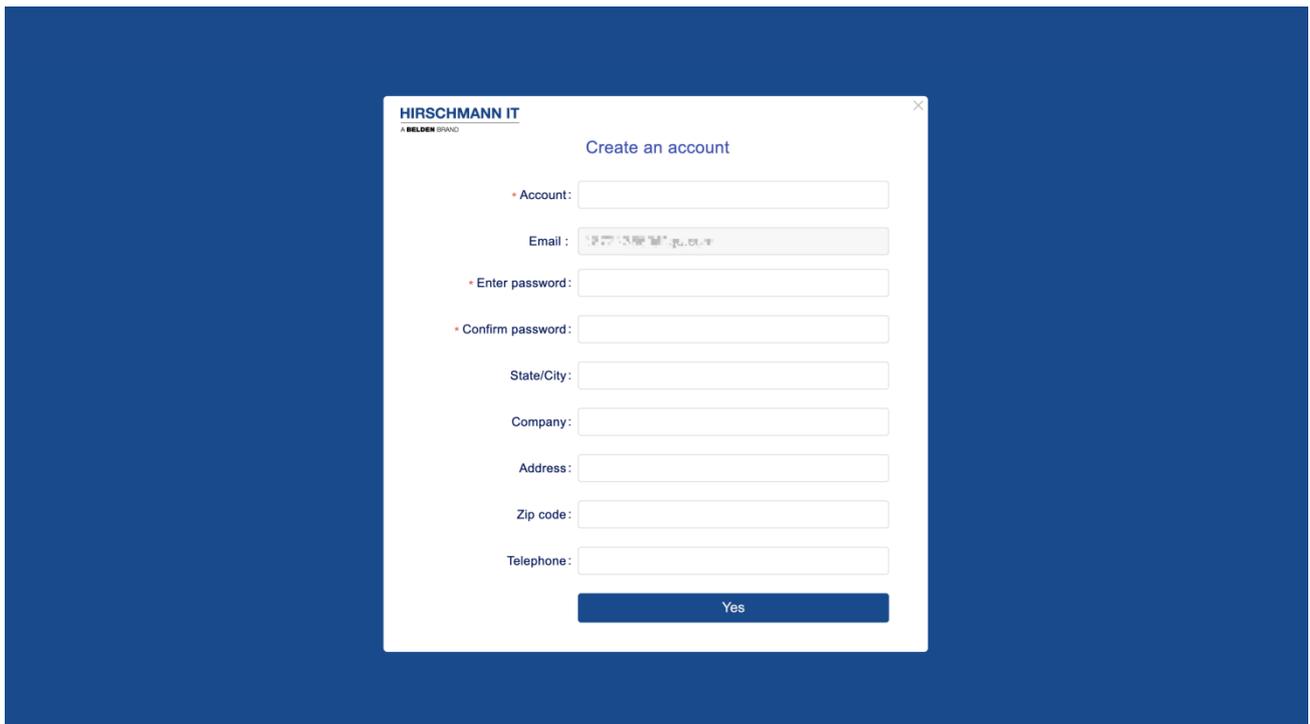


Figure 4-4-2-2

- **Account:** Account. Required.
- **Email:** The email that you will use to login. Required.
- **Enter Password:** The Password that you will use to login. Required.
- **Confirm Password:** Confirm the password. Required.
- **State/City:** State/City.
- **Company:** Name of your company.
- **Address:** Address of your company.
- **Zip code:** Zip code of your company.
- **Telephone:** Your telephone number.

4.4.3. Change Password

You can change password after login. Click the personal icon on navigation bar and click **Personal Settings** item to enter the personal setting page, and then click **Change password**.

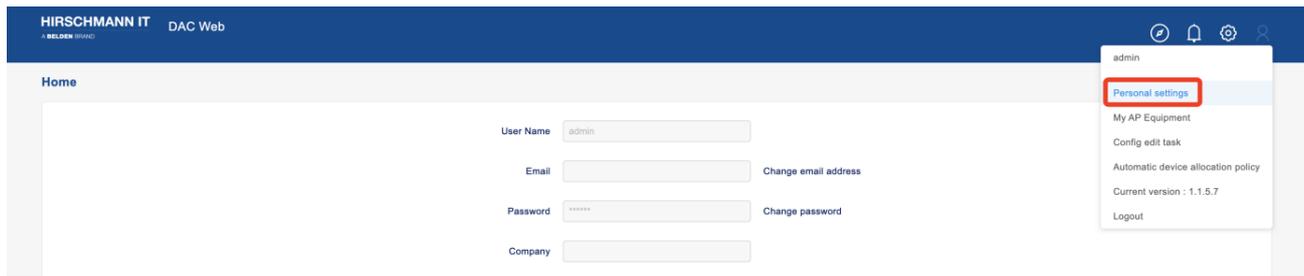


Figure 4-4-3-1

You can change your password in the **Change password** dialog.

- **Old password:** The password that you current use.
- **New password:** The password that you want to change to.
- **Confirm password:** Confirm the new password.

4.4.4. Forget Password

If you forget your password, you can recover your account. Click **Forgot password?** Link at the login page, then you can see the **Recover your account** page.

- **Email / Account:** Input you Email or Account.
- **Verification code:** When you enter the correct email or account, you can click the Get Code button. Then you can get Verification Code from your email.
- **New password:** Input the password that you want to set.
- **Confirm password:** Confirm the password.

4.5. Administrator Privileges

The "admin" account is the supper user of DAC. It is the Owner of AP devices, Licenses, and the network structures. Other users can only be invited to register by the "admin" account via email and become the administrator of a network.

The DAC administrators can be classified as follows:

Roles	Privileges	Access levels
admin	Owner	The owner of the network, including AP device and license; Can create network structures and assign AP to Site; Can use all management and monitoring functions; Can invite other users to manage and monitor the network based on the network organization structure;
	Manager	The manager of the network, not the owner of the device and license; Can use all management and monitoring functions;
Other Users	Viewer	The observer of the network, rather than the manager of the network, it has privileges for all monitoring functions, but does not have privileges for network management and configuration functions;
	Guest Operator	The manager for network visitors, rather than the manager of the overall network nor the owner of device and license; Have the management function for network visitors;

Table 4-5-1

The "admin" account is the Owner of the network, including all AP devices and licenses. The "admin" account can create new network structures (site, group, corporate) and assign APs to corresponding network structures and can assign administrators, managers or viewers to these network structures. The "admin" account has privileges for all management and monitoring functions. The "admin" account can initiate an invitation to other people to register an account. Only the email that receives the invitation can register an account on the DAC. The "admin" account can invite other users to register accounts, and grant them different privileges for different sites.

If a user has the Manager privileges of a Site, he can use all the management and monitoring functions

of the Site.

If a user has Viewer privileges on a site, he can view the site configuration and monitor the running status of the Site, but he cannot add or modify the site's configuration.

If a user has the Guest Operator privileges of a Site, he only has the permission to manage guest account of the Site.

4.5.1. Add authorization for Site

- Click "**Authorization Management**" tab in the Setting View of site.

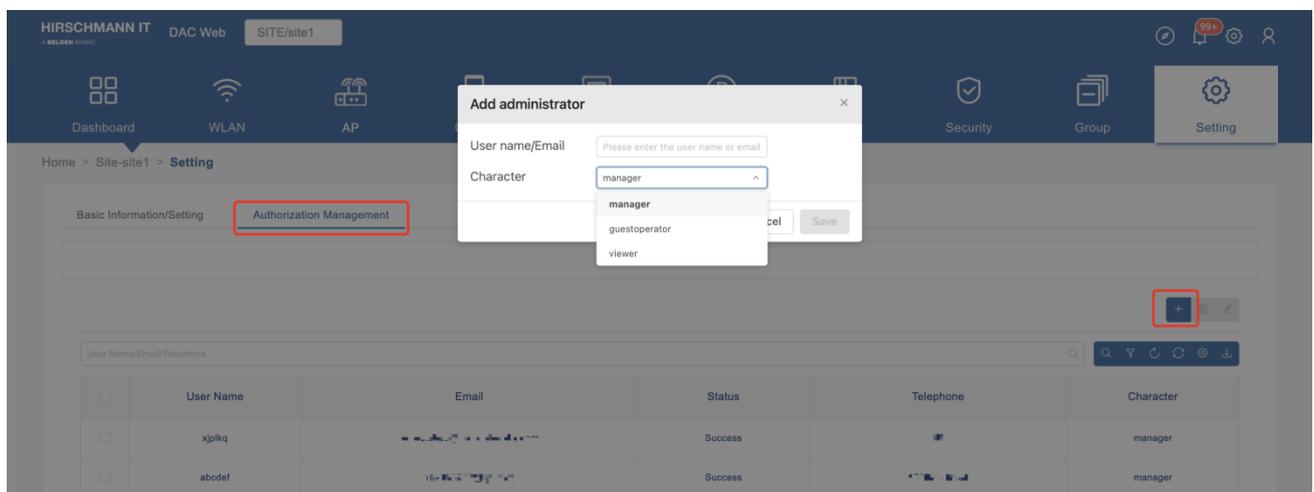


Figure 4-5-1-1

- Click + icon to bring up **Add administrator** screen.
- Fill the User name/Email which you want to add. The User name should Exist. Select the character in the drop down menu. You can also invite a new user to manage the current site. See [Create Account](#) for more information.
- Click Save to complete authorize.

4.5.2. Remove Authorization for Site

- Select the authorization that you want to remove in the list.
- Click **Delete** icon.
- Click **Yes** at the confirmation prompt.

5. DAC User Interface introduction

This chapter will introduce the basic operation of the user interface of the DAC.

This chapter contains the following topics:

- [Banner Tools](#)
- [Configuration/Display Icons](#)
- [Working with Tables](#)
- [User Home Page](#)
- [Site View](#)
- [Group View](#)

5.1. Banner Tools

Banner Tools	
	<p>Wizard</p> <p>To quickly enter the wizard mode, configure the relevant network structure and its corresponding license activation.</p>
	<p>Notice</p> <p>Click to enter the message notification based on user level.</p>
	<p>System Configuration</p> <p>You can enter License, SMTP(Email) Configuration and System Log from here.</p>
	<p>Common Information</p> <p>Quick access to personal configuration and some of its functions.</p>

Table 5-1-1

- **Wizard** - To quickly enter the wizard mode, configure the relevant network structure and its corresponding license activation. Refer to "[Start with Wizard](#)" for details.

- **Notice** - Click to enter the message notification based on user level.
 - **Message** – displays message notifications based on the account dimension
 - **Message Setting** - configure whether to receive relevant messages, and whether to send email notification for messages options. (it should be noted here that if relevant messages are configured, the corresponding message information can be generated only after the log module under the site is turned on. If the switch in site is not turned on, the message information based on the site will not be generated.)
- **System Configuration** - You can enter License, SMTP(Email) Configuration and System Log from here.
- **Common Information**
 - **Personal Settings** - Click to enter the personal information modification page. Email, password, address, and telephone number can be modified
 - **My AP Devices** - Click to enter my device page. Refer to user dashboard for details.
 - **Config edit task** - Click to view the list of config tasks under the current user. You can cancel or delete the config tasks on this page.
 - **Automatic device allocation policy** - To configuring the binding policy of subnet and site, the AP will be assigned to the corresponding site automatically.
 - **Current version** - Click to view the DAC Release Note.
 - **Logout** - Click to log out the current account.

5.2. Configuration/Display Icons

DAC provides standard tools for interacting with configuration/display screens. These icons/buttons include:

Configuration Icons/Buttons	
	<p>Add</p> <p>Click the Add icon to create a new entry within the configuration screen.</p>
	<p>Edit</p> <p>To edit an existing entry, select the entry in the configuration screen and click the Edit icon.</p>

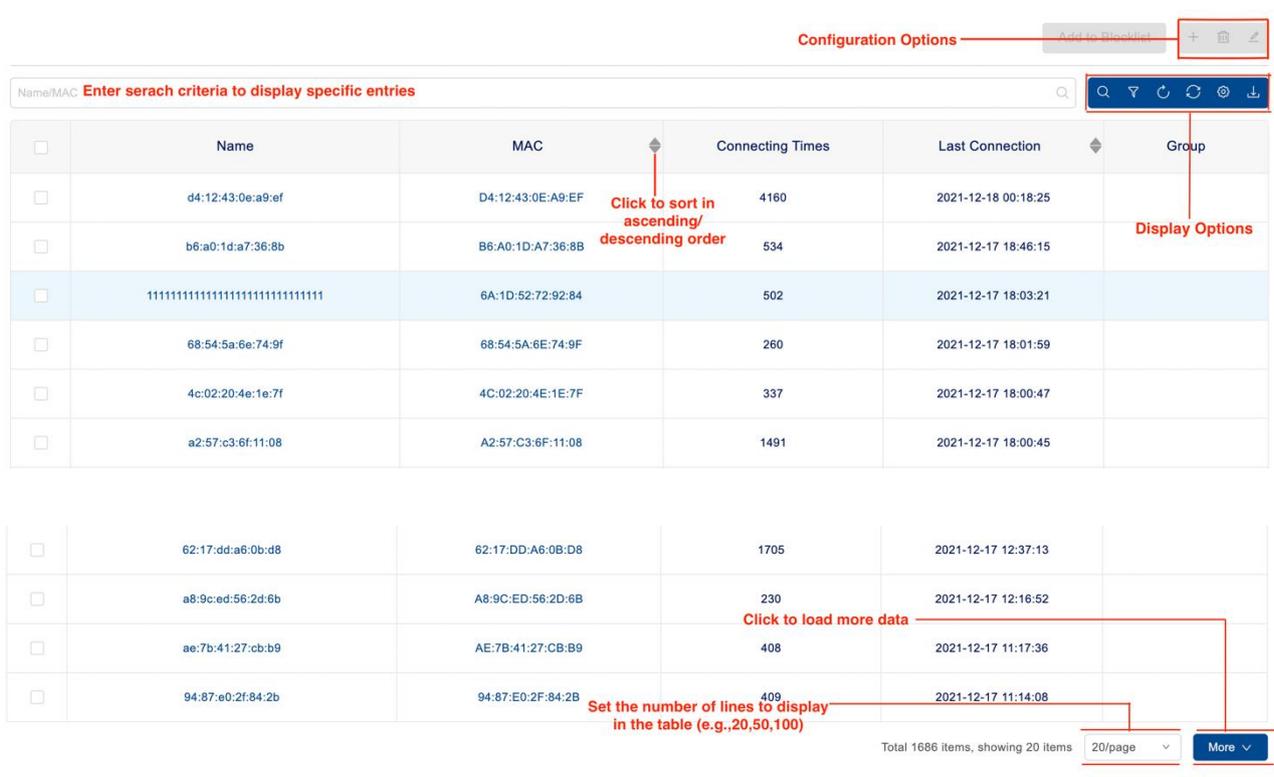
	<p>Delete</p> <p>To delete an entry, select the entry and click the Delete icon.</p>
	<p>Wizard</p> <p>To quickly enter the wizard mode, configure the relevant network structure and its corresponding license activation.</p>
	<p>Notice</p> <p>Click to enter the message notification based on user level.</p>
	<p>System Configuration</p> <p>You can enter License, SMTP(Email) Configuration and System Log from here.</p>
	<p>Common Information</p> <p>Quick access to personal configuration and its common functions.</p>
	<p>Help</p> <p>Click the help button to load the corresponding prompt.</p>
Table Icons/Buttons	
	<p>Search</p> <p>Click the Search button and enter search criteria in the "Search..." field to display specific entries in the table.</p>
	<p>Filter</p> <p>User can check the corresponding filter field for the table to display specific data</p>
	<p>Reset</p> <p>Click the Reset button after filtering a table to return to the original display.</p>
	<p>Refresh</p> <p>The Refresh button loads the latest data for an application table, chart or list.</p>
	<p>Settings</p> <p>Used to configure the column headings to display in a table, click on the Settings button and select the column headings you want to display.</p>

	<p>Export to CSV</p> <p>Click the CSV button to download information displayed in Table View to a CSV (spreadsheet) file.</p>
	<p>Sort</p> <p>Information displayed in List View may be sorted in alphabetical order, either ascending or descending, by clicking on the Sort button. You can also click on the Up/Down arrows at the top of any table column in Table View to sort the data in ascending or descending order based on the selected column.</p>

Table 5-2

5.3. Working with Tables

Information in DAC is primarily presented in table format. There are common functions/behaviors for tables in DAC. The general functionality of each area is described below. Details for each button are provided in the Configuration/Display Icons section.



The screenshot shows a table with the following data:

Name	MAC	Connecting Times	Last Connection	Group
d4:12:43:0e:a9:ef	D4:12:43:0E:A9:EF	4160	2021-12-18 00:18:25	
b6:a0:1d:a7:36:8b	B6:A0:1D:A7:36:8B	534	2021-12-17 18:46:15	
11111111111111111111111111111111	6A:1D:52:72:92:84	502	2021-12-17 18:03:21	
68:54:5a:6e:74:9f	68:54:5A:6E:74:9F	260	2021-12-17 18:01:59	
4c:02:20:4e:1e:7f	4C:02:20:4E:1E:7F	337	2021-12-17 18:00:47	
a2:57:c3:6f:11:08	A2:57:C3:6F:11:08	1491	2021-12-17 18:00:45	
62:17:dd:a6:0b:d8	62:17:DD:A6:0B:D8	1705	2021-12-17 12:37:13	
a8:9c:ed:56:2d:6b	A8:9C:ED:56:2D:6B	230	2021-12-17 12:16:52	
ae:7b:41:27:cb:b9	AE:7B:41:27:CB:B9	408	2021-12-17 11:17:36	
94:87:e0:2f:84:2b	94:87:E0:2F:84:2B	409	2021-12-17 11:14:08	

At the bottom of the table, it says: Total 1686 items, showing 20 items. 20/page More

Figure 5-3-1

- **Configuration Options** - Used to create, edit, delete entries (e.g., create, edit, delete a WLAN).

Details for each icon are provided in the Configuration/Display Icons section.

- **Display Options** - Used to change the table display from Table View to List view, to set the columns you want to display, and to refresh the data in the table. Details for each button are provided in the **Configuration/Display Buttons** section.
 - **Filter** - Hide/Display filter options.
 - **Download** - You can export the table into a .csv file.
 - **Search** - Enter search criteria in the Search... field to display specific entries in a table. As you enter criteria, only those entries matching the criteria will appear in the table. Click on the **Reset** button to return to the original table display.
- **Sort** - Click on one of the arrows at the top of a column to sort the table in ascending or descending order based on the column.
- **Set Lines to Display/Page in the List** - Set the number of lines to display in the list. Using the drop-down menu at the bottom left corner of the list.

5.4. User Home Page

Introduce the user home page, including Corporate / Site / Group, Device list, license and other information.

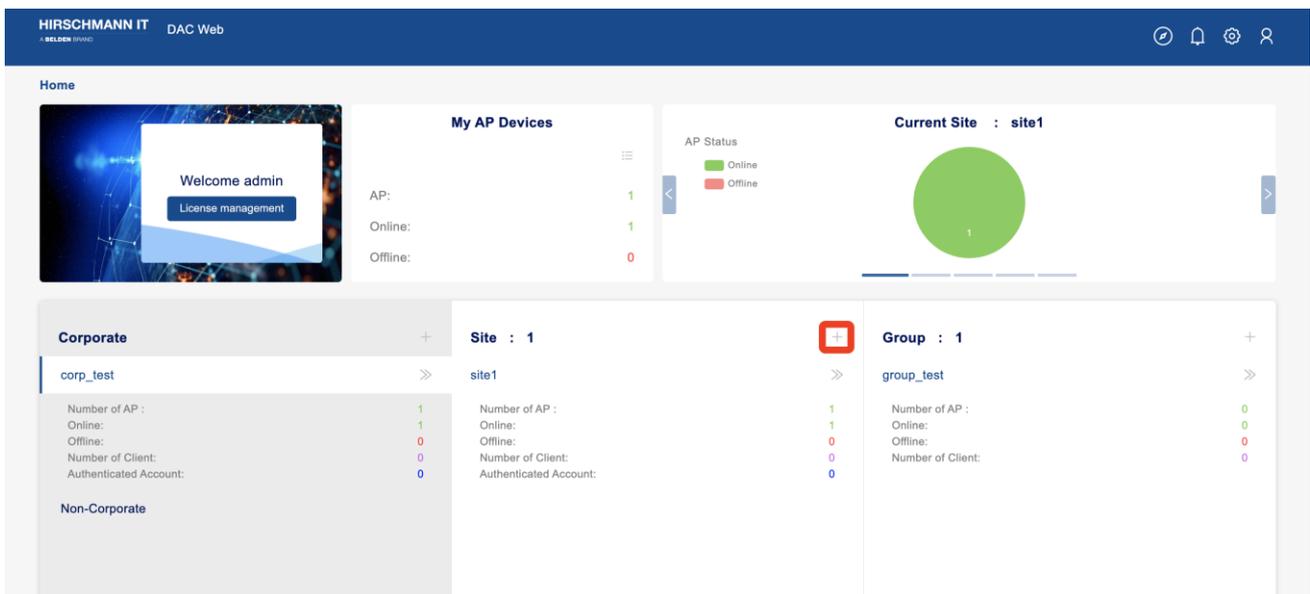


Figure 5-4-1

5.4.1. Home

- **Welcome Message and License Management** - After login, the customer account is shown on this panel. At the same time, the tab of this panel also provides the entry of "license management" function.
- **My AP Devices** - It is used to monitor the total number of APs, the number of APs online and the number of APS offline. Click the list icon quickly enter My Device Screen.
- **Current site**
 - **AP Status** - Pie chart of AP Status (Online/offline number)
 - **AP Model** - Model and quantity of AP device
 - **Client Number** - Statistics of clients
 - **Throughout** - Line chart of bandwidth
 - **Total Traffic** - Flow histogram of traffic
- **Network structure** - The customer network structure panel is divided into "Corporate" - "Site" - "Group" from left to right. The three-tier network structure adopts the progressive display method in design. If the customer has more than one "Corporate" or "Site", the corresponding "Site / Group" will be displayed when clicking a "Corporate / Site".

5.4.2. My Device

At the home page **My AP Devices** Panel, click the  icon can enter My Device Screen.



On My Device Screen, the top prominent positions are "count of online APs (green number)" and "count of offline APs(red number)".

5.4.3. AP Device

The list of all AP Device that you manage. You can select to show the Owner Permission device or Admin Permission device.

- **Name** - AP device name, you can change the name of AP, so that we can find it quickly. You can click it to enter AP detail view.
- **Site** - The site that this AP belongs to. You can click it to enter site view.
- **Group** - The group that this AP assigned to. You can click it to enter group view.
- **Corp** - The group that this AP belongs to.
- **MAC** - The MAC Address of this AP.
- **Status** - Online / offline status of this AP.
- **Firmware** - Firmware version of this AP.
- **Model** - Hardware type of this AP.
- **License** - License Status of AP. Can be enable or disable. If license is disable, AP will not broadcast SSID.
- **IP** - IP Address of this AP.
- **Serial Number** - Serial Number of this AP.
- **Client Number** - Number of clients on this AP currently.
- **Location** - Location of device
- **2.4G Channel** - The channel of 2.4G this DAP used.
- **5G All Channel** - The channel of 5G this DAP used.
- **Online Duration** - The duration of this DAP connect to DAC.
- **Last Offline Time** - The time of this DAP latest disconnect from DAC.

5.4.4. Assign DAPs to a Site/Group

In the Home -> My Device Screen, click **AP Device** Tab. Select APs that you want to assign to Site/Group. Click **Set Site** Button. Then click **Yes** button at the confirmation prompt. Then you can see the **Set Site** Screen. Select a site at the drop down menu, click Next step button. Then you can

select a group or do not set group, click Next Step. Finally confirm the information and click **Save** button.

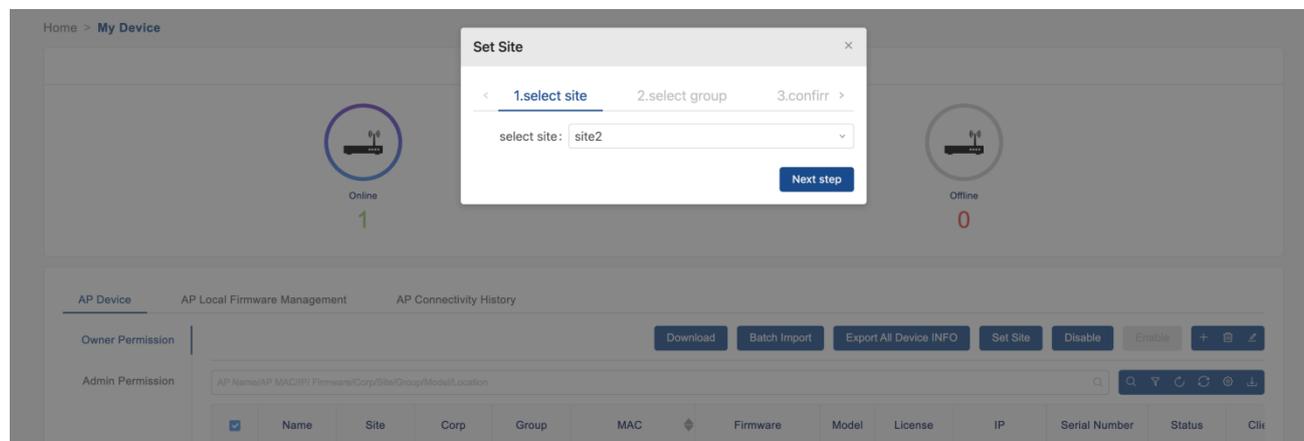


Figure 5-4-4-1

5.4.5. AP Local Firmware Management

In the Home -> My Device Page, click **AP Local Firmware Management** tab, you can manage local AP firmware.

Usually, the DAC will download the firmware of AP from the cloud. However, in some cases, we need to import the firmware of DAP from the DAC management page. The imported firmware is a compressed package that you can get from your supplier. Click + icon to bring up the **Upload** window. Click upload button and select the AP firmware package you obtained from the vendor. After the file is uploaded, it will be displayed in the list.

- **Firmware Version** - Version of DAP Firmware.
- **Firmware Description** - Firmware Description.
- **Upload Time** - When this firmware upload to this list.

And then, you can upgrade the firmware of AP devices on the AP device list page of site view. Please refer to [Firmware Management](#) to get more information.

5.4.6. AP Connectivity History

AP connect and disconnect record.

- **MAC** - MAC Address of AP device.
- **Name** - Name of AP device.
- **MQTT Connecting Time** - MQTT connect time of this AP.
- **MQTT disconnect time** - MQTT disconnect time of this AP.
- **MQTT connection Duration** - Duration of this connection

5.5. Site View

Click the site in User Home Page, then you will see the view of this site.

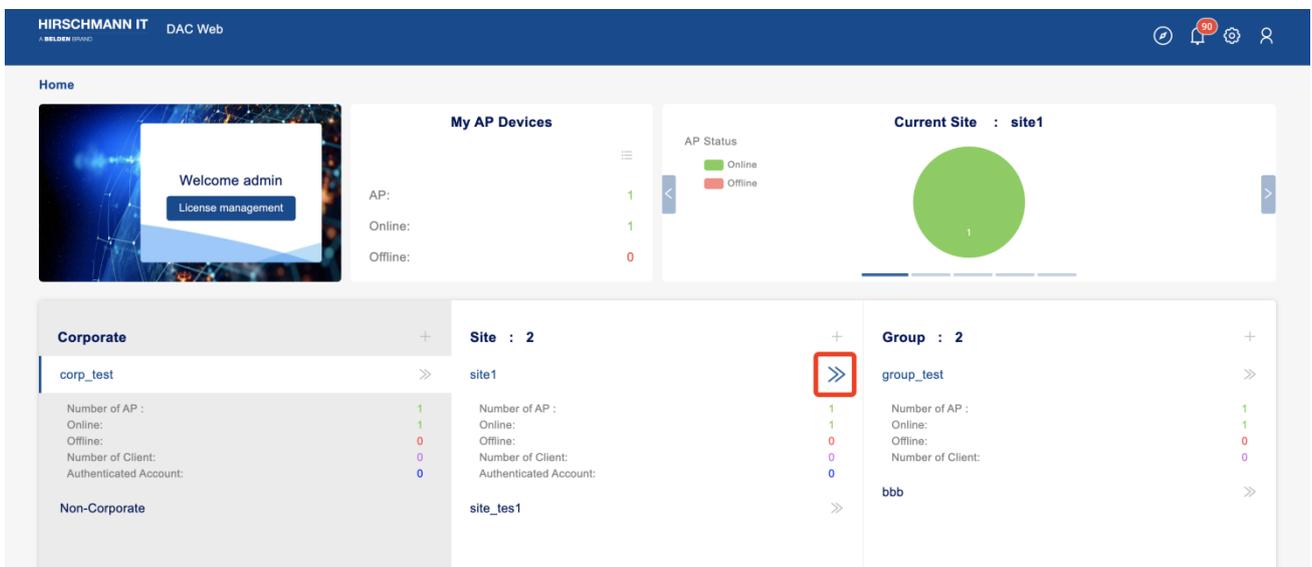


Figure 5-5-1

At this view, you can see the tabs of Dashboard, WLAN, AP, Clients, Authentication, RF, Log, Security, Group And Setting.

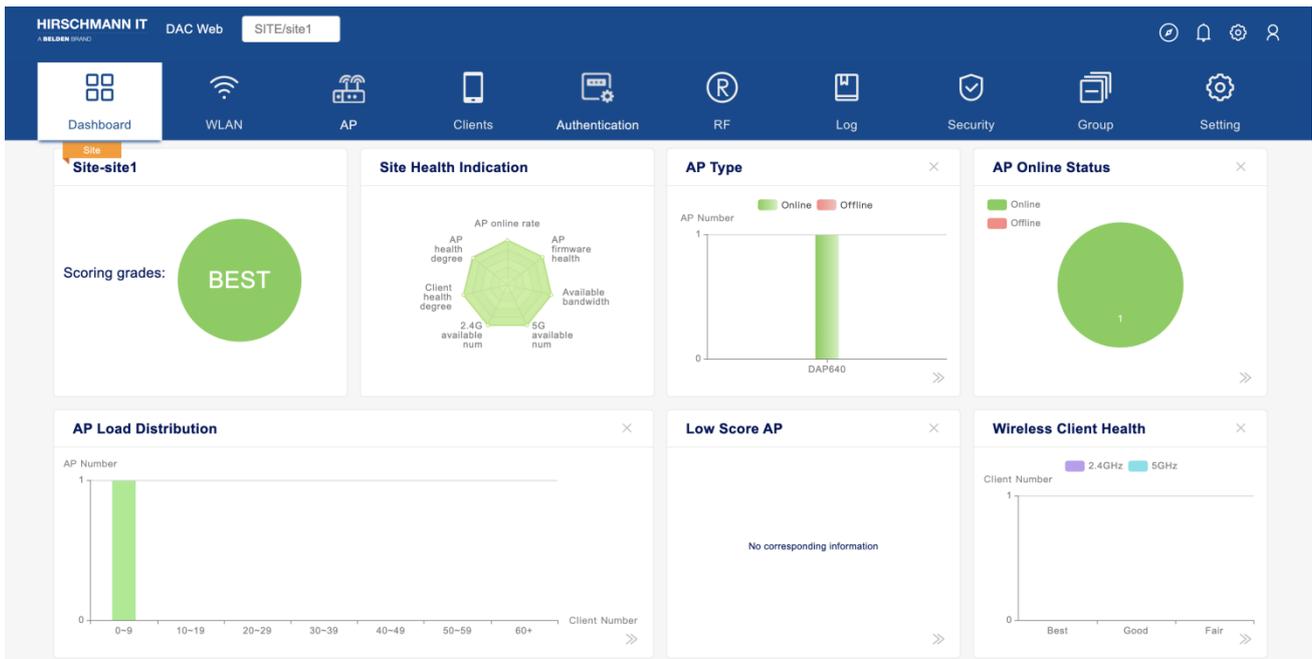


Figure 5-5-2

5.5.1. Dashboard

- **Today's data** - Display the current number of real-time terminals, the number of historical terminals of the day and traffic, the peak number of users counted by day within 7 days, cumulative users, uplink traffic statistics and downlink traffic statistics
- **Site Scoring** - Show the current site health level (best / good / fair / N/a)
- **Site Health Indication** - Display the specific health level details of all AP / terminal / bandwidth dimensions of the current field.
- **AP Type** - The specific model of AP and the corresponding histogram of the number of this model in the "site". The abscissa is the AP model and the ordinate is the number of corresponding models.
- **AP Online Status** - Pie chart percentage of AP online and offline.
- **AP Load Distribution** – Load balance of AP. On the abscissa, we provide seven reference values for the number of attached terminals, which are: < 10, 10, 20, 30, 40, 50, 60 / +, which means the number of attached terminals of AP; The ordinate is the number of APs.
- **Low Score AP** - Provide a list of APs whose scores are lower than the threshold standard, and remind customers to focus on the specific operation status and version information of these APs. The AP list in the low split AP tab is dynamic. If the AP indicators do not meet the threshold

requirements, the AP will be displayed in the tab. Customers can click to directly enter the equipment menu (level-1 menu) to view the specific situation; however, on the premise that the AP indicators restore the threshold requirements, the AP will automatically disappear in the tab. AP threshold indicators will be judged in the following five aspects: AP CPU utilization, AP memory utilization, AP flash memory utilization, number of terminal accesses, and AP used bandwidth

- **Group List** - Show the list of groups under the site
 - **Group Name** - Names of all groups included in this site. You can click the name to enter group view.
 - **AP Number** - Count of AP in this group.
 - **Client Number** - Count of client in this group.
 - **SSID Number** - Count of SSID created in group.
- **WLAN List** - Show the SSID list in this site
 - **SSID** - SSID name of wireless network.
 - **Client Number** - Client Count associated to this SSID.
 - **From** - Site or group, which means SSID is created from site / group
 - **Security** - Wireless security level, can be one of Open, Personal, Enterprise.
- **Wireless Client Health** - In the tab of terminal health, according to the signal strength (RSSI = received signals strength indicators) of the terminal signal uplink to the AP, we provide three levels of access health: the terminal meeting the best RSSI threshold is classified as "best", the terminal meeting the good RSSI threshold is classified as "good", and the terminal meeting the general RSSI threshold is classified as "fair" Level. At the same time, we use color to distinguish the access frequency band of the terminal.
- **Client Type** - The current hardware types of access terminals include computer, mobile and others
- **Operating System** - The operating system OS type of access terminal is intuitively given in the form of pie chart.
- **Current Intrusive AP** - show the proportion of interference AP and Rogue AP under "illegal AP" in the form of pie chart.
- **Current Intrusive Client** - show the proportion of interference AP and Rogue AP under "illegal

AP" in the form of pie chart.

- **Historical statistics** - You can select a time period from the drop-down list
 - **Client Number** - Line Chart of client count
 - **Throughput** - Line Chart of Throughput of this site
 - **Traffic** - Histogram of Traffic

5.5.2. WLAN

Create, modify, and delete SSIDs for the site; See "[WLAN](#)" for more detail.

5.5.3. AP

Provide management and monitoring of AP device; Management includes AP name modification, version management, NTP service management, etc.; Monitoring includes the records of syslog, the system log service for AP, and the key indicators in AP units; See "[AP](#)" section for more detail.

5.5.4. Clients

Provide terminal management and monitoring; Management includes Blocklist processing for terminals with abnormal behavior; Monitoring includes type statistics of terminals, OS type statistics, statistics and queries of various parameters of terminals attached to the network; See "[Clients](#)" section for more detail.

5.5.5. Authentication

Create, modify, and delete authentication and other related policy configurations; See "[Authentication](#)" section for details.

5.5.6. RF

Show AP RF configuration; Set the RF configuration base on the site. Set the RF configuration based on single AP (with higher priority than site configuration); See "[RF](#)" section for more details.

5.5.7. Log

Log of system or log of Device. See "Log" section for details.

5.5.8. Security

Configure Rogue AP strategy and wireless attack detection strategy; The wireless attack detection strategy includes: AP attack detection strategy, terminal attack detection strategy and Blocklist strategy; Statistics of illegal AP records, including interference AP, Rogue AP, attack AP and valid AP; Statistics of jamming terminal records, including: terminals associated with jamming AP, terminals associated with Rogue AP, terminals detected by terminal attack and terminals entered into Blocklist; Attack ranking statistics; See "Security" for more details.

5.5.9. Group

The entrance of the group belonging to the site; You can see all Group of this site, and each Group is shown in card.

Scoring Grades - Show the group health level (best / good / fair / N / a)

Health - Display the specific health level details of all AP / terminal / bandwidth dimensions of the current field.

AP - Online and Offline AP number.

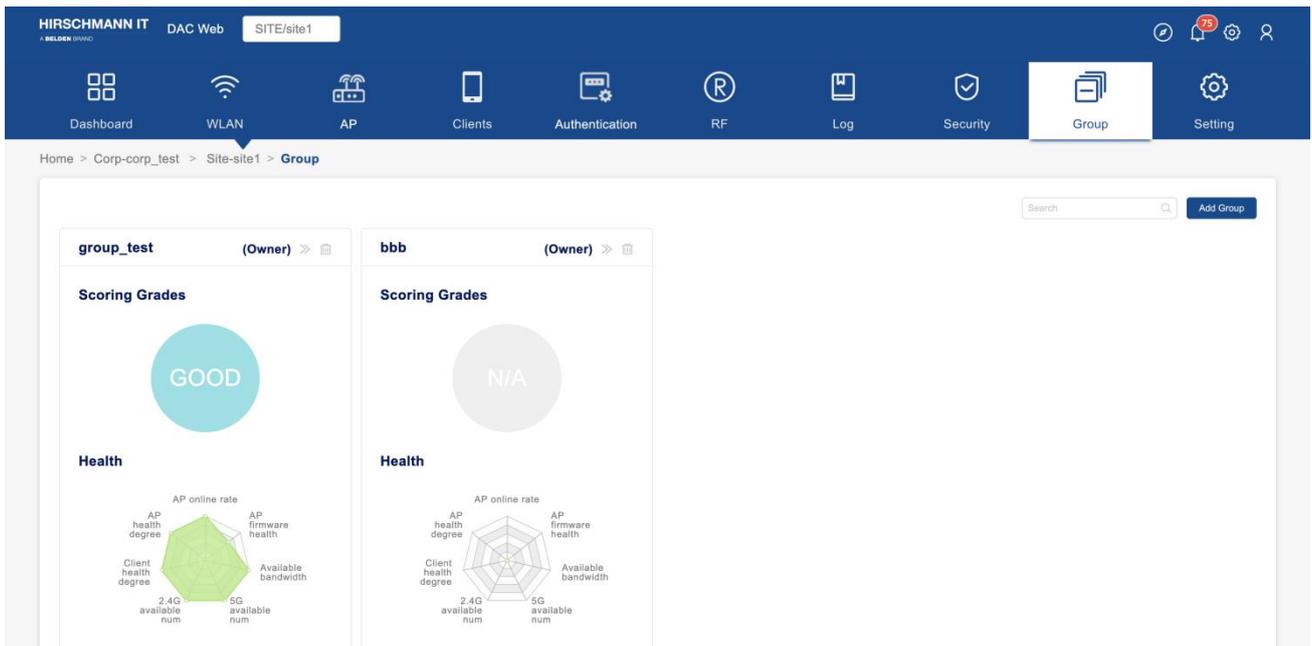


Figure 5-5-9-1

Create A Group

Click **Add Group** button, the **create group** window will open Input the Name and Description, Click Save button to save the group. Then you can see the new Group in the Group page.

Delete A Group

Click Delete Icon in the Group card, Click **Yes** button at the confirmation prompt.

5.5.10. Setting

Settings of this site.

Basic Information/Setting

- **Site Operation**

- **Edit** - Change site name or description.
- **Delete** - Delete this site.
- **Transfer Site** - Transfer site owner permissions to other users
- **Join Corporate** - You can assign this site to a Corporate by this function.

- **Corporate Operation** - will display after assign this Site to a Corporate
 - **Quit Corp** - Remove the current site from corporate.

Authorization Management

You can add other users to manage this Site. Only owner of this Site can view this feature.

- Administrator list
 - **User Name** - User Name
 - **Email** - Email
 - **Status** - success/fail
 - **Telephone** - Telephone of this user
 - **Character** - Character can be Manager/Viewer/Guest Operator

Add administrator

Click + icon to open Add administrator dialog, input User name or Email that you want to add. Select Character(Manager/Viewer/Guest Operator). Click **Save** to save it.

If the user account does not exist, you can use the target user's email to invite registration. The target user can register the account after receiving the registration invitation email. The registered account will have the corresponding permissions of the current site. You can see [Create Account](#) to get more information.

Delete administrator

Select the administrator who you want to delete, click delete icon, then click **Yes** at the confirmation prompt.

5.6. Group View

5.6.1. Dashboard

- **Today's data** - Display the current number of real-time terminals, the number of historical terminals of the day and traffic, the peak number of users counted by day within 7 days, cumulative users, uplink traffic statistics and downlink traffic statistics

- **Group Name** - Show the current group health level (best / good / fair / N / a)
- **Group Health Indication** - Display the specific health level details of all AP / terminal / bandwidth dimensions of the current field.
- **AP Type** - The specific model of AP and the corresponding histogram of the number of this model in the "site". The abscissa is the AP model and the ordinate is the number of corresponding models.
- **AP Online Status** - Pie chart percentage of AP online and offline.
- **AP Load Distribution** – Load balance of AP. On the abscissa, we provide seven reference values for the number of attached terminals, which are: < 10, 10, 20, 30, 40, 50, 60 / +, which means the number of attached terminals of AP; The ordinate is the number of APS.
- **Low Score AP** - Provide a list of APs whose scores are lower than the threshold standard, and remind customers to focus on the specific operation status and version information of these APS. The AP list in the low split AP tab is dynamic. If the AP indicators do not meet the threshold requirements, the AP will be displayed in the tab. Customers can click to directly enter the equipment menu (level-1 menu) to view the specific situation; however, on the premise that the AP indicators restore the threshold requirements, the AP will automatically disappear in the tab. AP threshold indicators will be judged in the following five aspects: AP CPU utilization, AP memory utilization, AP flash memory utilization, number of terminal accesses, and AP used bandwidth
- **WLAN List** - Show the SSID list in this group and its site
 - **SSID** - SSID name of wireless network.
 - **Client Number** - Client Count associated to this SSID.
 - **From** - Site or group, which means SSID is created from site / group
 - **Security** - Wireless security level, can be one of Open, Personal, Enterprise.
- **Wireless Client Health** - In the tab of terminal health, according to the signal strength (RSSI = received signals strength indicators) of the terminal signal uplink to the AP, we provide three levels of access health: the terminal meeting the best RSSI threshold is classified as "best", the terminal meeting the good RSSI threshold is classified as "good", and the terminal meeting the general RSSI threshold is classified as "fair" Level. At the same time, we use color to distinguish the access frequency band of the terminal.
- **Client Type** - The current hardware types of access terminals include computer, mobile and

others

- **Operating System** - The operating system OS type of access terminal is intuitively given in the form of pie chart.
- **Current Intrusive AP** - show the proportion of interference AP and Rogue AP under "illegal AP" in the form of pie chart.
- **Current Intrusive Client** - show the proportion of interference AP and Rogue AP under "illegal AP" in the form of pie chart.
- **Historical statistics** - You can select a period from the drop-down list
 - **Client Number** - Line Chart of client count
 - **Throughput** - Line Chart of Throughput of this site
 - **Traffic** - Histogram of Traffic

5.6.2. WLAN

Create, modify and delete wireless networks for the group; See "[Wireless Profile](#)" for more detail.

5.6.3. AP

Provide monitoring of AP device in this Group; Monitoring includes the records of syslog, the system log service for AP, and the key indicators in AP units; See "[AP](#)" section for more detail.

5.6.4. Clients

Provide terminal management and monitoring; Management includes Blocklist processing for terminals with abnormal behavior; Monitoring includes type statistics of terminals, OS type statistics, statistics and queries of various parameters of terminals attached to the network; See "[Clients](#)" section for more detail.

5.6.5. Authentication

Create, modify and delete authentication and other related policy configurations; See "authentication profiles" section for details.

5.6.6. RF

Show AP RF configuration; On the RF page of the group, you can only view the configuration of RF, cannot modify it.

5.6.7. Log

Log of system or log of Device. See "Log" section for details.

5.6.8. Security

You can see the AP Record, Client Record, Blocklist at this Page. If you want to Configure Rogue AP strategy and wireless attack detection strategy and so on, please go to Security View of Site.

5.6.9. Setting

Settings of this group.

Basic Information/Setting

- Group Operation
 - **Edit** - Change group name or description.
 - **Delete** - Delete this group.

Authorization Management

You can add other users to manage this Group. Only owner of Group can view this feature.

- Administrator list
 - **User Name** - User Name
 - **Email** - Email
 - **Status** - success/fail
 - **Telephone** - Telephone of this user
 - **Character** - Character can be admin or viewer

Add administrator

Click + icon to open Add administrator dialog, input User name or Email who you want to add. Select Character(admin/guestoperator/viewer). Click **Save** to save it.

Delete administrator

Select the administrator who you want to delete, click delete icon, then click **Yes** at the confirmation prompt.

6. License

Currently, DAC has two kinds of license:

- Basic License - Including Basic Function(create WLAN, terminal display and statistics, etc) and Client Access Function. Basic function is authorized based on the total number of APs, and Client Access function is authorized based on the total number of authentication terminals.
- Security License - Wireless security, include WIDS and WIPS. The security license is authorized based on the number of APs.

The licenses you can purchase are as follows:

Types	Part number	Part name	Description
Basic License	942999321	DAC-50	Software DAC platform with license for 50 AP and 1000 clients
	942999322	DAC-256	Software DAC platform with license for 256 AP and 5000 clients
	942999323	DAC-500	Software DAC platform with license for 500 AP and 10000 clients
	942999324	DAC-1000	Software DAC platform with license for 1000 AP and 20000 clients
Security License	942999327	DAC-Sec-50	Software DAC platform security features license for 50 AP
	942999328	DAC-Sec-256	Software DAC platform security features license for 256 AP
	942999329	DAC-Sec-500	Software DAC platform security features license for 500 AP
	942999330	DAC-Sec-1000	Software DAC platform security features license for 1000 AP

Table 6-1

The carrier of license is in the form of license code. According to the customer's actual purchase of AP products, they are distributed to the customer. The customer can activate the license code on the Web GUI and observe the consumption count from the Web GUI at any time.

You can click **License management** button at home page of user to bring up license Screen.

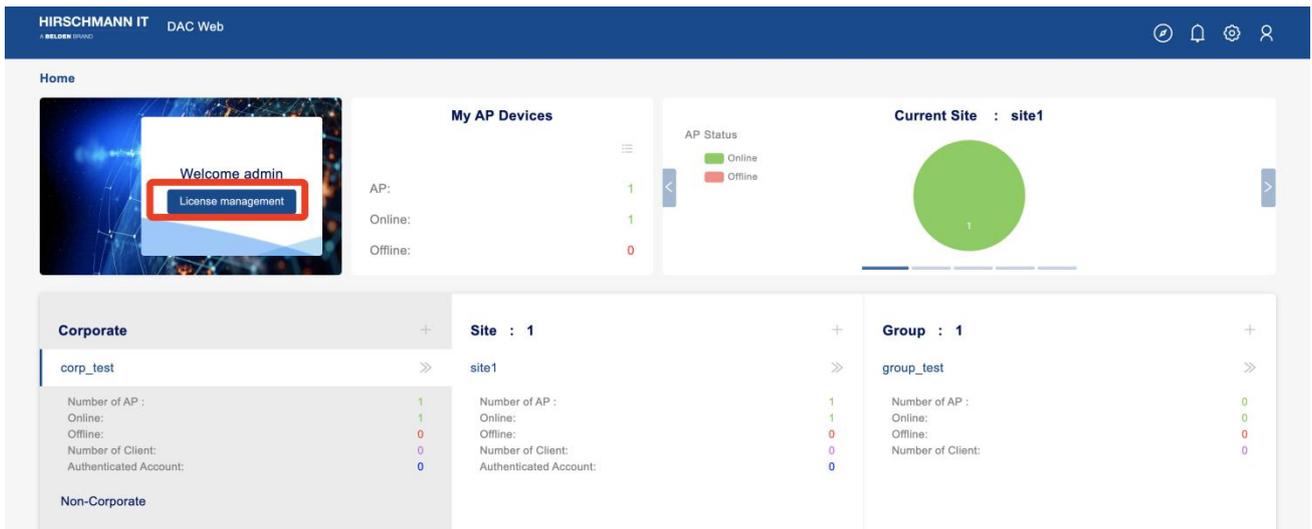


Figure 6-2

This chapter contains the following topics:

- [License Activation](#)
- [License Management](#)
- [License Record](#)
- [Device Code](#)

6.1. License Activation

At this page, you can active license code.

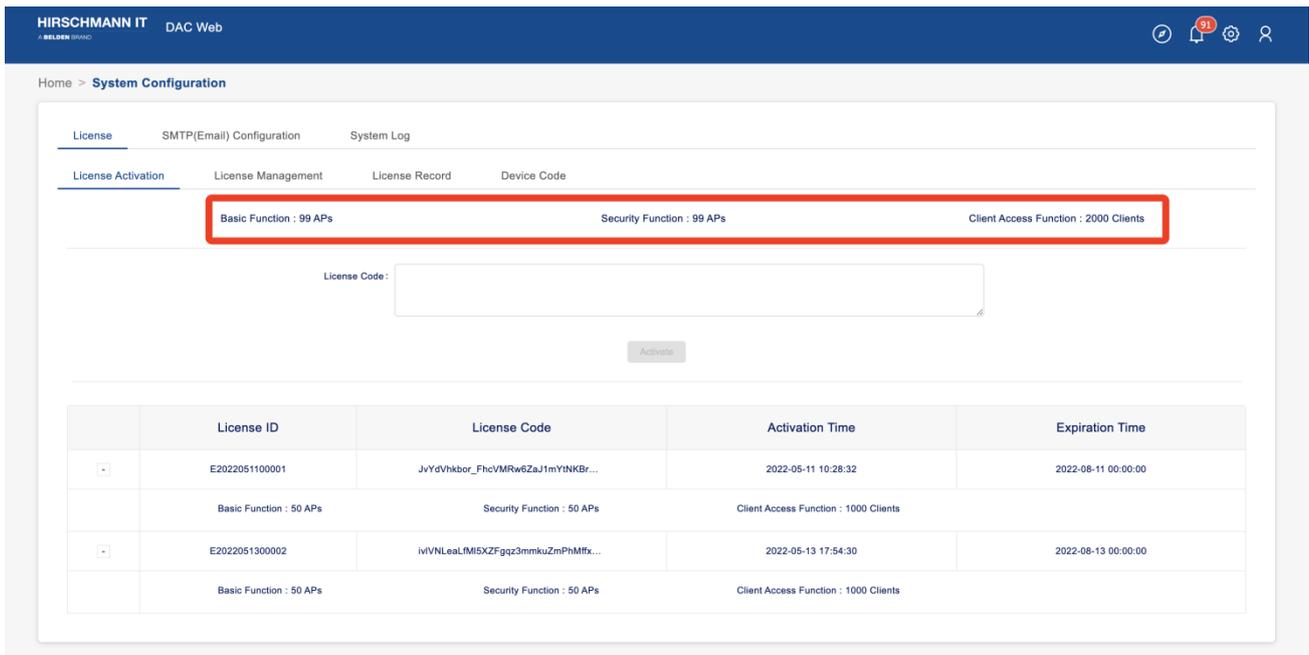


Figure 6-1-1

Fill in the license code obtained from the supplier into the input box and click **Active** button; then you can see the details of this license code. The details include points count of each function. Click **Activation** button on the detail window to activate this license. And then, you can see the newly activated licenses in the list of activated licenses.

If you have activated multiple licenses, you can view the actual activated functions and the number of functions of each license. At the same time, you can see the remaining APs count of Basic Functions, the remaining count of terminals that can be authenticated, and the remaining APs count of Security Functions.

List of activated licenses

- **License ID** - License ID.
- **License Code** - License Code.
- **Activate Time** - The Time that you active this License.
- **Expiration Time** - When the expiration time comes, the count of devices in the license will not be available.

The expiration date of the official license purchase is 2099-12-31; The expiration time of the trial license is 3 months from the date of the trial request.

6.2. License Management

On this page, you can manage and assign your license;

Select the corresponding site and click the function switch, then click **Yes** button to confirm to enable function.

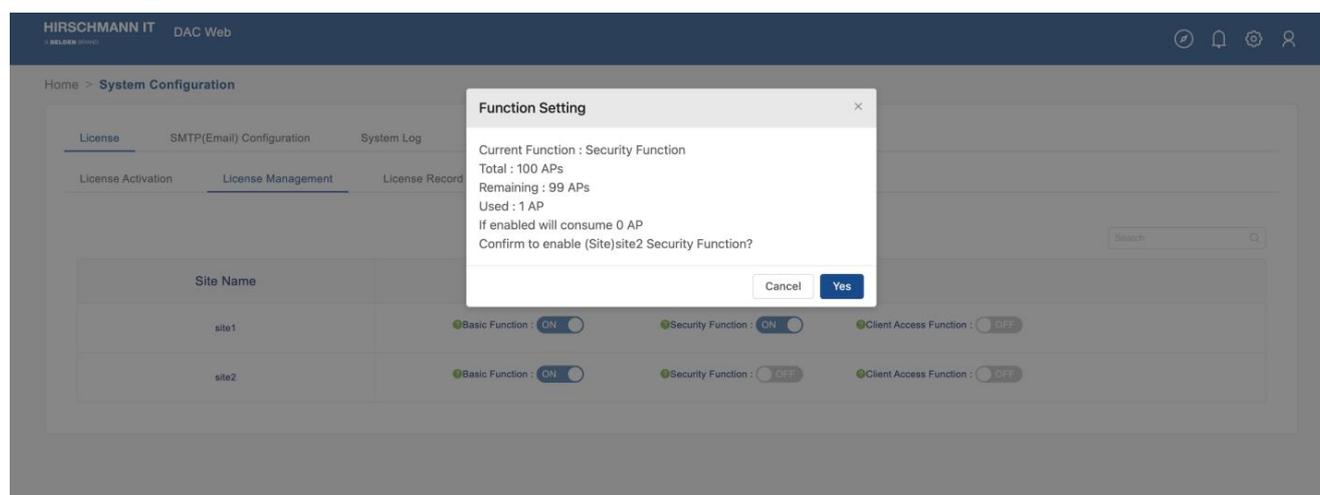


Figure 6-1-1

The total number of APS that can enable Basic Functions in all Site is less than or equal to the total number of unexpired Basic Function licenses. The total number of APS that can enable Security Functions in all Site is less than or equal to the total number of unexpired Security Function licenses. The total number of access clients that can authentication in all Site is less than or equal to the total number of unexpired Client Access Function.

6.3. License Record

Display the usage of each function in each site and the remaining / expired points of the current account based on the function. You can select Function to display at the drop down menu.

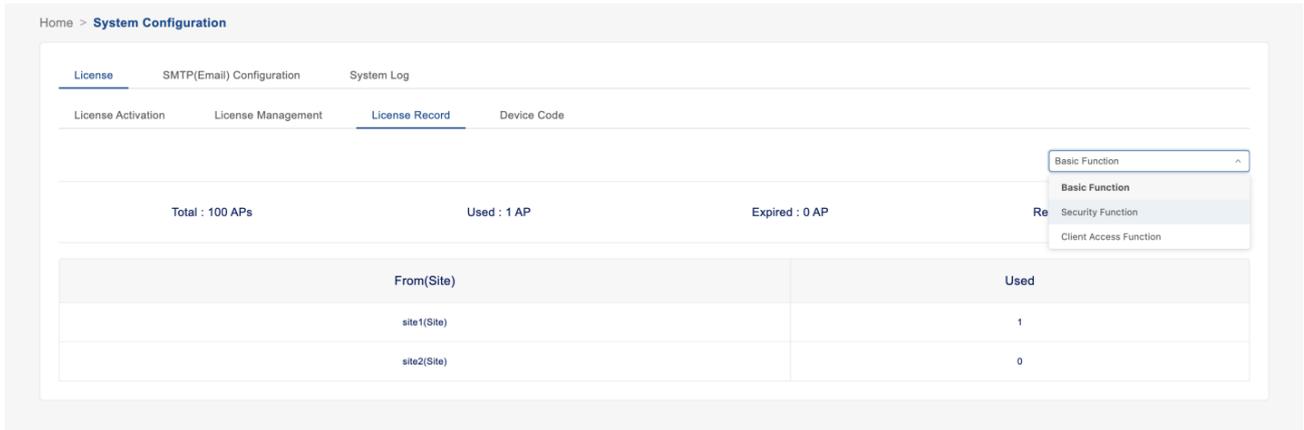


Figure 6-3-1

6.4. Device Code

Device code is the fingerprint of the DAC. When you want to apply for a license, you need to provide the device code to your supplier. The supplier will generate license code, which can only be applied to the current device, based on this device code.

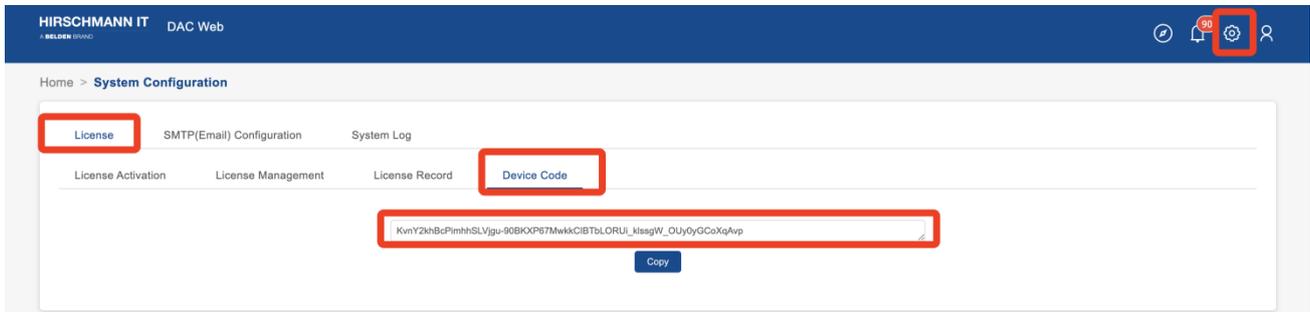


Figure 6-4-1

7. WLAN

This section describes the basic principles of wireless access and how to create / modify WLAN. You can configure WLAN in Site or Group View.

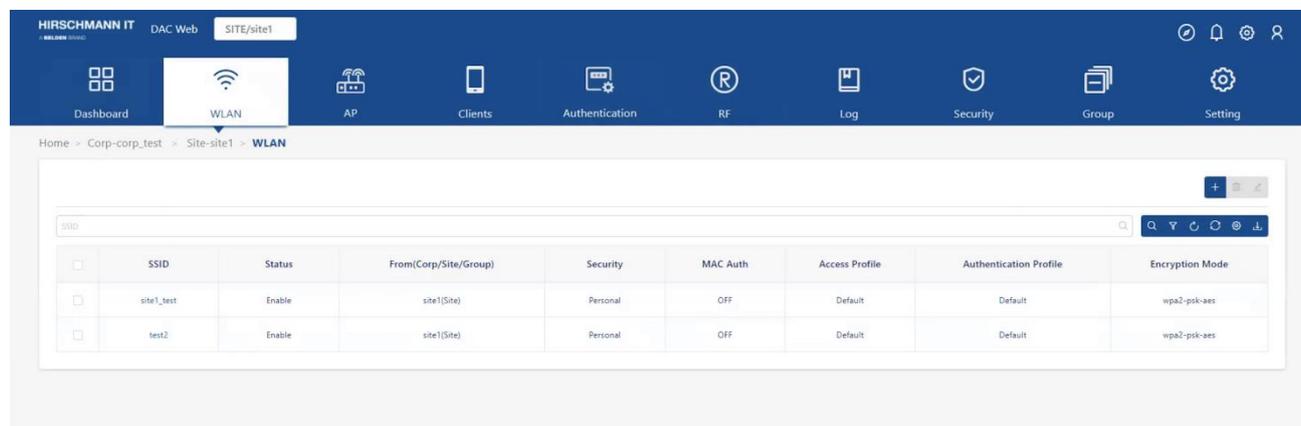


Figure 7-1

During start up, a wireless client searches for radio signals or beacon frames that originate from the nearest DAP. After locating the DAP, the following transactions take place between the client and the DAP:

- **WLAN Access Authentication** - When a wireless client attempts to connect to the DAP, the DAP needs to authenticate the client accordingly. The authentication method depends on the WLAN Security Level and is also affected by the MAC Authentication status on the WLAN.
- **WLAN Connection** - After successful WLAN Access Authentication, the client establishes a connection with the DAP.
- **Network Access(Captive Portal) Authentication** - After the client establishes a connection with DAP, it can further initiate Captive Portal Authentication as needed. It's not necessary.

This chapter contains the following topics:

- [Security Level](#)
- [Mac Authentication](#)
- [Create WLAN Service](#)
- [Edit WLAN Service](#)

- [Delete WLAN Service](#)

7.1. Security Level

- **Open** - The Wi-Fi without any security configuration.
- **Personal** - The Wi-Fi will be protected by a key. DAP will Authenticate the client by verification the Passphrase.
- **Enterprise** - An authentication server will be used to authenticate the connecting client via 802.1x Authentication.

7.2. Mac Authentication

MAC-based authentication authenticates devices based on their physical Media Access Control (MAC) address. While not the most secure and scalable method, MAC-based authentication implicitly provides an addition layer of security authentication devices. MAC-based authentication is often used to authenticate and allow network access through certain devices while denying access to the rest.

7.3. Create WLAN

Click >> at the site that you want to create WLAN to Enter the site view.

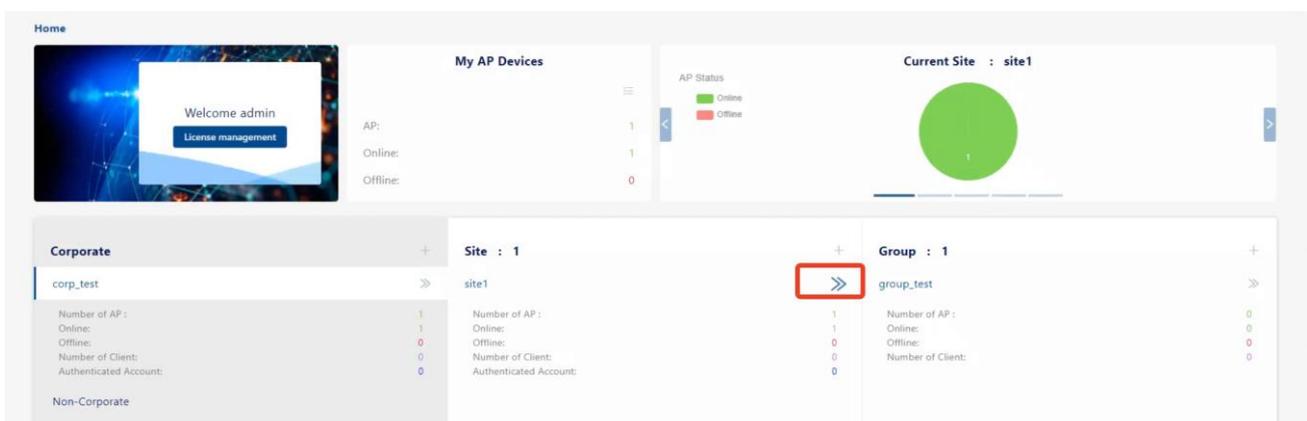


Figure 7-3-1

Click WLAN to enter WLAN list page.

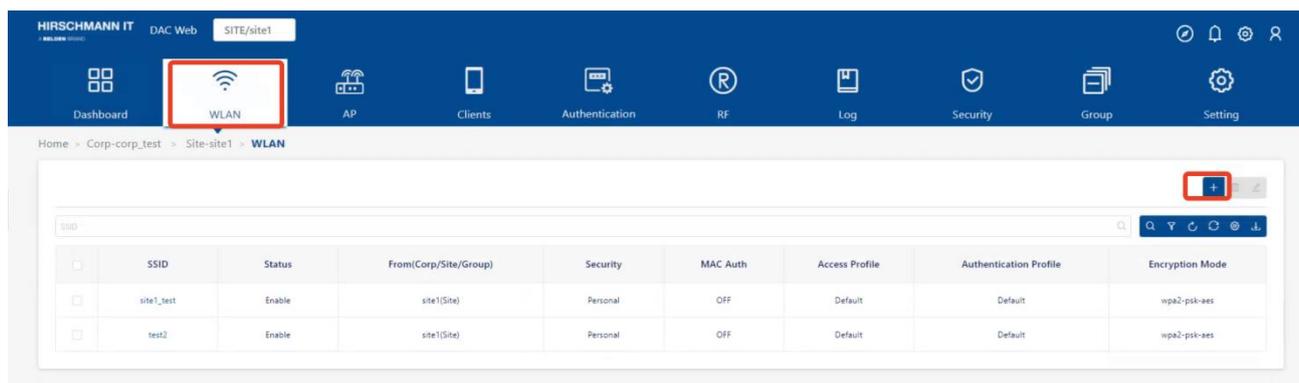


Figure 7-3-2

On the WLAN tab of the Site/Group View, Click the '+' icon on the head of WLAN List Table. The Create WLAN Service window will display.

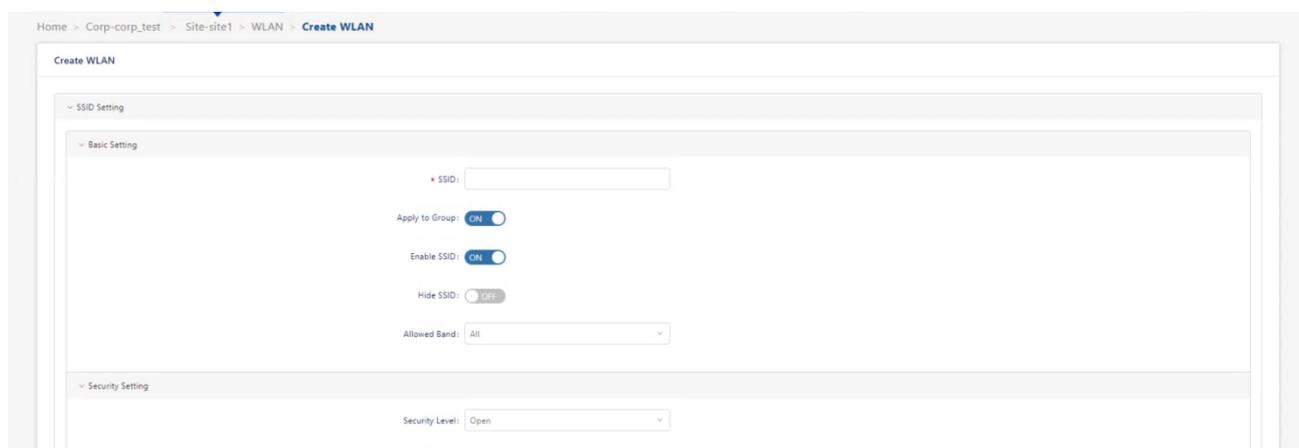


Figure 7-3-3

7.3.1. SSID Setting

Basic Setting

- **SSID** - User configured name that uniquely identifies a wireless network (up to 32 characters). If the SSID includes spaces, you must enclose it in quotation marks.
- **Apply to Group** - Does the WLAN take effect in the APs which is assigned to Group.
- **Hide SSID** - Enables/Disables SSID in beacon frames. Note that hiding the SSID does very little to increase security. (Default = Disabled)
- **Enable SSID** - Enables/Disables the SSID.

- **Allowed Band** - The band(s) available on the service:
 - 2.4 GHz
 - 5 GHz
 - All - 5 GHz and 2.4 GHz(default)

Security Setting

- **Security Level** - Select the security level for the WLAN Service:
- **Open** - The Wi-Fi will be unsecured. However, you can configure a default role or enable MAC Authentication to assign a role for clients.
- **Personal** - The Wi-Fi will be protected by a key. Select an Encryption Type from the drop-down menu, then enter a Passphrase.
 - **WPA_PSK_AES** - WPA with AES encryption using a pre-shared key.
 - **WPA_PSK_AES_TKIP** - WPA with TKIP and AES mixed encryption using a pre-shared key.
 - **WPA2_PSK_TKIP** - WPA2 with TKIP encryption using a pre-shared key.
 - **WPA2_PSK_AES** - WPA2 with AES encryption using a pre-shared key.
 - **WPA3_SAE_AES** - WPA3 with AES encryption using a pre-shared key, which ONLY allow WPA3 capable client accessing.
 - **WPA3_PSK_SAE_AES** - WPA3 and WPA2 mixed mode, which allow both WPA3 capable client as well as ONLY WPA2 capable client accessing.
- **Enterprise** - An authentication server will be used to authenticate the connecting client via 802.1X Authentication. Select an Encryption Type from the drop-down menu:
 - **DYNAMIC_WEP** - WEP with dynamic keys.
 - **WPA_TKIP** - WPA with TKIP encryption and dynamic keys using 802.1X.
 - **WPA2_TKIP** - WPA2 with TKIP encryption and dynamic keys using 802.1X.
 - **WPA2_AES** - WPA2 with AES encryption and dynamic keys using 802.1X.
 - **WPA3_AES256** - WPA3 with CNSA (Suite B) using 802.1X. Note that when WPA3_AES256 encryption is applied to an AP that does not support it, the encryption will automatically fall back to WPA2_AES.
 - **WPA3_AES** - WPA3 with AES encryption and dynamic keys using 802.1X.

- **Device Specific PSK** - Device Specific PSK provides more security than traditional PSK. If Device Specific PSK is enabled on a wireless network and a device is configured for Device Specific PSK, when the AAA Server sends the Radius Access Accept for MAC Authentication for the device, it will also send the specific pre-shared key for that device, differentiated by the device's MAC Address. This means that each device will have a different key. You can set Device Specific PSK for a MAC Address at [Company Device](#).
 - **Enable/Disabled** - Enables/Disables Device Specific PSK.
 - **Prefer Device Specific PSK** - by AAA Server will be always use Prefer Device Specific PSK - If the AAA Server sends the "AES-CBC-128" attribute along with the Radius Access Accept response, this value will be used. If the AAA server does NOT send the "AES-CBC-128" attribute, the key configured in the SSID will be used.
 - **Force Device Specific PSK** - The value of "AES-CBC-128" attribute returned d, whether it exists or not. Device Specific PSK can not work with a External RADIUS Server. Devices are configured for Device Specific PSK on the [Company Device](#).
- **MAC Auth** - Enables/Disables MAC Authentication.
- **Default Access Role Profile** - Select the default Access Role Profile that will be applied to clients if a role cannot be assigned by other role assignment methods. About Access Role Profile, see section "[Access Role Profile](#)" to get more information.
- **Authentication Profile**
 - **Default - Default** provides an easy and fast configuration way. Selecting **Default** means that you can select the web portal authentication of **Guest** or **Employee** for the current SSID, or set the access SSID for Company Device.
 - **Customization** - You need to manually create Access Policy, Authentication Strategy, even Guest Access Strategy or Employee Access Strategy. Please refer to the [Authentication](#) section for more details.
- **Authentication Type** - Can only be set when Authentication Profile set to Default.
 - **Guest** - This SSID is used for Guest access. You can customize the Portal Page by click Customization Page button.
 - **Employee** - This SSID is used for Employee access. You can customize the Portal Page by click Customization Page button.
 - **Company Device** - Set this SSID for devices owned by a company that can be assigned to

an employee for daily use (e.g., printers, IP phones, laptops, tablets). It is base on MAC authenticate. you can add Company Device MAC at Authentication - > Setting - > Company Device. See more informations by click [Company Device](#).

- **Customization Page** - Select the template page for web portal authentication, and customize the page as required. Can only set when the Authentication Type set to Guest or Employee.
- **PMF-Protected Management Frames** - Configures whether connections are accepted from clients supporting Protected Management Frame for certain Security Levels/Encryption Types (Enterprise - WPA2_AES / WPA3_AES256 / WPA3AES, Personal - WPA2_PSK_AES / WPA3_SAE_AES / WPA3_PSK_SAE_AES)
 - **Disabled** - Disables Protected Management Frame requirements. Protected Management Frame is required for WPA3 encryptions and cannot be disabled. The field is not configurable for WPA3 encryptions.
 - **Optional** - Allows connections from clients supporting Protected Management Frame and clients that do not.
 - **Required** - Only allows connections from clients supporting Protected Management Frame.

Advance Setting

- **Maximum clients allowed of single AP of this WLAN** - The maximum number of clients allowed under single AP and single band. The maximum number of terminals under the current SSID of the current AP(Range = 1 - 256, Default = 64)
- **WLAN Timing** - Control WLAN broadcast SSID by time. Turn on the switch and you will see more sub options.
 - **WLAN Work Cycle**
 - ◆ **Daily** - WLAN broadcast SSID every day.
 - ◆ **Weekday** - WLAN broadcast SSID every weekday.
 - ◆ **Weekend** - WLAN broadcast SSID every weekend.
 - **Custom WLAN work schedule** - enable/disable special time range configure on work cycle.
 - **WLAN work schedule** - select the time range.
- **802.11r** - Enables/Disables IEEE 802.11r (Fast BSS Transition). The Fast BSS Transition mechanism minimizes the delay when a client transitions from one BSS to another within the

same group.

- **User Access Limit of 802.11b/g** - The client is only allowed to connect in 802.11b/g mode. (For debug sometimes)
- **L3 Roaming** - Enables/Disables Layer 3 roaming. Layer 3 roaming allows client to move between Access Points and connect to a new IP subnet and VLAN.
- **Client Isolation** - Enables/Disables Client Isolation. If enabled, traffic between clients on the same AP in the SSID is blocked; client traffic can only go toward the router. (Default = Disabled)
- **802.11k** - Enables/Disables 802.11k. The 802.11k protocol enables APs and clients to dynamically measure the available radio resources. When 802.11k is enabled, APs and clients send neighbor reports, beacon reports, and link measurement reports to each other.
- **802.11v** - Enables/Disables 802.11v. 802.11v standard defines mechanisms for wireless network management enhancements and BSS transition management. It allows client devices to exchange information about the network topology and RF environment. The BSS transition management mechanism enables a DAP to request a voice client to transition to a specific AP, or suggest a set of preferred APs to a client due to network load balancing or BSS termination. It also helps the client identify the best AP to transition to as they roam.
- **2.4G Data Frame Rate** - 2.4G band client with lower data speed will not be given access, recommended value 12.
- **2.4G Manage Frame Rate** - 2.4G band wireless management frame transmit rate. Higher value means less coverage; lower value means larger coverage.
- **5G Data Frame Rate** - 5G band client with lower data speed will not be given access, recommended value 24.
- **5G Manage Frame Rate** - 5G band wireless management frame transmit rate. Higher value means less coverage; lower value means larger coverage.

7.3.2. QoS Settings

Configure the wireless QoS Settings for the profile as detailed below.

Bandwidth Contract

- **Upstream Bandwidth** - The maximum bandwidth for traffic from the AP to the client

- **Downstream Bandwidth** - The maximum bandwidth for traffic from the client to the AP.
- **Upstream Burst** - The maximum bucket size used for traffic from the AP to the client. The bucket size determines how much the traffic can burst over the maximum bandwidth rate.
- **Downstream Burst** -The maximum bucket size used for traffic from the client to the AP. The bucket size determines how much the traffic can burst over the maximum bandwidth rate.

802.1p Mapping Setting

Used to configure the uplink and downlink mapping mechanism between Wi-Fi Multimedia (WMM) Access Categories and 802.1p priority. Uplink traffic can only be mapped to a single value. Downlink traffic can be mapped to multiple values. Fields are populated with the default values. To modify a default uplink value, enter a new value in the field. To modify a default downlink value, enter a new value and click on the Add icon. To remove a value, click on the "x" next to the value.

- **Enable** - If enabled, the original 802.11p mapping for traffic is trusted (Default - Disabled).
- **Background** - WMM Background will be mapped to the 802.1p value.
 - **Uplink** - Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 1)
 - **Downlink** - Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 1, 2)
- **Best Effort** - WMM Best Effort will be mapped to the 802.1p value.
 - **Uplink** - Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 0)
 - **Downlink** - Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 0, 3)
- **Video** - WMM Video will be mapped to the 802.1p value.
 - **Uplink** - Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 4)
 - **Downlink** - Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 4, 5)
- **Voice** - WMM Voice will be mapped to the 802.1p value.
 - **Uplink** - Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 6)
 - **Downlink** - Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 6, 7)

DSCP Mapping Settings

Used to configure the uplink and downlink mapping mechanism between Wi-Fi Multimedia (WMM) Access Categories and DSCP priority. Uplink traffic can only be mapped to a single value. Downlink traffic can be mapped to multiple values. Fields are populated with the default values. To modify a default uplink value, enter a new value in the field. To modify a default downlink value, enter a new value and click on the Add

icon. To remove a value, click on the "x" next to the value.

- **Enable** - If enabled, the original DSCP mapping for traffic is trusted (Default - Disabled).
- **Background** - WMM Background will be mapped to the 802.1p value.
 - **Uplink** - Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 10)
 - **Downlink** - Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 2, 10)
- **Best Effort** - WMM Best Effort will be mapped to the 802.1p value.
 - **Uplink** - Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 0)
 - **Downlink** - Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 0, 18)
- **Video** - WMM Video will be mapped to the 802.1p value.
 - **Uplink** - Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 40)
 - **Downlink** - Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 24, 36, 40)
- **Voice** - WMM Voice will be mapped to the 802.1p value.
 - **Uplink** - Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 46)
 - **Downlink** - Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 46, 48, 56)

7.3.3. Broadcast/Multicast Optimization Settings

- **Broadcast Key Rotation** - Enables/Disables the broadcast key rotation function. If enabled, the broadcast key will be rotated after every interval time.
- **Broadcast Key Rotation Time Interval** - The interval, in minutes, to rotate the broadcast key (Range = 1 - 1440, Default = 15).
- **Broadcast Filter All** - Enables/Disables broadcast filtering. If enabled, all broadcast frames are dropped, except DHCP and Address Resolution Protocol (ARP) frames.
- **Broadcast Filter ARP** - Enables/Disables broadcast filtering for ARP. If enabled, the AP will act as an "ARP Proxy". If the ARP-request packet requests a client's MAC address and the AP knows the client's MAC and IP address, the AP will respond to the ARP-request but not forward the ARP-request (broadcast) to all broadcast domains. This reduces ARP broadcast packet forwarding and significantly improves network performance. Note that APs do not act as ARP proxy for

Gratuitous ARP packets. When the station gets an IP from DHCP or IP release/ renew, the station will send Gratuitous ARP packets. AP will not respond to such special ARP packets and broadcast them normally.

- **Multicast Optimization** - Enable/Disables multicast traffic rate optimization.
- **Multicast Based Channel Utilization** - Configures based channel utilization optimization percentage. (Range = 0 - 100, Default = 90)
- **Number of Clients** - Configure the threshold for multicast optimization. This is the maximum number of high throughput.

7.4. Edit WLAN

Select the WLAN from the WLAN list and click on the Edit icon to bring up the Edit WLAN Service screen. Edit the fields as described above then click on the **Immediately edit** button to save the changes to the server.

7.5. Delete WLAN

Select the WLAN from the WLAN list, and click on the Delete icon, then click **Yes** at the confirmation prompt. This removes the profile from the server.

8. AP

The AP Screen displays information about all DAP assigned to this site. You can configure APs NTP, update firmware of AP, reboot an AP, set APs LED Mode, and perform certain actions on APs (e.g., open the Web UI of Device to manage an individual AP, do some actions like ping/traceroute from an individual AP), and so on.

Click >> at the site that you want to manage to Enter the site view.

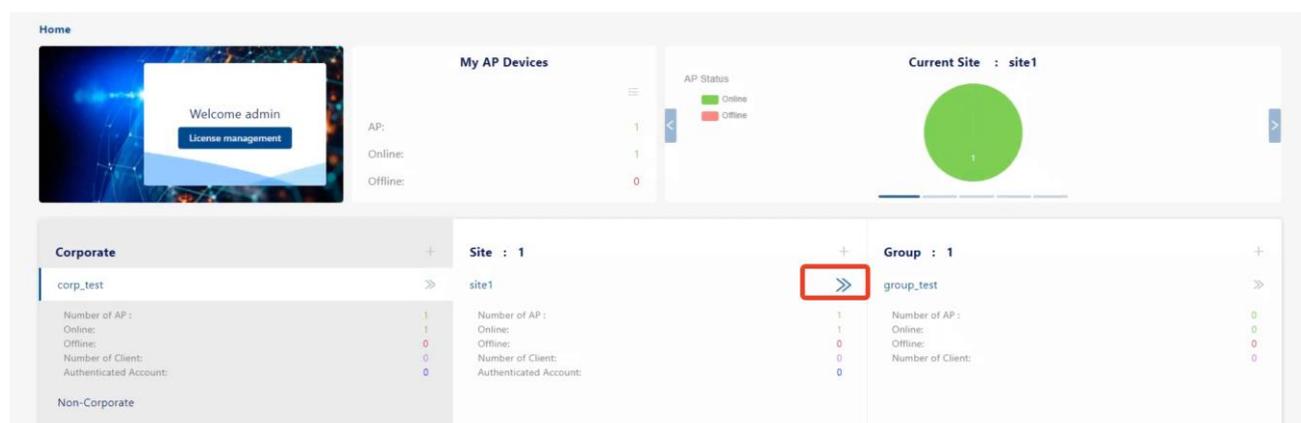


Figure 8-1

Click AP icon to bring up AP Screen.

This chapter contains the following topics:

- [Device List](#)
- [Configurations for AP](#)
- [Configure Bluetooth](#)
- [Reporting Config](#)
- [Operation Tools](#)
- [Do Actions from AP](#)
- [Device Connection Record](#)

8.1. Device List

This list shows all AP devices in current Site. You can filter the device according to the basic functions of the AP (including Wireless and Bluetooth). Select **All Devices** means that table will show all devices in this Site, select **Devices with WLAN** means that table will show devices has WLAN function, select **Devices with Bluetooth** means that table will show devices has Bluetooth function.

The screenshot shows the DAC Web interface for Hirschmann IT. The top navigation bar includes 'Dashboard', 'WLAN', 'AP', 'Clients', 'Authentication', 'RF', 'Log', 'Security', 'Group', and 'Setting'. The breadcrumb trail is 'Home > Corp-corp_test > Site-site1 > AP > Device List'. The main content area has filter tabs for 'All Devices', 'Devices with WLAN', and 'Devices with Bluetooth'. Below the filters are various configuration buttons for System Config (Fragmentation, IGMP Snooping/OFF, Turn ON Telnet, Turn OFF Telnet, Turn OFF LED, Turn OFF USB, AP Firmware, System Syslog, AP Syslog, NTP, AP WebUI, Set Group, PMD), Bluetooth Config (Site Wireless Uplink, AP Wireless Uplink, Site Uplink/Fallback, Bluetooth Gateway, Site Bluetooth, AP Bluetooth, Site Bluetooth/Fallback), Reporting Config (Site Reporting, AP Reporting, Site Reporting/Fallback), and Operation Tools (Connectivity Test, Reboot, Log Snapshot, Export All Device, Action). A table below displays device information with columns: Name/MAC/IP/Firmware/Group/Model/Location, MAC, Name, Group, Firmware, Model, License, IP, Status, Client Number, Working Mode, Location, Online Duration, and Li. One device is listed with MAC 94-AE-E3-0B-A4-40, Name AP-A4-40, Group group_test, Firmware 4.0.3.4060, Model DAP640, License Enable, IP 192.168.4.48, Status Online, Client Number 0, Working Mode Normal Mode, Location, Online Duration 35d 3h 9m 20s, and Li 20. The footer of the table indicates 'Total 1 Items, showing 1 Items'.

Figure 8-1-1

- **MAC** - MAC address of device
- **Name** - Device Name
- **Group** - Group of the device.
- **Firmware** - Firmware version of device.
- **Model** - The model type of the Device (e.g., DAP640).
- **License** - License status of device. If it is disable, DAC do not send configuration to this DAP. So the DAP do not broadcast SSID.
- **IP** - The IP address of the device.
- **Status** - The AP status. Can be Online or Offline.

- **Client Number** - Clients count on device currently. Due to the data reporting interval, the count will be delayed compared with the actual number of clients on the AP.
- **Working Model**
 - **Normal Mode** - AP serving wireless clients
 - **Full Scan Mode** - At this mode, all radios under the AP will not broadcast SSID.
- **Location** - Location of device.
- **Online Duration** - Online duration of this AP.
- **Last Offline Time** - The last time the device was disconnected.

8.2. Configurations for AP

8.2.1. Datagram Fragmentation

UDP packet forwarding optimization needs to be turned on under certain circumstances to avoid excessive device load. The default is off.

8.2.2. Turn On/Off IGMP Snooping

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. IGMP is an integral part of IP multicast and allows the network to direct multicast transmissions only to hosts that have requested them.

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic to control delivery of IP multicasts. Network switches with IGMP snooping listen in on the IGMP conversation between hosts and routers and maintain a map of which links need which IP multicast transmission. Multicasts may be filtered from the links which do not need them, conserving bandwidth on those links.

Click "**IGMP Snooping/ON**" button to turn on this function. And click it again, IGMP snooping will be turned off.

8.2.3. Turn On/Off Telnet

Select APs that you want to enable telnet, click **Turn On Telnet** button, then Click **Yes** at the confirmation prompt. The telnet function of selected APs will be turned on.

If any APs telnet is enable, the **Turn Off Telnet** button will enable, click it to turn off telnet for all APs in current Site.

8.2.4. Turn On/Off LED

Click "**Turn On LED**" button to turn led on. This setting is effective for all APs in current Site. Then this button will change to "**Turn Off LED**", click it to turn off led for all APs in current Site.

8.2.5. Turn On/Off USB

Click "**Turn On/Off USB**" button to turn on or turn off USB port on device. This setting is effective for all devices in current site. This function is only effective for devices with USB interface. When the power supply is insufficient, the USB interface on the device may also fail to open.

8.2.6. Firmware Management

Click the **Firmware** button to pop-up the **Firmware** module window, from which you can configure firmware upgrade strategy. It includes **Smart Upgrade** and **Customization Upgrade**. You can only select one of them for firmware upgrade.

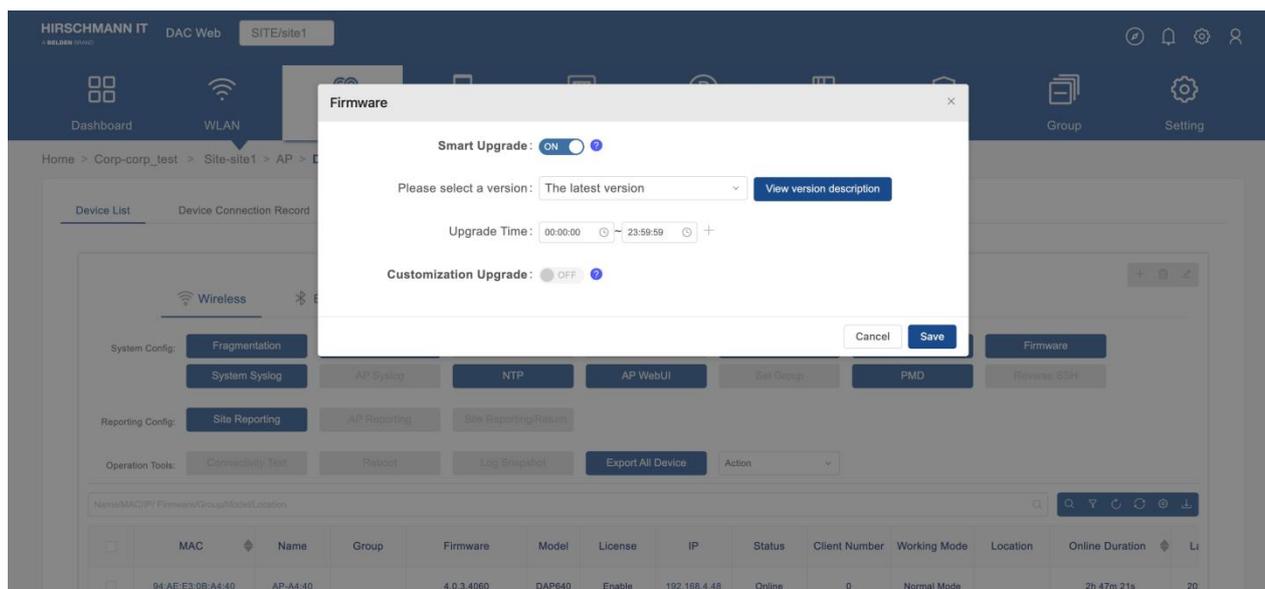


Figure 8-2-6-1

Usually, the DAC synchronizes the available DAP firmware image files from the cloud when DAC can access the cloud. If your deployment environment does not allow DAC to access cloud, you can also get DAP firmwares from the supplier and upload firmware to DAC manually. See more information from [AP Local Firmware Management](#) section. And then, whether you choose **Smart Upgrade** or **Manually Upgrade**, DAP will download the firmware which required for the upgrade from the DAC.

- **Smart Upgrade** - You should select a firmware version (**usually you should choose the latest version, which means that the DAC will try to synchronize the latest version from the cloud every day, and will automatically complete the firmware upgrade of the AP according to the rules of smart upgrade. If you are not sure which version to choose, please contact the supplier**) and set the upgrade time periods that you want the devices do upgrade. Once the upgrade time periods that you set is reached, all devices in current Site will be automatically checked and upgraded to the version selected by the user. At the same time, there will be 20 DAPs for version downloading and upgrading, and other devices are waiting. If the devices in current site are not upgrade after the time reaches the end of the period, the devices that have entered the upgrading status will continue to upgrade, and the devices waiting for upgrade will suspend until the next allowed period arrives. You can add several time periods of the day to the upgraded time period list to avoid the use periods of the devices.
- **Customization Upgrade** - The customization upgrade task will only be updated at the set time, and the task will be automatically cleared after the device upgrade (only once). If device upgrade

failed, you need to manually perform the next upgrade. This is the main difference from Smart upgrade.

8.2.7. Device Syslog Config

Sometimes, in order to locate the problem of the device conveniently, we need to upload the log of the device to the specified log server. Click the **System Syslog** button to set the address of all devices reporting logs under the current site. Or click the **AP Syslog** button to set the address of the selected devices reporting log.

- **Remote Log Switch** - Turn on/off device logging to remote syslog server.
- **Remote Log Server Config** - Default means logging to DAC, Custom means logging to the manual setting.
- **Remote Log Server** - remote syslog server address.
- **Log Level** - Log level that will send.

8.2.8. Configure NTP of Device

The **Network Time Protocol (NTP)** is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

Click **NTP Config** button to open NTP Config window.

- **Time Zone** - Select a time zone form the drop-down list.
- **NTP Server** - Input a NTP Server address, and click **Add** button to add device to NTP Server List. DAC has a built-in NTP Server, and by default, it will send this NTP Server to devices in current Site. By this way, the time synchronization of DAP and DAC is maintained.
- **NTP Server List** - NTP Server List Currently Added.

Click **Save** button to save these configurations add apply these configurations to device in this Site. The currently supported NTP protocol is version 4.

8.2.9. Access to AP Web UI

Sometimes it is necessary to directly access the WebUI of AP device for some maintenance

operations. Click the **AP WebUI** button to open the **AP WebUI** module window.

- **AP Page** - Turn On or Turn Off AP WebUI.
- **Login Name** - The login name must be administrator.
- **Password** - Password of administrator. Then you can login to AP WebUI with this password.
- **Confirm password** - Confirm the password.

Click the **Save** button to save the configurations. Then you can access the AP's webUI by click the AP's IP address in Device List. You should input the password you just set at the AP WebUI Login Page.

8.2.10. Assign APs To Group

Select APs at the Device List, click **Set Group** Button, the **Set Group** module window will open, select a group from the drop down menu, click **Next step** button, at the confirmation of information view, click **Save** button, then the APs that you select will be assigned to the Group. If you want to assign APs to a new Group, you should create the new group refer to [Create New Group](#).

8.2.11. PMD

Post Mortem Dump (PMD) is a troubleshooting method helping to identify root cause of a core dump and exception pointers after a fatal crash.

If PMD is enabled and configured, the DAP will send PMD files to a specific TFTP server immediately when there is key process crashing on the DAP. By default, PMD files sending to external TFTP server is disabled.

Select the APs that you want to collect PMD files in AP list, click **PMD** button, the **PMD** module window will open. Turn on the switch, and fill Server address with TFTP server address. Click **Save** button to save this config.

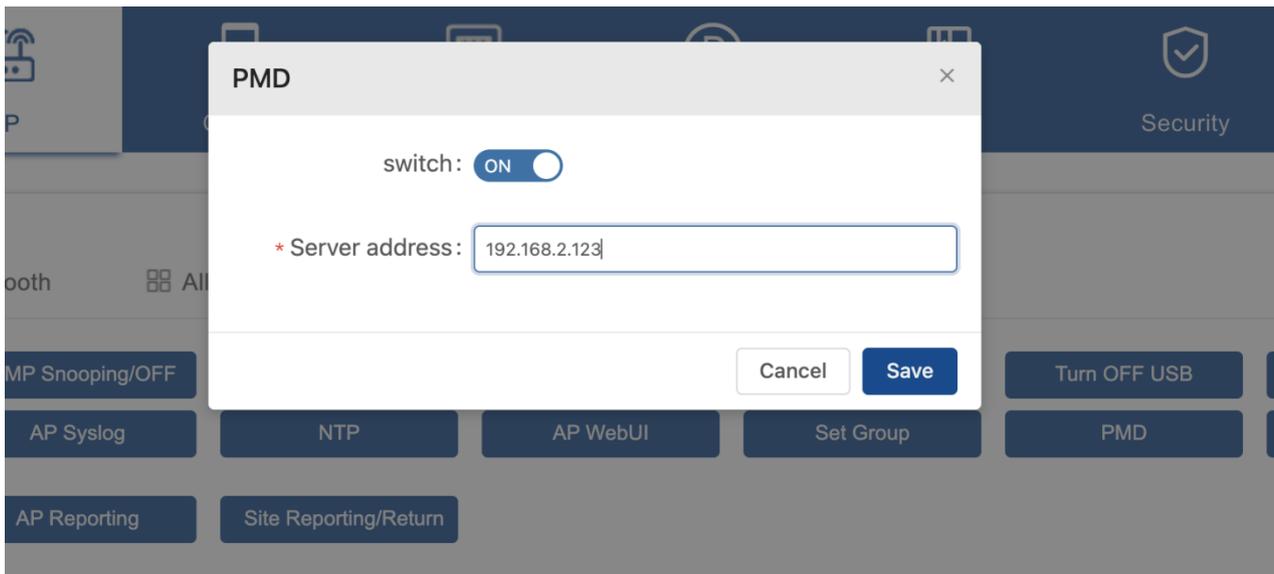


Figure 8-2-11-1

8.2.12. Reverse SSH

Sometimes, in order to find problem on the device, we need to log in to the specified device remotely. However, the device is usually on the customer's intranet, and it is not convenient for the customer to add the public network mapping of the device. Through reverse SSH, we can connect the device to the ssh server on the public network, and then the R & D can access the ssh server of the device from the public server.

Select a device that you want to log in with SSH, click **Reverse SSH** button, the **Edit AP reverse SSH** module window will open.

- **Username** - The username of the ssh server on the public network.
- **Password** - The password of the ssh server on the public network.
- **Server address** - The address of the ssh server on the public network.
- **Port** - The port of the ssh server
- **Reverse SSH Status** - Turn on/off this reverse ssh configuration.
- **Expire** - How long the reverse ssh connection will keep.

8.3. Configure Bluetooth

8.3.1. Bluetooth configurations

You can set the Bluetooth configuration of the whole site or select a specific AP for private Bluetooth configuration. The AP's private Bluetooth configuration takes precedence over the site's overall configuration. You can select the AP, and then click the site Bluetooth / return button to clear the independent Bluetooth configuration of the AP, and then these APS will reuse the Bluetooth configuration of the site.

Click Site Bluetooth button to open Site Bluetooth Configuration module window. Or select AP, click AP Bluetooth button to open AP Bluetooth Configuration module window.

- **Bluetooth** - Switch of Bluetooth. If On, all Bluetooth devices in this site or the selected devices will turn on its Bluetooth.
- **Work Mode** -
 - **Scanner Mode** - Enable the Bluetooth beacon scanning function for the AP.
 - **Advertise Mode** - Enable the BLE advertising function for the Device. If enabled, the Device will broadcast BLE packets.
 - **Advertise & Scanner Mode** - Enable Bluetooth beacon scanning and BLE advertising function

Details of Scanner Mode

- **Scan Type**
 - **Passive Scanning** - Passive Scanning
 - **Active Scanning** - Active Scanning
- **Scan Interval** - The Bluetooth scanning interval for the AP, in milliseconds. (Range = 4 -10240, Default = 100)
- **Scan Window** - Duration of each scan, in milliseconds. (Range = 4 - 10240)
- **Scan Filter** - enable/disable scan filter

Details of Advertise Mode

- **Broadcast Power** - The transmit power used to broadcast BLE packets. (Range = - 20 - 10,

Default = 4)

- **Broadcast Frequency** - The time circle during which the BLE packets will be broadcast, in milliseconds. (Range = 20 - 9,000,000, Default = 200)
- **Broadcast channel** - The transmit channel used to broadcast BLE packets.
- **Beacon Mode** - Specify the BLE protocol used to define the broadcasting BLE beacon format.
 - **iBeacon** - Apple iBeacon format.
 - **Edyuid** - Google Eddysone format. A unique static ID with a 10-byte Namespace component and a 6-byte Instance component.
 - **Namespace** - 20 characters containing 0-9a-f.
 - **Instance ID** - 12 characters containing 0-9a-f.
- **Edyurl** - Google Eddysone format. A compressed URL that, once parsed and decompressed, is directly usable by the client.
- **Plain_URL** - Plain URL which will be compressed

8.3.2. Config Bluetooth WLAN Uplink

Some devices include WLAN and Bluetooth modules. You can use the WLAN module as a client to connect to the network, which is used as the device management / data link to complete the device registration, Bluetooth information reporting, etc.

Click "**Site Wireless Uplink**" button, it will open the config window of **Site Bluetooth Wireless Uplink Configuration**. Or click **AP Wireless Uplink** button, it will open the window of **Bluetooth Wireless Uplink Configuration**.

- **Wireless Uplink** - WLAN uplink status on/off.
- **Mode** - Station (Cannot change).
- **SSID** - SSID of Bluetooth device will connect.
- **Security Level** - The security level of SSID which this Bluetooth device will connect. It can be open or personal.
- **Password** - When security level is personal, you should set a password.

Click **Save** button to apply configurations to Bluetooth Devices in this site.

8.4. Reporting Config

This function is to set AP device to report some of its own information, such as terminal list, RSSI, etc., to the third-party system through MQTT broker. The third-party system can make some new applications based on this information, such as indoor location, etc. You can click **Site Reporting** button to set all devices to report its information or select devices and click **AP Reporting** button to set the selected devices to report its information.

- **Service Switch** - Turn on/off this function.
- **Data Type** - Select Bluetooth Data or Wi-Fi Data or Both of them.
- **Advertise Address** - Advertise Address
- **Bluetooth Topic** - Send message to MQTT broker with this Topic.
- **Advertise Type**
 - **iBeacon** - iBeacon is a protocol developed by Apple, it can be used to determine the device's physical location, track customers, or trigger a location-based action on the device.
 - **Edyuid** - Google Eddysone format. A unique static ID with a 10-byte Namespace component and a 6-byte Instance component.
 - **Edyurl** - Google Eddysone format. A compressed URL that, once parsed and decompressed, is directly usable by the client.
 - **Other** - other advertise type.
- **Group ID** - Group ID of device
- **Access Key** - access key to connect MQTT broker
- **Secret Key** - secret key to connect MQTT broker
- **Bluetooth Reporting Interval** - reporting interval of Bluetooth message.(Range 1~20)
- **Wi-Fi Reporting Interval** - reporting interval of Wi-Fi message.(Range 1 ~ 20)
- **Building ID** - Building ID

8.5. Operation Tools

Operation tools provides a set of small tools to facilitate users to carry out simple operation and maintenance operations.

8.5.1. Connectivity Test

Test whether the selected device can be reached from DAC through the ping command. Select one or more APs (no more than 10), click Connectivity Testing button the Connectivity Testing Dialog will show in several seconds. You will see a table containing the Ping results.

- **AP MAC** - AP MAC
- **AP name** - Name of this AP
- **AP IP** - IP Address of this AP
- **AP status** - AP Online/Offline
- **Send number** - The number of send ping package
- **Receiving number** - The number of receiving package
- **Package loss rate** - package loss rate
- **Average latency** - Average latency
- **Connectivity status** - Connectivity Status Abnormal

8.5.2. Reboot a Device

You can manually reboot a Device by select the Device(s) and clicking on the **Reboot** button. When a Device is rebooted, it will reconnect to DAC. Then, the latest configuration available on DAC is downloaded to the AP. If the AP is unable to connect to DAC, the AP will reboot with the latest saved local configuration.

8.5.3. Log Snapshot

Sometimes it is necessary to collect some information from the device to facilitate R & D to find problems. Select a device and click **Log Snapshot** button. It's needed to wait a moment for Device upload it's snapshot log file to DAC. You need to stay on the current page during file uploading. When

the file transfer is completed, the browser will automatically start downloading the file.

8.5.4. Export All Device

Click **Export All Device** button, you can export all devices in this site. At the download file windows, you can change the export file name. The file is xlsx type, which can be open with Microsoft Office Excel.

8.6. Do Actions from AP

Executes a specific command on the device and returns the output of the command. You can do actions from the drop down menu.

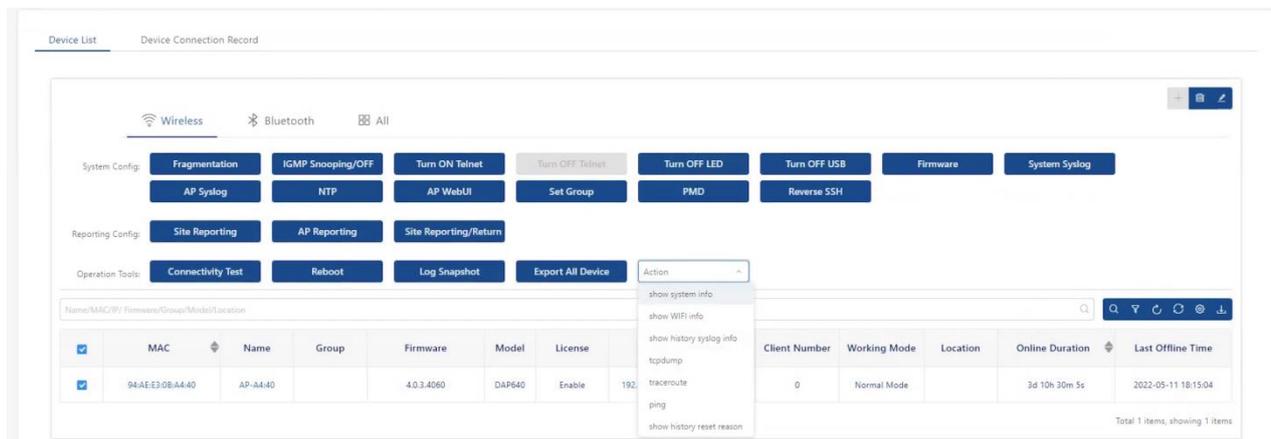


Figure 8-6-1

8.6.1. Show System Info

This action will show system information of device, like memory usage on device and usage of file system.

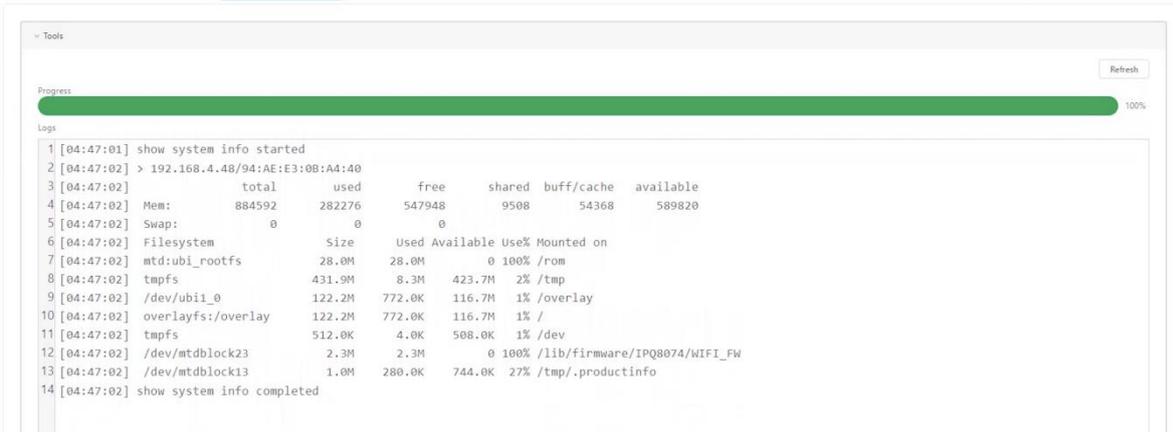


Figure 8-6-1-1

8.6.2. Show WiFi Info

Show wireless interface information of specified DAP which includes:

- Output information of commands 'iwconfig' and 'wlanconfig', for example the DAP working channel, transmit power, BSSID, etc.
- PHY information of client, for example the MAC address and RSSI, etc.

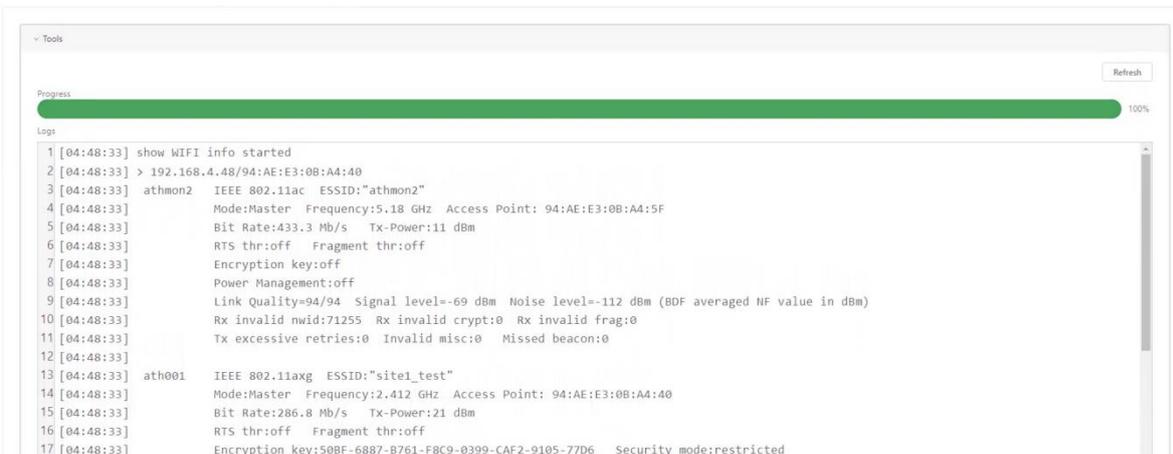


Figure 8-6-2-1

8.6.3. Show history syslog info

Show historic Syslog messages generated in last time system running (Before this time system up) of specified DAP

```

1 [04:50:43] show history syslog info started
2 [04:50:43] > 192.168.4.48/94:AE:E3:08:A4:40
3 [04:50:43] 2022-05-11 10:11:50.543 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:08:A4:40@] <kernel> : [ 153.629546]
4 [04:50:43] 2022-05-11 10:11:50.543 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:08:A4:40@] <kernel> : [ 153.629570] wlan: [1226:E:ANY] [soc1] FWLOG: [15670:
5 [04:50:43] 2022-05-11 10:11:50.543 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:08:A4:40@] <kernel> : [ 153.629570]
6 [04:50:43] 2022-05-11 10:11:51.543 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:08:A4:40@] <kernel> : [ 154.629807] wlan: [1226:E:ANY] [soc1] FWLOG: [15686
7 [04:50:43] 2022-05-11 10:11:51.543 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:08:A4:40@] <kernel> : [ 154.629807]
8 [04:50:43] 2022-05-11 10:11:51.543 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:08:A4:40@] <kernel> : [ 154.629846] wlan: [1226:E:ANY] [soc1] FWLOG: [15701
9 [04:50:43] 2022-05-11 10:11:51.543 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:08:A4:40@] <kernel> : [ 154.629846]
10 [04:50:43] 2022-05-11 10:11:51.543 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:08:A4:40@] <kernel> : [ 154.629870] wlan: [1226:E:ANY] [soc1] FWLOG: [15717
11 [04:50:43] 2022-05-11 10:11:51.543 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:08:A4:40@] <kernel> : [ 154.629870]
12 [04:50:43] 2022-05-11 10:11:52.555 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:08:A4:40@] : udhccp[17139]: receive offer for 192.168.4.48...
13 [04:50:43] 2022-05-11 10:11:52.556 Ap-Debug syslog[null] <NOTICE> [AP 94:AE:E3:08:A4:40@] : : wan (17139): udhccp: receive offer for 192.168.4.48...
14 [04:50:43] 2022-05-11 10:11:52.564 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:08:A4:40@] : udhccp[17139]: OFFER_INFO_INIT priority = 0 offer_count = 0 mode
15 [04:50:43] 2022-05-11 10:11:52.564 Ap-Debug syslog[null] <NOTICE> [AP 94:AE:E3:08:A4:40@] : : wan (17139): udhc'c: OFFER_INFO_INIT priority = 0 offer_cou
16 [04:50:43] 2022-05-11 10:11:53.566 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:08:A4:40@] : udhccp[17139]: offer selecting timeout 1s
17 [04:50:43] 2022-05-11 10:11:53.566 Ap-Debug syslog[null] <NOTICE> [AP 94:AE:E3:08:A4:40@] : : wan (17139): udhccp: offer selecting timeout 1s

```

Figure 8-6-3-1

8.6.4. Tcpdump

This action will capture many packets on device.

```

1 [04:52:52] tcpdump started
2 [04:53:00] > 192.168.4.48/94:AE:E3:08:A4:40
3 [04:53:00] tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
4 [04:53:00] listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
5 [04:53:00] 04:52:57.439267 ARP, Request who-has 192.168.6.244 tell 192.168.6.1, length 46
6 [04:53:00] 20 packets captured
7 [04:53:00] 143 packets received by filter
8 [04:53:00] 0 packets dropped by kernel
9 [04:53:00] 04:52:57.486179 IP 192.168.4.79.47188 > 192.168.4.255.32767: UDP, length 510
10 [04:53:00] 04:52:57.619910 STP 802.1s, Rapid STP, CIST Flags [Learn, Forward], length 102
11 [04:53:00] 04:52:57.626907 ARP, Request who-has 192.168.4.48 tell 192.168.4.76, length 46
12 [04:53:00] 04:52:57.626985 ARP, Reply 192.168.4.48 is-at 94:ae:e3:08:a4:40 (oui Unknown), length 28
13 [04:53:00] 04:52:57.641614 IP 192.168.4.41.57777 > 192.168.4.255.32767: UDP, length 198
14 [04:53:00] 04:52:57.661919 IP 192.168.4.18.56872 > 192.168.4.255.32767: UDP, length 401
15 [04:53:00] 04:52:57.708831 ARP, Request who-has 192.168.5.250 tell 192.168.5.1, length 46
16 [04:53:00] 04:52:57.821566 IP 192.168.4.63.51829 > 192.168.4.255.32767: UDP, length 184
17 [04:53:00] 04:52:57.823652 ARP, Request who-has 192.168.6.244 tell 192.168.6.245, length 46

```

Figure 8-6-4-1

8.6.5. Traceroute

Traceroute from specified DAP to another host in the network.

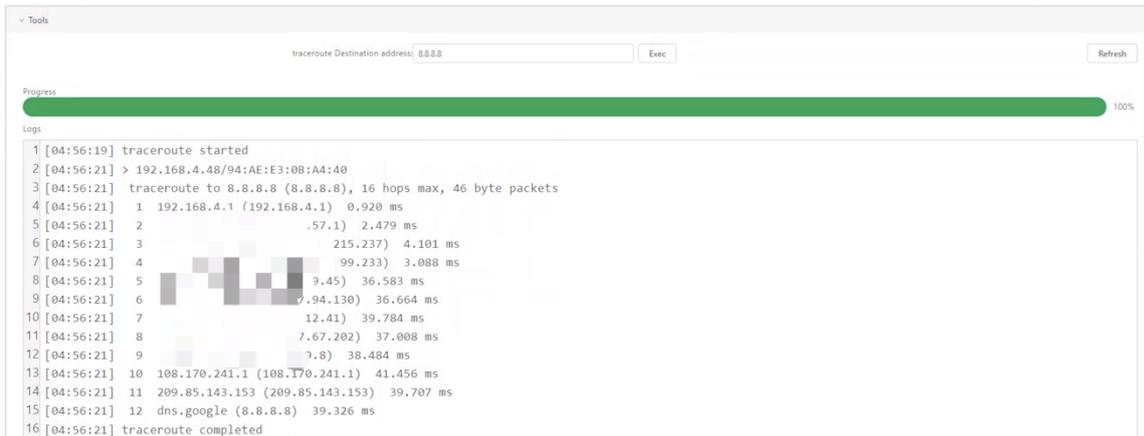


Figure 8-6-5-1

8.6.6. Ping

Ping operation from specified DAP to another host in the network.

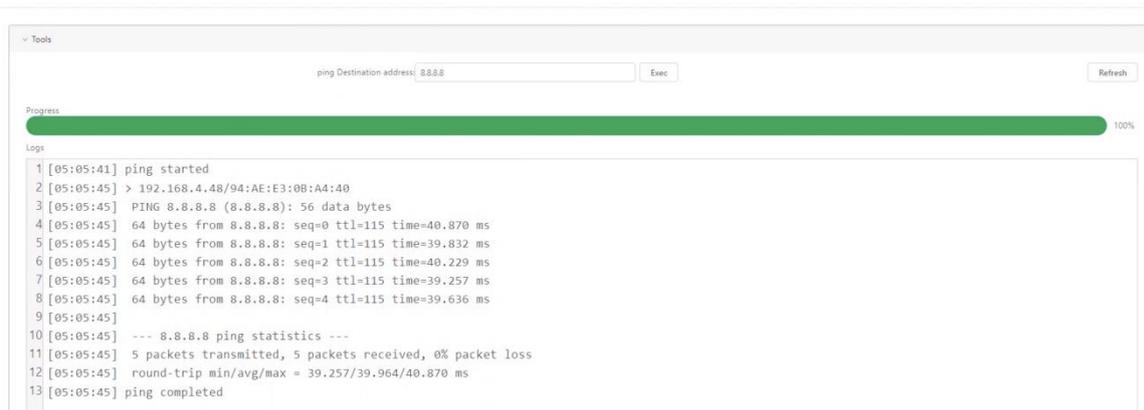


Figure 8-6-6

8.6.7. Show history reset reason

Show latest 10 reboot records of specified DAP which includes reboot time, reboot reason; it's the same output for command `reset_record get` under DAP CLI mod

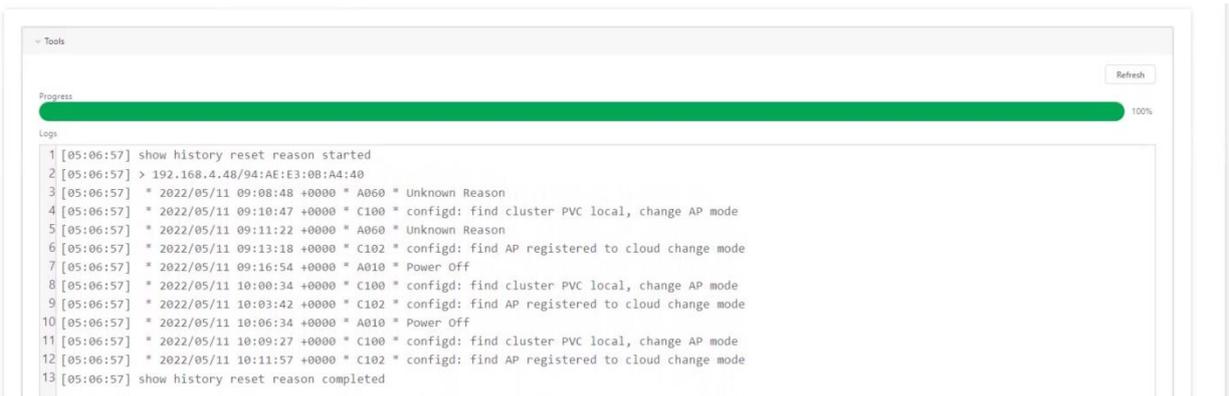


Figure 8-6-6-1

8.7. Device Connection Record

This list contains the connection history of the device. A record will be generated when the device is connected to the DAC. When the device is disconnected, MQTT disconnected time will be updated.

- **MAC** - MAC address of device.
- **Name** - Name of device.
- **MQTT Connected Time** - The record last update at this time.
- **MQTT Disconnected Time** - MQTT disconnect time of this connection.
- **MQTT Connected Duration** - MQTT connect time of this connection.

9. Clients

This page show clients that connect to current Site.

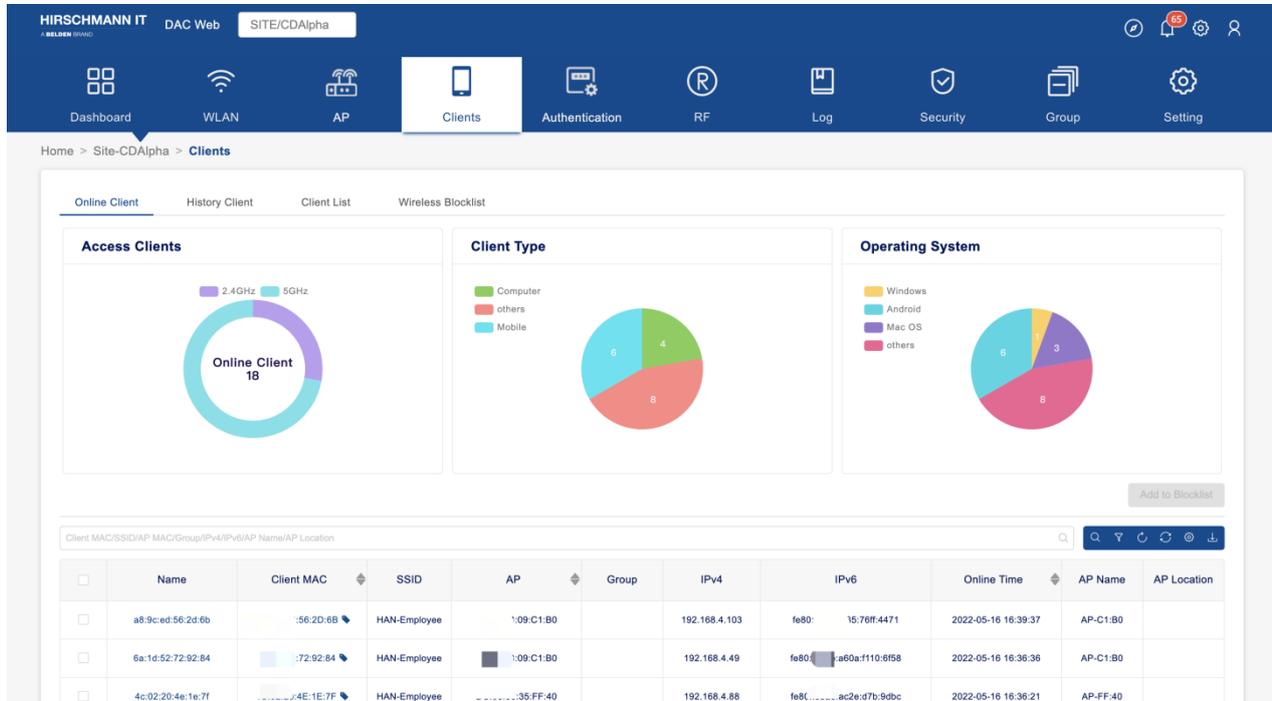


Figure 9-1

This chapter contains the following topics:

- [Online Clients](#)
- [History Clients](#)
- [Client List](#)
- [Wireless Blocklist](#)

9.1. Online Clients

This module shows the list of online clients currently. And there are three pie charts show the distribution of clients in different dimensions.

- **Access Clients** - Pie chart of client band(2.4G/5G).

- **Client Type** - Pie chart of client type, including Computer, Mobile, Others.
- **Operating System** - Pie chart of client's operating system.

List of clients

This list shows the clients currently connected to the AP under the site. Because there is a certain interval for AP data reporting, there is a certain delay in data update here.

- **Name** - Client Name
- **Client MAC** - MAC Address of client.
- **IPv4** - IPv4 Address of client.
- **IPv6** - IPv6 Address of client.
- **SSID** - SSID to which the client is associated.
- **AP** - The MAC address of the AP to which the client associated.
- **Group** - The group of the AP to which the client associated.
- **Connection time** - The time when the client associated to the wireless network.
- **AP Location** - Location of the AP device.
- **Access Band** - The radio band through which the client attached to the AP (2.4GHz or 5GHz).
- **RSSI** - The Received Signal Strength Indicator of the client (Range = 0 - 99).
- **SNR** - Signal-to-noise ratio.

There is a bookmark next to the MAC address of the client. Click the bookmark to view more details of the terminal.

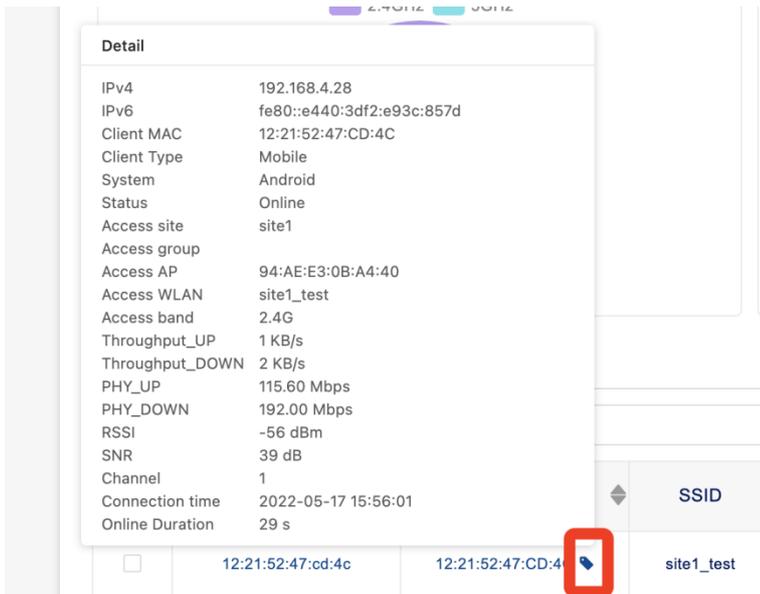


Figure 9-1-1

- **Client Type** - The Client device type, including PC, Mobile, others.
- **System** - The operating system of the client.
- **Throughput UP** - The packet receives rate of the client.
- **Throughput DOWN** - The packet sending rate of the client.
- **PHY_UP** - The physical receive rate of the client.
- **PHY_DOWN** - The physical sending rate of the client.
- **Channel** - The working channel of the client.

9.1.1. Add Client to Blocklist from online clients

To block a client, select the client(s) in the List of Clients and click on the **Add to Blocklist** button. Click **Save** at the Confirmation Prompt. The client will no longer be able to access to the network and will be displayed on the [Wireless Blocklist](#) Screen.

9.2. History Clients

This table shows the connection records in the past.

- **MAC** - MAC Address of client.
- **IPv4** - IPv4 Address of client.
- **IPv6** - IPv4 Address of client.
- **SSID** - SSID to which the client was associated.
- **AP** - The MAC address of the AP to which the client associated.
- **Group** - The group of the AP to which the client associated.
- **Connection Time** - The time when the client associated to the wireless network.
- **Offline Time** - The time when the client disassociated from the wireless network.

9.3. Client List

The total counts of connections of all clients that once connected to this site, and the last connection time are recorded.

- **Name** - Client Name. Default is MAC of client. In order to find the terminal conveniently, you can modify it. Select one client, click edit icon, input name that you want, click **Save** button.
- **MAC** - Mac address of client.
- **Connecting Times** - Count of connecting of this client.
- **Last Connecting** - Time when the client last accessed the site.
- **Group** - The group that client last accessed the site.

9.4. Wireless Blocklist

Blocklist focus on the basic access control mechanism for users connecting to SSID based on the client level; those clients on the Blocklist are denied associating to the DAP, once a client is in the Blocklist, it cannot connect to any WLAN of any security level (Enterprise/Personal/Open). You can add/delete the Blocklist based on client's MAC address.

The Wireless Blocklist Screen show information about all clients that have been blocked in this Site. It is also used to manually add clients to the Blocklist.

- **Client MAC** - MAC address of the client in the Blocklist.
- **Start Time** - The start time for the block. During the duration, the client is not allowed to access to the wireless network.
- **Expiry Time** - The expiry time for the item. The client can access the wireless network after the expiry time.
- **Type** - The reason why the client was added to Blocklist.
 - **manual** - Added into the Blocklist by the user.
 - **auto** - Dynamically added by the WIPS policy.
- **From(Site/Group)** - This record is added from Site or Group.

9.4.1. Adding a Client to the Blocklist Manual

Click on the **+** icon to bring up the **Add to Blocklist** module window. Enter the client's MAC address, then click on the **Save** button. Repeat to add additional clients. You should set an Expire time for the client. That means the client cannot connect to SSID of this Site until expire time.

9.4.2. Deleting a Client from The Blocklist

Select the client(s) in the Blocklist and click on the Delete icon. Click **Yes** at the confirmation prompt.

10. Authentication

DAC has built-in AAA server. According to the WLAN configuration, the DAP will send an authentication request to the DAC, which may be 1x authentication or Mac authentication or other authentication.

This chapter contains the following topics:

- [Concepts of Authentication](#)
- [Network Control](#)
- [Authentication](#)
- [Guest Access](#)
- [Employee Access](#)
- [Setting](#)
- [Default Config and Quick Entrance](#)
- [Configuration instance for Authentication](#)

10.1. Concepts of Authentication

802.1X Authentication

IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

802.1X is an Institute of Electrical and Electronics Engineers (IEEE) standard that provides an authentication framework for WLANs. 802.1x uses the Extensible Authentication Protocol (EAP) to exchange messages during the authentication process. The authentication protocols that operate inside the 802.1X framework that are suitable for wireless networks include EAPTransport Layer Security (EAP-TLS), Protected EAP (PEAP), and EAPTunneled TLS (EAPTTLS). These protocols allow the network to authenticate the client while also allowing the client to authenticate the network.

802.1x authentication consists of three components:

- **Client** - The device attempting to gain access to the network.
- **Authenticator** - The gatekeeper to the network and permits or denies access to the clients. The wireless controller acts as the authenticator, relaying information between the authentication server and the client. Note that the EAP type must be consistent between the authentication server and supplicant, and is transparent to the controller.
- **Authentication Server** - Provides a database of information required for authentication, and informs the Authenticator to deny or permit access to the client. The 802.1X authentication server is typically an EAP-compliant Remote Access Dial-In User Service (RADIUS) Server which can authenticate either users (through passwords or certificates) or the client computer.

In our system, DAP acts as an authenticator and DAC acts as authentication server. DAC can use different data sources for user authentication.

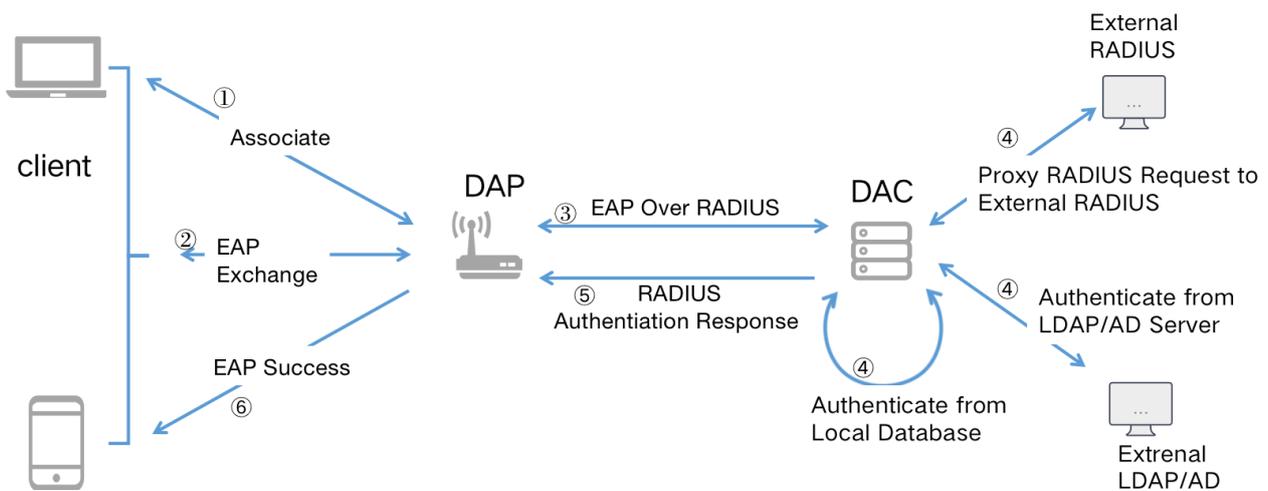


Figure 10-1-1

Figure 10-1-1 shows the basic process of 802.1x authentication process in our system. For Step four, DAC can use different Data Sources to verify user.

- ① The client initiates Wireless Association.
- ② The client starts EAP interaction with DAP, which is a handshake process with several messages.

- ③ The DAP forwards the corresponding EAP message to the DAC through RADIUS protocol.
- ④ The DAC use different Data Sources (based on different configuration) to verify user.
- ⑤ The DAC returns EAP authentication result to DAP through RADIUS protocol.
- ⑥ The DAP returns EAP authentication result to client

Mac Authentication

MAC authentication authenticates devices based on their physical Media Access Control (MAC) address. The MAC of devices will be used as User-name and Password in the RADIUS Access Request. Mac authentication is a necessary preprocess for web authentication. When a wireless terminal accesses the DAP, the DAP will initiate MAC authentication. The RADIUS Access Request will go through the rule matching of **Access Policy** and enter the corresponding **Authentication Strategy** for processing. If the **Authentication Strategy** is configured with **Guest / Employee Access Strategy**, and the MAC has been authenticated by portal before, and the corresponding account has been bound, and the binding has not expired, the authentication module will directly return the authentication success and return the corresponding Access Role to AP. If the MAC has not undergone portal authentication before, or the previously bound record has expired, the portal URL of the **Guest / Employee Access Strategy** configured in the **Authentication Strategy** will be sent to the terminal. After the terminal opens the page, fill in the user name and password to complete the portal authentication process. If successes, the MAC authentication binding record will be saved according to the policy.

Web Portal Authentication

Web Portal Authentication is mechanism by which user credentials are obtained through Web pages and authenticated through a RADIUS server. If the authentication is successful, the RADIUS server may return an **Access Role** that is applied to traffic from the user device. The DAC implementation supports Web Portal mechanism.

Web Portal authentication is a configurable option for an **Access Role Profile** that is applied after a user is assigned to the profile (after the initial MAC authentication). This type of authentication does not change the Access Role Profile assignment for the user device. Instead, Web Portal provides a secondary level of authentication that is used to apply a new Access Role to the user.

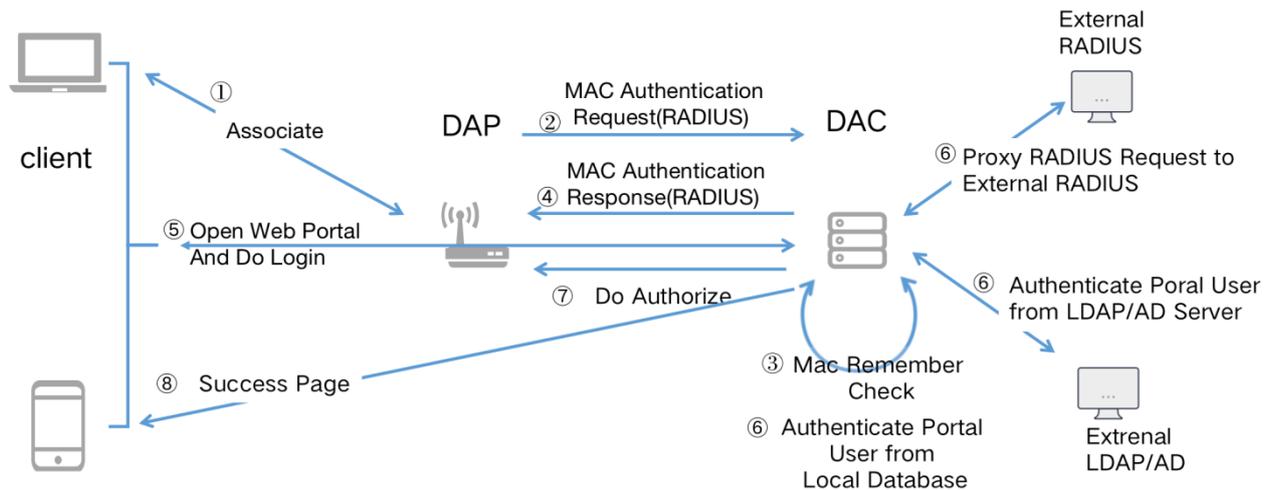


Figure 10-1-2

Figure 10-1-2 shows the basic process of WEB Portal authentication process in our system. For Step six, DAC can use different Data Sources to verify user.

- ① The client initiates Wireless Association.
- ② The DAP initiates MAC authentication through RADIUS protocol.
- ③ The DAC performs remember check (check if the MAC of client bind to an account is valid)
- ④ The DAC replies the result of the remember check to the DAP. If the client has an unexpired remember check record, the DAP will directly authorize the client and the client will not redirect to the Web Portal; Otherwise, according to the configuration, the DAC will return the corresponding Web Portal to the DAP, and the DAP will redirect the client's HTTP request to the Web Portal page (via HTTP 302).
- ⑤ The client browser opens the web portal page, enters the user name and password, and initiates the login request. The request is submitted directly to the DAC.
- ⑥ The DAC use different Data Sources (based on different configuration) to verify user.
- ⑦ The DAC sends the authorization information(Access Role Profile) of the client to the DAP according to the authentication results.
- ⑧ The web page displaying authentication results on client browser.

Access Role

Each wireless client will be assigned an **Access Role** when accessing or authenticating. The assignment of the **Access Role** on the terminal may be obtained directly from the WLAN, or it can be assigned according to the strategies in the authentication process, and can also be set on the authentication Account. For detailed configuration information of Access Roles, you can refer to [Access Role Profile](#).

Access Policy

RADIUS package carries several users / terminal related attributes. When the authentication module receives the RADIUS package, the **Access Policy** will match the corresponding rules and use the corresponding **Authentication Strategy** for authentication. For detailed configuration information of **Access Policy**, you can refer to [Access Policy](#).

Authentication Strategy

Defines the relevant policy parameters of MAC authentication or 802.1x authentication, including authentication source, **Access Role**, whether to enable Web authentication and other attributes; When selecting different authentication sources, there will be some constraints on the selection of Web authentication. For detailed configuration information of **Authentication Strategy**, you can refer to [Authentication Strategy](#).

Guest Access Strategy

Define the web Authentication Strategy for Guest. You can Customize the web page by click **Edit Page** button. Check the [Captive Portal](#) section for more information on customizing portal pages. For detailed configuration information for Guest Access Strategy, you can refer to [Guest Access Strategy](#).

Employee Access Strategy

Define the web Authentication Strategy for Employee. For detailed configuration information for **Employee Access Strategy**, you can refer to [Employee Access Strategy](#).

Authentication Source

The data source used in authentication. You will see the configuration in **Authentication Strategy** and **Guest / Employee Access Strategy**. This option may have the following values:

- **None** - It can only be selected in **Authentication Strategy**. If this **Authentication Source** is selected in Authentication Strategy, it means that only remember verification will be performed at

this stage and **CANNOT** be used for 802.1x authentication.

- **Local Database** - Local Authentication Database. It can be used in **Authentication Strategy** or **Guest / Employee Access Strategy**. For 802.1x authentication, you need to add Employee Accounts in **Authentication** -> **Employee Access** -> **Employee Access Strategy**, and these accounts can also be used for Web Portal Authentication in **Employee Access Strategy**. For web portal authentication in **Guest Access Strategy**, only local database can be selected as the **Authentication Source**.
- **External LDAP/AD** - Using external LDAP / AD as the **Authentication Source**. It can be used for **Authentication Strategy** or **Employee Access Strategy**. You need to complete parameter setting in **Authentication** -> **Setting** -> **LDAP / AD Configuration**. For detailed information of **External LDAP/AD**, you can refer to [LDAP / AD configuration](#).
- **External Radius** - Using External Radius as the **Authentication Source**. It can be used for **Authentication Strategy** or **Employee Access Strategy**. You can add External Radius at **Authentication** -> **Setting** -> **External Radius**.

Remember Devices

It is used to simplify the process of **Web Portal Authentication**. After the **Web Portal Authentication** is passed, the binding relationship between the MAC address and Account of the terminal and the authorized **Access Role Profile** are recorded. When the terminal accesses the wireless network again within the validity period of remember, the terminal does not need do **Web Portal Authentication**.

Relationship among **Access Policy**, **Authentication Strategy**, **Guest Access Strategy** and **Employee Access Strategy**:

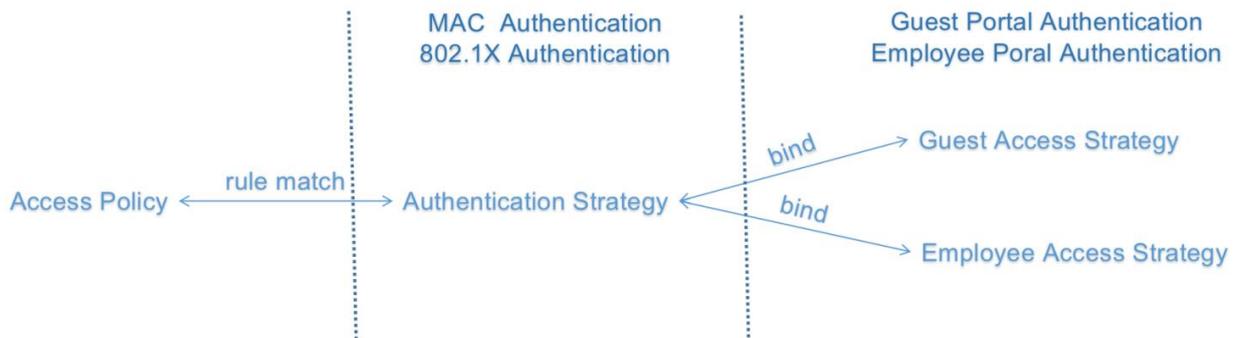


Figure 10-1-3

In summary, terminal access may require two authentication steps, MAC / 1X authentication and web authentication. **Authentication Strategy** is used to define MAC / 1X authentication, and the authentication result determines whether subsequent web authentication is required. **Guest / Employee Access Strategy** is configuration of web authentication.

10.2. Network Control

Network control used to control user's online behavior. It consists of Access Role Profile, Location Policy, Period Policy, Policies and Policy List.

10.2.1. Access Role Profile

The Access Role Profile Screen displays all configured Access Role Profiles and is used to create, edit, and delete Access Role Profiles. An Access Role Profile contains the various properties (e.g., VLAN or Bandwidth Control) for users assigned to the profile. An Access Role Profile is considered as a user role with which every client in the wireless network is associated.

Creating an Access Role Profile

Click on the '+' icon. Enter a Profile Name and configure the profile as described below, then click on the **Save** button.

Policy & Policy List

An Access Role Profile can be configured with an existing Policy List. The set of rules within the Policy List are then applied to the traffic that passes through wireless devices. Only one Policy List is allowed per profile, but multiple profiles may use the same Policy List. Select a Policy List for the profile from the drop-down menu. You can also click the "Add" link to create a new one.

Location Policy

Select a Location Access Policy from the drop-down menu.

Period Policy

Select a Period Policy from the drop-down menu.

Bandwidth Control Settings

- **Upstream Bandwidth** - The maximum bandwidth limit allocated for ingress traffic on UNP ports assigned to the profile. If the maximum ingress bandwidth value is set to zero, all ingress traffic is not limited.
- **Downstream Bandwidth** - The maximum bandwidth limit allocated for egress traffic on UNP ports assigned to the profile. If the maximum egress bandwidth value is set to zero, all egress traffic is allowed on the UNP port.
- **Upstream Burst** - The maximum ingress depth value that is applied to traffic on UNP ports that are assigned to the profile. This value determines how much the traffic can burst over the maximum ingress bandwidth rate. The maximum ingress depth value is configured in conjunction with the maximum ingress bandwidth parameter.
- **Downstream Burst** - The maximum egress depth value that is applied to traffic on UNP ports that are assigned to profile. This value determines how much the traffic can burst over the maximum egress bandwidth rate. The maximum egress depth value is configured in conjunction with the maximum egress bandwidth parameter.

VLAN & VLAN Pool

You can set a signal VLAN or multiple VLANs (as a VLAN pool) for an Access Role Profile. For signal VLAN type, you can set VLAN ID to zero, which means map an Access Role Profile to untagged traffic. Also note that you can select a VLAN Pool, by entering multiple VLANs. You can enter VLANs as a range (e.g., 10-20), as individual VLANs (21, 23, 25), or both (10-20, 21,23, 25).

Editing an Access Role Profile

Select the profile in the Access Role Profile List and click on the Edit icon to bring up the Edit Access Role Profile Screen. Edit the fields as described above then click on the **Save** button to save the changes to the server. (Note that you cannot edit the Access Role Profile Name.)

Deleting an Access Role Profile

Select the profile in the Access Role Profile Screen and click on the Delete icon, then click **Yes** at the confirmation prompt. This removes the profile from the server.

10.2.2. Policies

The Policies Screen application displays configured Policies and is used to create, edit, delete, and

view Policies. Policies are QoS Policies that can be applied to DAP. Policies are created using a wizard that guides you through each of the steps needed to create the Policy.

Creating Policy

Policies are created using a wizard that guides you through each of the steps needed to create the policy. To create a Policy, click on the + icon. The wizard will then guide you through the following screens:

- **Config** - Basic policy configuration (e.g., Policy Name, Precedence)
- **Set Condition** - Specify the conditions that must be true before traffic will be allowed to flow.
- **Set Action** - Specify parameters for the traffic that will flow.
- **Validity Period** - Specify the time period for the policy to be effective.
- **Confirm** - Review the policy details before creating the policy.

Config

The Policies Config for Policy Screen is used to configure basic Policy parameters.

When you have completed all of the parameters, click the **Next** button at the bottom of the screen to move to the next step.

- **Name** - The Policy name.
- **Precedence** - The Policy precedence. By default, the precedence field is pre-filled with the lowest unused precedence value (Range = 0 - 65535).

Set Condition

The Policies Set Condition Screen contains a list of Conditions that you can configure for the Policy (e.g., MAC Condition, IP Condition). When you create a Condition, the Condition(s) you configure must be true before traffic is allowed to flow. Click on a Condition to show the configuration options for the Condition. (Click again on the Condition to hide the configuration options.) When you have completed all of the parameters for the Condition(s), click the **Next** button at the bottom of the screen to move to the next step. If necessary, you can also click the **Back** button to return to the Config screen. A brief description of each Condition is provided below. Click the hyperlink for each Condition for detailed configuration instructions.

- **L2 MACs** - Create a Condition that applies the policy to traffic originating from a MAC address/group/range or to traffic flowing to a MAC address/group.
- **L3 IPs** - Create a Condition that applies the policy to traffic originating from an IP address/network group or to traffic flowing to an IP address/network group. (Note that any IP address can be masked).
- **L3 DSCP/TOS** - Create a Condition that applies the policy to traffic with a specified value in either the DSCP (Differentiated Services Code Point) byte or in the IP TOS (IP Type of Service) byte. Both DSCP and IP TOS are mechanisms used to convey QoS information in the IP header of frames.
- **L4 Services** - Create a Condition that applies the policy to traffic flowing between two TCP or UDP ports, or to all traffic originating from a TCP or UDP port, or to all traffic flowing to a TCP or UDP port. You can also create a Condition using an existing service/service group.

L2 MACs

A MAC Condition applies the Policy to traffic flowing from/to a MAC Address/Group. Note that Layer 2 Conditions (conditions that specify MAC Addresses) are "lost" when traffic passes through a router. For this reason, it may be advisable to specify other types of Conditions (such as a Layer 3 Condition, which specifies IP Addresses) when traffic is expected to travel more than one router hop.

Select the parameter(s) you want to configure by selecting the applicable check bottom. Click on **Single** to configure a single MAC Address or **Group** to configure a MAC Group, then enter a MAC address or select a MAC Group from the drop-down menu. (You can also click the Add icon to go to the Groups application and create a new MAC Group.)

- **Source MAC Address/MAC Group** - Configuring a Source MAC Address/Group Condition restricts the policy to traffic that flows from this MAC Address/Group only. If you do not select this option, you are effectively stating that the Source MAC Address/Group traffic is not a criterion for the policy.
- **Destination MAC Address/MAC Group** - Configuring a Destination MAC Address/Group Condition restricts the policy to traffic that flows to this MAC Address/Group only. If you do not select this option, you are effectively stating that the Destination MAC Address/Group traffic is not a criterion for the policy.

L3 IPs

An IP Condition applies the Policy to traffic originating from, or flowing to, an IP Address/Network group. Any IP Address can be masked. Select the parameter(s) you want to configure by selecting the applicable check button. For Source/Destination IP Address, click on Single to configure a single IP Address, or click on Group to configure a Network Group, then enter an IP Address or select a Network Group from the drop-down menu. (You can also click the + icon to go to the Groups application and create a new Network Group.)

- **Source IP Address/Network Group** - Configuring a Source IP Address/Network Group Condition restricts the policy to traffic that flows from this IP Address or Subnet Mask/Network Group only. If you do not select this option, you are effectively stating that the Source IP Address or Subnet Mask/Network Group traffic is not a criterion for the policy.
- **Destination IP Address/Network Group** - Configuring a Destination IP Address/Network Group Condition restricts the policy to traffic that flows to this IP Address/Network Group only. If you do not select this option, you are effectively stating that the Destination IP Address or Subnet Mask/Network Group traffic is not a criterion for the policy.

L3 DSCP/TOS

A DSCP/TOS Condition applies the Policy to incoming traffic that has a specified value in either the DSCP (Differentiated Services Code Point) byte or in the TOS (Type of Service) byte. Both DSCP and TOS are mechanisms used to convey QoS information in the IP header of frames. DSCP and TOS are mutually exclusive - you can use either DSCP or TOS but not both. Click on the applicable button (DSCP or TOS) and enter a value.

- **DSCP** - Defines the QoS treatment a frame is to receive from each network device. This is referred to as per-hop behavior. If you are using DSCP, you can define any value in the range 0 - 63 as the DSCP value in the IP header of the frame. Traffic that contains this value will match this condition.
- **TOS** - A TOS value creates a condition that applies the policy to traffic that has the specified TOS value in the IP header of frames. Enter any value from 0 - 7 to specify the value of the precedence field in the TOS byte that will match this condition. A value of 7 has the highest precedence and a value of 0 has the lowest.

L4 Services

A Service Condition applies the policy to Service Protocol traffic (TCP or UDP) flowing from/to two

TCP or UDP ports, or to traffic flowing from/to a TCP or UDP Service or Service Group. Select a type of Service Condition you want to configure, then configure the parameter(s) as described below.

- **Protocol Only** - Select TCP or UDP to create a condition for a Service Protocol only.
- **Port(s)** - To configure the Condition for a specific Service Port, select a Source and Destination Port from the drop-down menu to specify a specific port for the service you selected. You can also click on the Add icon to go to the Groups application and create new Service Ports.
- **Service** - Select a Service from the drop-down menu. You can also click on the Add icon to go to the Groups application and create a new Service.
- **Service Group** - Select a Service Group from the drop-down menu. You can also click on the Add icon to go to the Groups application and create a new Service Group.

Set Action

The Policies Set Action Screen contains a list of Actions that you can configure for the Policy (e.g., QoS, TCM). A Policy Action enables you to specify the treatment traffic is to receive when it flows. This includes the priority the traffic will receive, its minimum and maximum output rates, and the values to which specified bits in the frame headers will be set upon egress from the switch. When the Conditions specified by the Policy Condition are true, traffic will flow as specified by the Policy Action. Click on an Action to show the configuration options for the Action. (Click again on the Action to hide the Action.) When you have completed all of the parameters for the Action(s), click the **Next** button at the bottom of the screen or click on Validity Period on the left side of the screen to move to the next step. If necessary, you can also click the **Back** button to return to the screen.

A brief description of each Action is provided below. Click the hyperlink for each Action for detailed configuration instructions.

- **QoS** - Set Action to specify QoS actions to impose on traffic that meets the configured policy condition(s). When the conditions specified by the policy are true, traffic will flow as specified by the policy action. Quality of Service applies to Session Type for wireless devices.
- **TCM** - Create an Action to specify Tri-Color Marking (TCM) actions to impose on traffic that meets the configured policy condition(s). TCM provides a mechanism for policing network traffic by limiting the rate at which traffic is sent or received on a switch interface. TCM meters traffic based on user-configured packet rates and burst sizes and "marks" the metered packets as green, yellow, or red based on whether the traffic meets the configured rates. This "color marking"

determines the packet's precedence when congestion occurs. TCM is not supported on wireless devices and is ignored when applied to those devices.

QoS

The QoS Policy Action option enables you to specify QoS actions to impose on traffic that meets the configured policy condition(s). When the conditions specified by the policy are true, traffic will flow as specified by the policy action.

- **Behavior** - Set the Action to Accept or Drop traffic that meets the configured condition(s).
- **Priority** - Specify the QoS priority the traffic will receive if it meets the configured condition(s).
- **Max Output Rate** - Specify the maximum amount of traffic, in kilobits per-second, which is guaranteed to be transmitted from the port. Even if no other traffic exists, the output will be limited to the rate specified here.
- **802.1p Priority Level** - If you want outgoing packets tagged with an 802.1p priority level, set the 802.1p Priority Level field to any value between 0 to 7 to specify the desired outgoing 802.1p priority for the traffic. A value of 7 indicates the highest priority and a value of 0 indicates the lowest priority. Note that for ports that are configured for 802.1q, this value is used in the 802.1q header and indicates the outgoing priority of the frame. When a frame is de-queued for transmission, it is assigned the priority of the queue and mapped to the outgoing 802.1p priority. This priority is combined with the VLAN group ID to create the 802.1p/q header for transmission. Note that if traffic matches the criteria specified by the policy condition, but the outgoing port does not support 802.1p tagging, the policy action will fail. This parameter is not supported on AOS Wireless Devices and is ignored when applied to those devices.
- **DSCP/TOS** - Enable/Disable DSCP/TOS Precedence. The TOS byte is defined in RFC 791. This byte contains two fields. The precedence field is the three high-order bits (0-2) and is used to indicate the priority for the frame. The type of service field (bits 3-6) defines the throughput, delay, reliability, or cost for the frame; however, in practice these bits are not used. If you enable the **TOS Precedence radio**, set the associated field to any value from 0-7 to specify the value that will be inserted into the precedence field of the TOS byte upon egress from the switch. A value of 7 has the highest precedence and a value of 0 has the lowest precedence. Note that you can enable either the DSCP or the TOS Precedence radio to specify the mechanism you want to use (if any) to convey QoS information in the IP header of frames. DSCP and TOS are mutually exclusive. You can use either DSCP or TOS, but not both. This parameter is not supported on

AOS Wireless Devices and is ignored when applied to those devices.

TCM

The TCM Policy Action option enables you to specify Three-Color Marking (TCM) actions action to impose on traffic that meets the configured policy condition(s). TCM provides a mechanism for policing network traffic by limiting the rate at which traffic is sent or received on a switch interface. TCM meters traffic based on user-configured packet rates and burst sizes and "marks" the metered packets as green, yellow, or red based on whether the traffic meets the configured rates. This "color marking" determines the packet's precedence when congestion occurs. TCM is not supported on AOS Wireless Devices and is ignored when applied to those devices.

- **Committed Information Rate** - The guaranteed bandwidth, in bits-per-second, for all traffic that ingresses on the port. (256~65535 kbit/s)
- **Peak Information Rate** - The peak bandwidth, in bits-per-second, for all traffic that ingresses on the port. (256~65535 kbit/s)

Validity Period

The Policies Validity Period Screen enables you to add a validity period to a condition by specifying the time periods when the policy is active and enforced. Select a validity period from the Validity Periods drop-down list:

- **AllTheTime** - The policy will be enforced all days of the week, all months of the year, and all hours of the day.
- **Weekdays** - The policy will be enforced on weekdays (Monday - Friday), all months of the year. Each weekday is 24 hours (midnight to midnight).
- **Weekends** - The policy will be enforced on Saturday and Sunday, all months of the year. Each Saturday and Sunday is 24 hours (midnight to midnight).
- **WorkingDay** - The policy will be enforced on weekdays (Monday - Friday), from 9:00 a.m. to 5:00 p.m., all months of the year.
- **Custom** - Select to create a custom validity period by specifying specific days, months, and times.

When you have completed all of the parameters, click the **Next** button at the bottom of the screen to move to the next step. If necessary, you can also click the **Back** button to return to the screen.

Note: The pre-configured validity period **AllTheTime** is the default and is automatically assigned to the condition when the Ignore Validity Period in defining Policy Condition checkbox is checked. You can configure a validity period when configuring an IP Condition or Service Condition. If you do not specify an IP or Service Condition, the configured period is not applied for Wireless Controllers.

Editing a Policy

To edit a policy, select the policy in the Existing Policies Table and click on the Edit icon. Use the wizard to make any edits.

Deleting Policy

To delete a policy(ies), select the policy(ies) in the Existing Unified Policies Table, click on the Delete icon, then click **Yes** at the confirmation prompt.

10.2.3. Policy List

The Policy List Screen displays all configured Policy Lists, including the Policies included in each list, and is used to create, edit, delete, view and apply Policy Lists. A Policy List is a set of Policies that are grouped together and assigned to devices as a group. A Policy List can be applied to DAPs. A Policy List must be applied as part of an Access Role Profile.

Creating a Policy List

Click on the '+' icon. The Create Policy List Wizard appears. Complete the screens as described below, then click on the **Add** button.

Config for Policy List

Enter a Name for the Policy List and select the Policies you want to include in the list from the Add Policies drop-down menu. All of the currently configured Unified Policies appear in the list. You can also click the Add icon to call create policy panel and create a new Policy to add to the list. When you select a Policy from the drop-down menu, the Policy will appear in a table below. Review the Policy List configuration(s) in the table, then click the **Add** button. The new Policy List will appear on the Policy Lists Screen.

Editing a Policy List

You can edit the Policies included in a Policy List or edit the Precedence value of any Policy in the list. Select a Unified Policy List and click on the Edit icon. The Edit Policy List Screen appears. Click on the Add Unified Policies drop-down menu. All of the currently configured Unified Policies appear in the list. You can also click the Add icon to go to Create Policy Screen and create a new policy to add to the list. Finished editing the Unified Policy, click the **Edit** button. The updated Policy List will appear on the Policy Lists Screen.

Deleting a Policy List

To delete a Policy List(s), select the list(s), click on the Delete icon, then click **Yes** at the confirmation prompt. Note that you cannot delete a Policy List that is associated with an Access Role Profile. To delete the list, you must first remove it from associated Access Role Profile.

10.2.4. Location Policy

The Location Policy Screen displays all configured Location Policies is used to create, edit, and delete Location Policies. A Location Policy defines a specific location where a device can access the network. The policy is associated with an Access Role Profile and applied to devices classified into the Access Role Profile.

Creating a Location Policy

Click on the + icon and complete the fields as described below. When you are finished, click on the **Save** button.

- **Name** - User-configured Location Policy Name.
- **AP Location** - The configured location for the Access Point from which the device can access the network.
- **AP Name** - The configured AP name for the Access Point from which the device can access the network.

Editing a Location Policy

Select the policy in the Location Policy List and click on the Edit icon to bring up the Edit Location Policy Screen. Edit the fields as described above then click on the **Save** button to save the changes. Note that you cannot edit the profile name.

Deleting a Location Policy

Select the policy in the Location Policy List and click on the Delete icon, then click **Yes** at the confirmation prompt.

10.2.5. Period Policy

The Period Policy Screen displays all configured Period Policies is used to create, edit, and delete Period Policies. A Period Policy specifies the days and times during which a device can access the network. The policy is associated with an Access Role Profile and applied to devices classified into the Access Role Profile.

Creating a Period Policy

Click on the + icon and complete the fields as described below. When you are finished, click on the **Save** button.

- **Name** - User-configured Period Policy Name.
- **Date/Time** - Click on the Days/Months, Date/Time, and Time of Day sliders to configure the time when the devices can access the network.
- **Timezone** - Select the in which the Period Policy is active.

Editing a Period Policy

Select the policy in the Period Policy List and click on the Edit icon to bring up the Edit Period Policy Screen. Edit the fields as described above then click on the **Save** button to save the changes. Note that you cannot edit the profile name.

Deleting a Period Policy

Select the policy in the Period Policy List and click on the Delete icon, then click **Yes** at the confirmation prompt.

10.3. Authentication

The Authentication module used for configuration of user Access Strategy.

10.3.1. Dashboard

Dashboard consist of four diagram.

Authentication Result Statistic: This diagram demonstrates the result of authentication (Success/Failure). Dimension of authentication method consist of MAC,802.1x, Captive Portal. Dimension of client type consist of Employee, Company Device, Unknown, Guest. Dimension of time zone consist of several time zone.

The remaining three diagram show the contents describe in the label. They are "Top 10 AP with Authentication Request ", "Top 10 AP with Authentication Request "and "Top 10 Reason of Authentication Failure".

10.3.2. Access Policy

Authentication Access Policies are used to define the mapping conditions for an authentication strategy. Through Access Policy configuration, **Authentication Strategy** can be applied to different user groups, which can be divided by SSID or other attributes. The **Access Policy** Screen displays all configured Access Policies and is used to create, edit, and delete Access Policies.

- **Name** - User-configured policy name
- **Authentication Strategy** - Authentication strategy that will be utilized when the Access Policy is matched
- **Priority** - Access Policy Priority. A user requesting authentication may match several access policies and the one with highest priority will take effect after passing the authentication. (Range = 1 - 99, 1 is the highest priority and 99 is the lowest)
- **Mapping Condition** - Descriptions of conditions that you add in this policy.

Creating an Access Policy

Click on the + icon to bring up the **Create Access Policy Screen**. Complete the fields as described below, then click on the **Save** button.

- **Policy Name** - User-configured policy name
- **Priority** - Access Policy Priority. A user requesting authentication may match several access policies and the one with highest priority will take effect after passing the authentication. (Range

= 1 - 99, 1 is the highest priority and 99 is the lowest)

- **Mapping Condition** - Select "Show Basic Attribute Selection" to display basic conditions, select "Show Advanced Attribute Selection" to show advanced conditions. Select an Attribute and corresponding Operator, then select or enter a Value
- **Authentication Type**
 - **802.1X** - 802.1X authentication
 - **MAC** - MAC authentication
- **Network Type**
 - **Wireless** - Wireless network
- **SSID**
 - Select the Wireless network SSID in this Site
- **AP IP**
 - Enter the AP IP address or select AP IP from drop down menu
- **AP Name**
 - Enter the AP Name or select AP Name from drop down menu
- **User Mac**
 - Enter the User Mac address
- **Authentication Strategy** - Authentication strategy that will be utilized when the Access Policy is matched

Editing an Access Policy

Select a policy in the Access Policy List and click on the Edit icon. Edit the field(s) as described above and click on the **Save** button. Note that you cannot edit a Policy Name.

Deleting an Access Policy

Select a policy in the Access Policy List and click on the Delete icon. Click **Yes** at the Confirmation Prompt.

10.3.3. Authentication Strategy

Authentication Strategy is used to set up a user profile source and login method (web page or not) for authentication, as well as the network attributes applied after passing the authentication.

The **Authentication Strategy Screen** displays all configured authentication strategies and is used to create, edit, and delete Authentication Strategies.

Creating an Authentication Strategy

Click on the + icon to bring up the Create Authentication Strategy Screen. Complete the fields as described below, then click on the **Save** button.

General

- **Strategy Name** - Authentication strategy name
- **Authentication Source** - Specify the source of the user profile (Account/Password). The user profile can reside different servers and is required to specified so that Authenticate is able to obtain the user profile for authentication.
 - **None** - Authenticate against "None". This is only supported for MAC authentication, which requires captive portal authentication. 802.1x Authentication is not supported. In this case, a user needs to pass captive portal authentication first (authentication method could be by Account + Password / Access Code), the MAC address of the user will be stored and the user will complete the MAC authentication. For a guest user, the devices will be displayed in Authenticate Profile - Guest Access - Guest Device - Remembered Device Screen. For an Employee user, the devices will be displayed in Authenticate Profile - BYOD Access - BYOD Device - Remember Device Screen.
 - **Local Database** - Authenticate against the user profile in the local database. An Employee or Guest user must be created before authentication. An Employee User is created on the Authentication – Employee Access - Employee Account Screen. A Guest User is created on the Authentication - Guest Access - Guest Account Screen.
 - **External LDAP/AD** - Authenticate against the user profile in an external LDAP/AD sever. The server is configured on the Authentication – Setting - LDAP/AD Configuration Screen.
 - **External Radius** - Authenticate against the user profile in an external RADIUS server. The server is configured on the Authentication – Setting - External Radius Screen.

Web Redirection Enforcement Policy

- **Web Authentication** - Specify whether or not web redirection is required and which web login page is going to be used during the authentication.
 - **None** - No web redirection during the authentication.
 - **Guest** - Redirect to the guest login page during the authentication.
 - **Employee** - Redirect to the employee login page during the authentication.
- **Access Strategy** - Specify the access strategy for each user group.
 - **Guest Access Strategy** - Specify the access strategy for guest users.
 - **Employee Access Strategy** - Specify the access strategy for employee users.

Network Enforcement Policy

- **Default Access Role Profile** - Default Access Role Profile for the authentication strategy.
- **Default Policy List** - Default Access Policy for the authentication strategy.
- **Session Timeout Status** - If set to OFF, the User Session never timeout.
- **Session Timeout Interval** - The Session Timeout Interval is the maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt. If not configured, the device's default session timeout policy will take effect. (Range = 12000 - 86400, Default = 43200)
- **Account External Radius** - Whether to forward accounting message to external radius
- **Accounting Interim Interval** - Interval for RADIUS accounting, in seconds. If not configured, the device's default accounting policy will take effect. (Range = 60 – 1200, Default = 600)

10.3.4. Role Mapping for LDAP

Authentication Role Mapping for LDAP/AD enables you to assign different Access Role Profiles and Policy Lists to different sub-user groups by creating mapping rules based on user attributes. The Role Mapping for LDAP/AD Screen displays all configured mappings and is used to create, edit, and delete mappings.

The Role Mapping List displays information about all configured mappings.

- **Condition** - The mapping condition configured for the policy
- **Default Access Role Profile** - Access Role Profile applied to the user after matching the role mapping rule.
- **Default Policy List** - Policy List applied to the user after matching the role mapping rule.
- **Name** - User-configured name for the mapping rule.
- **Priority** - Priority of the role mapping rule. A user requesting LDAP/AD authentication may match several role mapping rules; the one with highest priority will take effect after passing authentication. (Range = 1 - 99, 1 is the highest priority and 99 is the lowest).

Create Role mapping for LDAP

- **Name** - User-configured name for the mapping rule. Required.
- **Priority** - Priority of the role mapping rule. A user requesting LDAP/AD authentication may match several role mapping rules; the one with highest priority will take effect after passing authentication. (Range = 1 - 99, 1 is the highest priority and 99 is the lowest). Required.
- **LDAP/AD Attribute Condition** - Pairs of Attribute and Value for referring to LDAP/AD account.
 - **Attribute** - LDAP/AD attributes used as role mapping rule key.
 - **Value** - Role mapping rule value
- **Default Access Role Profile** - Access Role Profile applied to the user after matching the role mapping rule.
- **Default Policy List** - Policy List applied to the user after matching the role mapping rule.

Editing a Mapping

Select a mapping Role Mapping List and click on the Edit icon. Edit the field(s) as described above and click on the Save button. Note that you cannot edit a Mapping Name.

Deleting a Mapping

Select a mapping in the Role Mapping List and click on the Delete icon. Click **Yes** at the Confirmation Prompt.

10.3.5. Authentication Record

The Authentication Record Screen displays authentication information for all devices authenticated. The Authentication Record List provides basic information.

- **Account** - Indicates the user name of the user to be authenticated.
 - **MAC Authentication** - Account name is the MAC address of the user device.
 - **802.1X Authentication** - Account name is the user name of the employee user.
 - **Captive Portal Authentication** - Account name is user name of the guest user or employee user.
- **Device IPv4** - The IPv4 address of the client of the user device requesting authentication. Note that IP addresses are displayed only if they are known at the time the RADIUS Accounting packets are sent/received. For MAC Authentication, the Accounting Start packets typically do not contain client IP addresses.
- **Device IPv6** - The IPv6 address of the client of the user device requesting authentication. Note that IP addresses are displayed only if they are known at the time the RADIUS Accounting packets are sent/received. For MAC Authentication, the Accounting Start packets typically do not contain client IP addresses.
- **Device MAC** - MAC address of the user device requesting authentication.
- **Account Type** - Group to which the requesting authentication user belongs:
 - Guest
 - Employee
 - Unknown (MAC authentication without captive portal)
- **Session Start** - The time when the user passed authentication and a connection session was created.
- **Acc Status Type** - The accounting status.
- **Acct Interim Interval** - The number of seconds between each interim update, in seconds, for this specific session.
- **Session Timeout** - Specifies the maximum number of seconds of service provided prior to session termination.
- **Session ID** - Session ID that makes it easy to match start and stop records in a log file. The start

and stop records for a given session MUST have the same Session ID.

- **Access Device MAC** - MAC address of the NAS to which the user device is attached.
- **Access Device Name** - System name of the NAS to which the user device is attached.
- **Association SSID** - Wireless service broadcast by the DAPs and connected by user device (only valid for wireless access).
- **Auth Resource** - User profile database used in authentication, including None, Local Database, LDAP/AD and external RADIUS server, can refer to the authentication strategy definition.
- **Expire Time** - The time when the account is going to expire.
- **Framed MTU** - User profile database used in authentication, including None, Local Database, LDAP/AD and external RADIUS server, can refer to the authentication strategy definition.
- **NAS IP** - IP Address of the NAS
- **NAS Port** - The physical port number of the NAS authenticating the user. For AP, it is the Wireless Radio index.
- **Network Type** - It can only be Wireless - Wireless network.
- **Service Type** - This attribute indicates the type of service the user has requested, or the type of service to be provided. It may be used in both Access-Request and Access-Accept packets. A NAS is not required to implement all of these service types, and must treat unknown or unsupported Service-Types as though an Access-Reject had been received. .
- **Access Device Location** - Location of the DAP which the user device is attached.

10.3.6. Portal Access Record

The Authentication Portal Access Record Screen displays captive portal information for all devices authenticated on DAC. The Portal Access Record List provides basic information.

- **User Name** - User name of the device requesting authentication.
- **User MAC** - MAC address of the user device requesting captive portal authentication.
- **AP MAC** - AP MAC address.
- **ESSID** - ESSID that the portal user associated.
- **Connections Time** - The portal user login at this time.

- **Offline Time** - The portal user logoff or timeout at this time.
- **Status** - Result for the user authentication request
 - **Online** - This Captive portal authentication is Accept.
 - **Reject** - This Captive portal authentication is Reject.
 - **Empty Value** - Captive portal authentication is not activated.
- **Portal Type** - The Captive Portal usage (Employee/Guest).
- **AP Name** - The name of AP that the user attached.
- **AP Location** - The Location of AP that the user attached.

10.4. Guest Access

The Guest Access is used to manage guest users accessing the network. Guest Access service is based on the captive portal authentication. It consists of Dashboard, Guest Access Strategy, Guest Account, Guest Device.

10.4.1. Dashboard

Dashboard consist of four dial gram, they are Guest Account and Devices Statistics, Guest Device Browser, Guest Device Category and Guest Account Creation Mode alternatively.

Guest Account and Device Statistics - Count the number of different types of accounts (New created account, Active guest account, Total guest account) or devices (Total guest device).

Guest Device Browser - Pie chart of browser type (Chrome, IE and so on).

Guest Device Category - Pie chart of Device Category (COMPUTER, MOBILIE and so on)

Guest Account Creation Mode - Pie chart of Account Creation Mode

10.4.2. Guest Access Strategy

The Guest Access Strategy Screen is used to configure access attributes for guest users. The screen can be used to create, edit, and delete Guest Access Strategies. There is a preconfigured Default Guest Access Strategy that you can edit, or you can create new Guest Access Strategies.

- **Name** - The Guest Access Strategy name.
- **Account Validity Period** - Account validity period
- **Device Validity Period** - Device Mac authentication validity period.
- **Max Device per Account** - Limits of device which use this guest account on the same time.
- **Fixed Access Role Profile** - The Access Role Profile assigned to the guest user after passing authentication.
- **Fixed Policy List** - The Policy List assigned to the guest user after passing authentication.
- **Authentication Resource** - Local Database

Creating a Guest Access Strategy

Click on the + icon and complete the fields as described below. When you are finished, click on the **Save** button.

General

Configure redirect and authentication attributes.

- **Name** - Guest strategy name
- **Authentication Resource** - The guest user profile database, which is the local database (Local Database). Guest user accounts can be added on the Authentication Profile - Guest Access - Guest Account Screen.

Registration Strategy

- **Account Validity Period** - The length of time that the guest account is valid. (Range = 1 – 180 Days, Default = 90 Days).
- **Device Validity Unit** - The classifier of Device Validity Period. Can be select as day or minute.
- **Device Validity Period** - The length of time that the user device is valid. (Range = 1 – 365 Days, Default = 1 Days). After authentication success, it will remember the device MAC address. The MAC address check will be performed first and the device allowed access without re-authentication.
- **Max Device per Account** - The maximum number of devices that can access the network with one single account. (Range = 1 – 10, Default = 1).

Portal

- **Custom Portal Page** - You can edit the page type and page style at the time of portal authentication. See [Captive Portal](#) for more details

Post Portal Authentication Enforcement

- **Fixed Access Role Profile** - The Access Role Profile assigned to the Guest device after it is authorized.
- **Fixed Policy List** - The Policy List assigned to the Guest device after it is authorized.
- **Session Timeout Status** - Enable/Disable the Session Timeout.
- **Session Timeout Interval** - The Session Timeout Interval is the maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt. If not configured, the device's default session timeout policy will take effect. (Range = 12000 - 86400, Default = 43200)
- **Accounting Interim Status** - Enable/Disable the Accounting Interim.
- **Accounting Interim Interval** - Interval for RADIUS accounting, in seconds. (Range = 60 - 1200, Default = 600)

Editing a Guest Access Strategy

Select a strategy in the Guest Access Strategy List and click on the Edit icon. Edit any fields as described above and click on the **Save** button. Note that you cannot edit the Strategy Name.

Deleting a Guest Access Strategy

Select a strategy(ies) in the Guest Access Strategy List and click on the Delete icon. Click **Yes** at the Confirmation Prompt. You cannot delete the Default Guest Access Strategy.

10.4.3. Guest Account

Guest Account use to manage the set of guest accounts. You could add one item through clicking the + icon. Or you can download the account template and fill it with the guest accounts you want. Then batch import the accounts use the **Batch Import** button. Also, you could enable or disable the guest account manually by click the **enable/disable** button.

Creating a Guest Account:

Guest can access by Account or Access Code. Access code is a special type of account, which is distinguished by internal tags. When logging in, users use the portal template of access code. They only need to enter access code without entering password.

Click on the Add icon to bring up the Create Guest Account Screen. Complete the fields as described below, then click on the Save button. When an account is created, it is automatically enabled. To disable and account, select the account and click on the Disable icon at the top of the screen.

Guest Type in Account:

- **Guest Account Name** - Account identifier (e.g., name of the guest). **Required**
- **Password** - Password for the account. **Required**
- **Confirm Password** - Re-enter and confirm the account password. **Required**
- **Full Name** - Full name of the Guest User.
- **Company** - Company name. **Optional**
- **Account Valid Period** - The length of time that the guest account is valid. (Range = 1 – 180 Days, Default = 90 Days). **Required**
- **Telephone** - Telephone number of the Guest User. **Optional**
- **Email** - Email address of the Guest User. **Optional**
- **Description** - Description for the account. **Optional**

Guest Type in Access Code:

- **Access Code** - Access Code. **Required**
- **Account Validity Period** - The length of time that the guest account is valid. (Range = 1 – 180 Days, Default = 90 Days). **Required**
- **Description** - Description for the Access Code. **Optional**.

Editing a Guest Account/Access Code

Select a Guest Account in the Guest Account List and click on the Edit icon. Edit the field(s) as described above and click on the **Save** button. Note that you cannot edit an Account Name.

Deleting a Guest Account/Access Code

Select a Guest Account in the Guest Account List and click on the Delete icon. Click **Yes** at the Confirmation Prompt.

10.4.4. Guest Device

There are two kinds of device list, Online Devices list and Remember Devices list.

Online Devices

Online Devices list the devices online currently.

- **Account Name** - The account of terminal access network.
- **Device IPv4** - The IPv4 address of the client of the user device requesting authentication. Note that IP addresses are displayed only if they are known at the time the RADIUS Accounting packets are sent/received. For MAC Authentication, the Accounting Start packets typically do not contain client IP addresses. It would be updated after next Accounting Update packet received.
- **Device IPv6** - The IPv6 address of the client of the user device requesting authentication. Note that IP addresses are displayed only if they are known at the time the RADIUS Accounting packets are sent/received. For MAC Authentication, the Accounting Start packets typically do not contain client IP addresses
- **Device MAC** - MAC address of Device.
- **Session Start** - The time when the user passed authentication and a connection session was created.
- **Acct Status Type** - Indicates whether this Accounting-Request marks the beginning of the user service or the end.
- **Acct Interim Interval** - The number of seconds between each interim update, in seconds, for this specific session.
- **Session Timeout** - The Session Timeout is the maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt.
- **Session ID** - Session ID that makes it easy to match start and stop records in a log file. The start and stop records for a given session MUST have the same Session ID.

- **Access Device MAC** - The MAC address of device which the terminal associated.
- **Access Device Name** - The name of device which the terminal associated.
- **Association SSID** - The SSID that the terminal association.
- **Auth Resource** - The user profile database used in authentication (e.g., None, Local Database, LDAP/AD, external RADIUS server); can refer to the authentication strategy definition.
- **Expire Time** - Expire time of this device.
- **Framed MTU** - The Maximum Transmission Unit to be configured for the user when it is not negotiated by some other means (e.g., PPP). It is a fixed value = 1400.
- **NAS IP** - The IP Address of the DAP.
- **NAS Port** - The physical port number of the NAS authenticating the user. For AP, it is the Wireless Radio index.
- **Network Type** - Network Type. It can only be wireless.
- **Response Type** - Response Type.
- **Service Type** - This attribute indicates the type of service the user has requested, or the type of service to be provided. It can only by Login User
- **Access Device Location** - The location of device which the terminal associated.

Remember Devices

The Remembered Device List displays all authenticated GUEST devices saved in DAC and can be utilized for MAC authentication

- **Account Name** - The account of the remembered device.
- **Device Name** - The name of the remembered device.
- **Device MAC** - The MAC address of the remembered device.
- **Device OS** - The OS of the remembered device.
- **Expiration Time** - Expire time of this device.
- **First Login Time** - This remember item is record at this time.

10.5. Employee Access

The Employee Access is used to manage employee users accessing the network. It consists of Dashboard, Employee Access Strategy, Employee Account, Employee Device.

10.5.1. Dashboard

Dashboard consist of three dial gram, they are Remembered Employee Device Statistics, Devices Category, Device Family alternatively.

Remembered Employee Device: Histogram of remember device and online device last 7 days.

Devices Category: Pie chart of Device Category (COMPUTER, MOBILIE and so on)

Device Family: Displays information by device family (e.g., Apple, IBM, HUAWEI, XIAOMI) in a pie chart format

10.5.2. Employee Access Strategy

The employee strategy module is used to configure employee portal policies. It can configure portal account authentication sources (including local database, external LDAP / AD, external radius), account validity and device validity, maximum number of online devices, specify Access Role Profile policies, edit portal templates, etc.

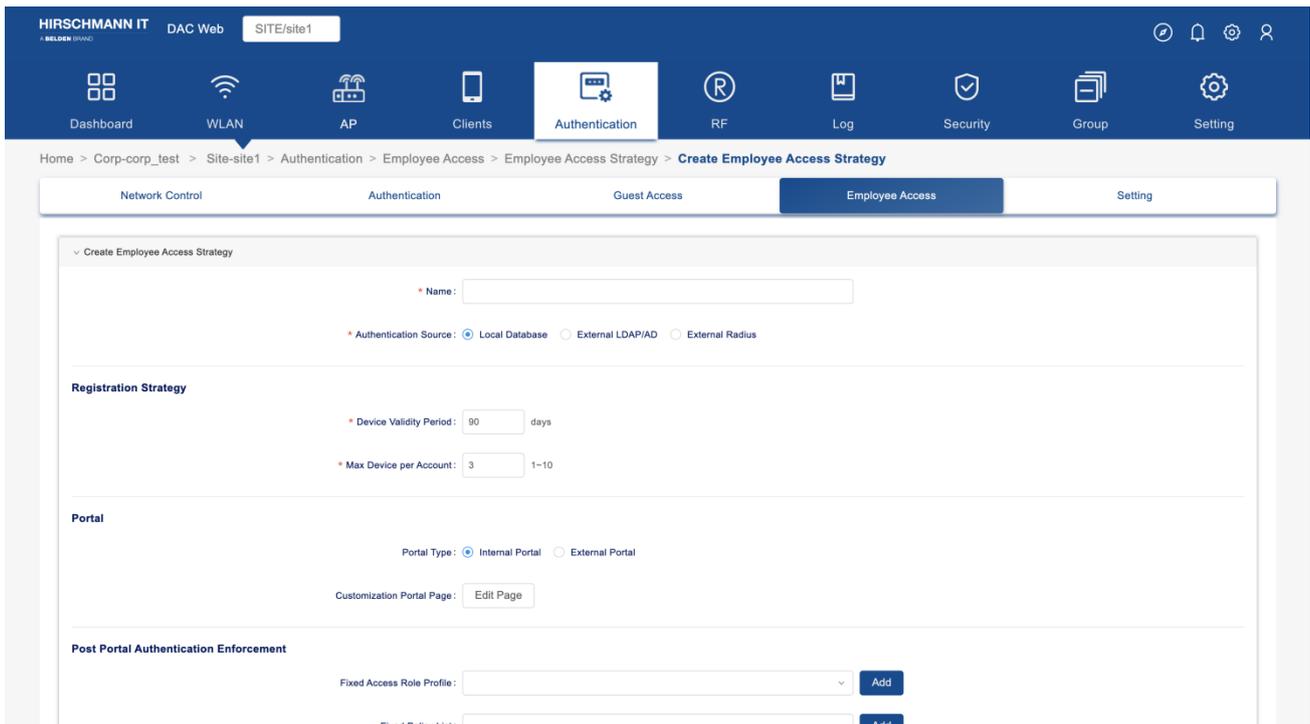


Figure 10-5-2-1

- **Strategy Name** - Employee strategy name
- **Device Validity Period** - After the visitor passes the authentication, there will be an authentication free record. The validity period of the authentication free record is specified here
- **Max Device per Account** - Number of terminals that can be sign in on the same time with the same account
- **Customization Portal Page** - You can edit the page type and page style at the time of portal authentication
- **Fixed Access Role Profile** - When this authentication phase is over, the Access Role Profile assigned to the terminal is used to control the Internet access behavior of the terminal
- **Account External Radius** - Whether to forward accounting message to external radius
- **Accounting Interim Interval** - Specify the time interval for AP to send accounting message to US.

10.5.3. Employee Account

Employee Account use to manage the set of Employee terminal accounts. You could add one item through clicking the + icon or download the account template and fill it with the employee accounts

you want; the batch import the accounts. Also, you could enable or disable the employee account manually by click the **enable/disable** button.

The Employee Account List displays information about all configured Employee accounts.

- **Username** - User name for the employee account.
- **Telephone** - Telephone number of the employee.
- **Email** - Email address of the employee.
- **Effective Date** - The date and time the account was created.
- **Full Name** - Full name of the employee.
- **Department** - Department of the employee.
- **Position** - Employee position in the company.
- **Description** - Description of the employee account.
- **Access Role Profile** - Access Role Profile that is bound to the employee account. It is prior to the Access Role Profile configured in Authentication Strategy.
- **Policy List** - Policy List that is bound to the employee account. It is prior to the Policy List configured in an Authentication Strategy.

Create Employee Account:

- **Username** - User name for the employee account. **Required**
- **Password** - Password for the employee account. **Required**
- **Repeat Password** - Re-enter to confirm the employee password. **Required**
- **Telephone** - telephone number of the employee. **Optional**
- **Email** - Email address of the employee. **Optional**
- **Access Role Profile** - Access Role Profile that is bound to the employee account. It is prior to the Access Role Profile configured in Authentication Strategy. **Optional**
- **Policy List** - Policy List that is bound to the employee account. It is prior to the Policy List configured in an Authentication Strategy. **Optional**
- **Full Name** - Full name of the employee. **Optional**
- **Department** - Department of the employee. **Optional**

- **Position** - Employee position in the company. **Optional**
- **Description** - Description of the employee account. **Optional**

Editing an Employee Account

Select an employee in the Employee Account List and click on the Edit icon. Edit the field(s) as described above and click on the Apply button. Note that you cannot edit a Username.

Deleting an Employee Account

Select an employee in the Employee Account List and click on the Delete icon. Click **Yes** at the Confirmation Prompt.

10.5.4. Employee Device

Employee Device divide into two kind of devices, one is Online Devices, another is Remember Devices.

Online Devices list the devices online.

Online Device

The Online Devices List displays information about devices associated with an Employee account that have accessed the network. You can also select a device(s) in the list and click on the **Kick-off** button to immediately log the user out of the network. The user will have to log in again to connect to the network again.

- **Account** - The employee account to which the company device is associated
- **Device IPv4** - The IPv4 address of the client of the user device requesting authentication. Note that IP addresses are displayed only if they are known at the time the RADIUS Accounting packets are sent/received. For MAC Authentication, the Accounting Start packets typically do not contain client IP addresses.
- **Device IPv6** - The IPv6 address of the client of the user device requesting authentication. Note that IP addresses are displayed only if they are known at the time the RADIUS Accounting packets are sent/received. For MAC Authentication, the Accounting Start packets typically do not contain client IP addresses.
- **Device MAC** - MAC address of the device.

- **Session Start** - The time when the user passed authentication and a connection session was created.
- **Acct Status Type** - Indicates whether this Accounting-Request marks the beginning of the user service or the end.
- **Acct Interim Interval** - The number of seconds between each interim update, in seconds, for this specific session.
- **Session Timeout** - The Session Timeout is the maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt.
- **Session ID** - Session ID that makes it easy to match start and stop records in a log file. The start and stop records for a given session MUST have the same Session ID.
- **Access Device MAC** - The MAC address of device which the terminal associated.
- **Access Device Name** - The name of device which the terminal associated.
- **Association SSID** - The SSID that the terminal association.
- **Auth Resource** - The user profile database used in authentication (e.g., None, Local Database, LDAP/AD, external RADIUS server); can refer to the authentication strategy definition.
- **Expire Time** - Expire time of this device.
- **Framed MTU** - The Maximum Transmission Unit to be configured for the user when it is not negotiated by some other means (e.g., PPP). It is a fixed value = 1400.
- **NAS IP** - The IP Address of the DAP.
- **NAS Port** - The physical port number of the NAS authenticating the user. For AP, it is the Wireless Radio index.
- **Network Type** - Network Type. It can only be wireless.
- **Response Type** - Response Type.
- **Service Type** - This attribute indicates the type of service the user has requested, or the type of service to be provided. It can only by Login User.
- **Access Device Location** - The location of device which the terminal associated.

Remember Device

Remember Device list the devices that those devices will not be authenticate again in the next access

process.

- **Account** - The account of the remembered device.
- **Device Name** - The name of the remembered device.
- **Device MAC** - The MAC address of the remembered device.
- **Device OS** - The OS of the remembered device.
- **Expiration Time** - Expire time of this device.
- **First Login Time** - This record is record at this time.

10.6. Setting

The item of Setting includes several additional configurations.

10.6.1. Company Device

Company Device use to manage the set of devices owned by a company, such as printers, IP phones, laptops, tablets. You could add one item through clicking the + icon, or download the account template and fill it with the Company Device you want, the batch import the accounts. Also, you could export all the Company Device in format of .xlsx.

Create Company Device

- **Device MAC** - MAC address of the company device. **Required**
- **Device Name** - System name of the company device.
- **Account** - The employee account to which the company device is associated.
- **Device Category** - Category of the company device (e.g., Computer, Mobile Tablet).
- **Device Family** - Production vendor of the company device (e.g., Apple, HUAWEI, IBM).
- **Device OS** - Operation system of the company device (e.g., Linux, Windows, IOS).
- **Device Specific PSK** - If enabled, you should be setting the password and Passphrase Validity Period. This function needs to work with WLAN settings of [Device Specific PSK](#).
- **Access Role Profile** - Access Role Profile that is bound to the company device. It is prior to the ARP configured in authentication strategy.

- **Policy List** - Policy List that is bound to the company device. It is prior to the policy list configured in authentication strategy.

Delete Company Device

Select the Company Devices that you want to delete, click Delete icon, then click **Yes** button at the confirmation prompt.

10.6.2. LDAP/AD Configuration

The LDAP / AD module is used to configure the LDAP / AD source. When LDAP / AD authentication is selected for a policy, the authentication source will be used for authentication.

- **LDAP/AD Server** - Enable/Disable to Using LDAP or AD server
- **Server Type** - Selector of LDAP or AD server

For LDAP Configuration

- **IP Address** - The IP address of LDAP Server
- **Port** - The port of LDAP server
- **Use TLS Encryption** - The switch of using TLS. If turn it on, should upload the certification.
- **Certificate** - To upload certification used by TLS. You should get the certification from the external LDAP Server.
- **Admin Name** - Administrator account used to login into the LDAP server. Format: cn=,DC=< 8-64 characters >.
- **Admin Password** - Administrator password used to login into the LDAP server. (1 – 32 characters)
- **Search Base** - < 8-64 characters >
- **Username Attribution** - The field in an LDAP entry that represents the username used for authentication. (1 - 32 characters)
- **Password Attribution** - The field in an LDAP entry that represents the password used for authentication. (1 - 32 characters)
- **Object Class** - Define named collections of attributes and classify them into sets of required and optional attributes. (1 - 32 characters)

For AD Configuration

- **Workgroup Name** - workgroup of the AD Server
- **Realm** - realm of the AD Server.
- **Realm IP** - IP of the AD Server.
- **Username** - Username used to access the AD Server.
- **Password** - Password used to access AD Server.
- **AD Port** - Port used to access the AD Server



Note

To load Windows AD server configuration, please configure DNS settings for Ubuntu system or VM initialization.

10.6.3. External RADIUS

The external radius module is used to configure the external radius authentication source. When an external radius authentication is selected for a policy, the authentication source will be used for authentication.

- **Server Name** - Name of the RADIUS Server.
- **IP Address** - External Radius Server host name/IP address
- **Backup IP Address** - Back up external radius server host name/IP address
- **Retries** - Number of times DAC will attempt to reconnect to the External Radius Server when the connection timeout occurs before concluding that the External Radius Server is unreachable. (range = 1 – 3, Default = 3)
- **Timeout** - The amount of time, in seconds, that DAC will attempt a connection to the External Radius Server before timing out. (Range = 1 – 30, Default = 5)
- **Shared Secret** - Shared key that DAC uses to communicate with External Radius Server. (4 - 64 characters)
- **Confirm Secret** - Re-enter to confirm the shared secret key. (4 - 64 characters)
- **Authentication Port** - UDP port used to perform authentication. (Range – 1 – 65535, Default = 1812)
- **Accounting Port** - TCP/UDP port used to perform accounting. (Range – 1 – 65535, Default =

1813)

10.6.4. Allowed IP

An allowed IP is a IP address that terminal can access before login from captive portal. Usually you should add portal server's IP to Allowed IP.

Create an Allowed IP

Click + icon to bring up the **Create Allowed IP Screen**, input **Name** and **IP Address** fields, click **Save** button to save the allowed IP.

- **Name** - The identify of allowed IP. Required.
- **IP Address** - setting of the IP address. Required

Edit an Allowed IP

Select the allowed IP from the list, click edit icon to bring up the **Edit Allowed IP Screen**. Edit the **IP Address** and click **Save** button to save this change. Notice that the **Name** field cannot change.

Delete an Allowed IP

Select the items that you want to delete, click on the **Delete** icon, then click **Yes** button at the confirmation prompt.

10.6.5. MAC Groups

The Groups MAC Groups Screen displays all configured MAC Groups. The screen is used to create, edit, and delete MAC Groups, which can be used in creating various policy conditions, such as source MAC group condition and destination MAC group condition.

Creating a MAC Group

Click on the + icon to bring up the **Create MAC Group Screen**. Enter a Name for the MAC Group. Enter a MAC Address and click on the **Add** button. Repeat to add additional addresses. When you are done, click on the **Add** button at the bottom. The MAC Group will appear in MAC Groups List. Note that you must enter at least one MAC Address.

Editing a MAC Group

Select the MAC Group that you want to edit, click the **edit** icon to bring up the **Edit MAC Group Screen**. Note that you cannot edit a MAC Group name. To edit a MAC Group name, you must delete the MAC Group and create a new one.

- To add a MAC Address to the Group, enter the MAC Address, then click on the **Add** button. Repeat to add additional addresses. When you are done, click on **Edit** button.
- To delete a MAC Address, click on the Delete icon next to the MAC Address you want to delete. Repeat to delete additional addresses. When you are done, click on the **Edit** button.
- To edit a MAC Address, you should delete it and then add a new one.

Deleting a MAC Group

To delete a MAC Group(s), select the checkbox next to the group(s) in the list, click on the **Delete** icon, then click **Yes** at the confirmation prompt.



Note

MAC Groups that are in use by policy conditions cannot be deleted. To delete these MAC groups, remove them from the policy conditions.

10.6.6. IP Groups

The Groups IP Groups Screen displays all configured IP Groups. The screen is used to create, edit, and delete Network Groups.

Creating a IP Group

Click on the + icon. Enter a Name for the IP Group. Enter a Subnet IP/Subnet Mask and click on the Add button. Repeat to add additional subnets. When you are finished, click on the **Add** button at bottom. The IP Group will appear in IP Groups List. Note that you must enter at least one Subnet IP/Subnet Mask.

Editing a IP Group

Click on the IP Group that you want to edit to view the Subnets in the IP Group. Note that you cannot edit a IP Group name. To edit a IP Group name, you must delete the Network Group and create a new one.

- To add a Subnet Address to the Group, enter a Subnet IP/Subnet Mask and click on the Add icon. Repeat to add additional subnets. When you are finished, click on the **Edit** button.
- To delete a Subnet, click on the Delete icon next to the Subnet you want to delete. Repeat to delete Subnets. When you are done, click on the **Edit** button.
- To edit a Subnet, you should delete the Subnet and add a new one. When you are done, click on the **Edit** button.

Deleting a IP Group

To delete a IP Group(s), select the checkbox next to the group(s) in the list, click on the Delete icon, then click **Yes** at the confirmation prompt. IP Groups that are in use by policy conditions cannot be deleted. To delete these IP groups, remove them from the policy conditions.

10.6.7. Service Port

The Groups Service Port Screen displays all configured Service Ports, which are used to create Services. By default, the TCP radio is selected and TCP Services are displayed. Click on the UDP radio to display UDP Services. The screen is used to create, edit, and delete Service Ports.

Creating a Service Port

Click on the Add icon. Complete the fields as described below, then click on the **Save** button.

- **Name** - User-configured name for the Service Port.
- **Source Port Range** - Enter a Source Port number or Port number range(set range like 22:33).
- **Destination Port Range** - Enter a Destination Port number or Port number range.

Editing a Service Port

Click on the Service Port that you want to edit, then click on the Edit Icon. Edit the field(s) as described above then click on the **Save** button. You cannot edit a Service Port name and the protocol. To edit a Service Port name, you must delete the Service Port and create a new one.

Deleting a Service Port

To delete a Service Port(s), select the checkbox next to the port(s) in the list, click on the Delete icon, then click **Yes** at the confirmation prompt. Service Ports that are in use by Services cannot be deleted.

To delete these Service Ports, remove them from the Service.

10.6.8. Services

The Groups Services Screen displays all configured Services, which are used to create Service Groups. The screen is used to create, edit, and delete Services.

Creating a Service

Click on the + icon. Complete the fields as described below, then click on the **Save** button.

- **Service Name** - User-configured name for the Service.
- **Protocol** - Select a protocol for the Service. By default, the TCP radio is selected and TCP ports are displayed. Click on the UDP radio to display UDP ports.
- **Service Port** - Select a service port from the drop-down list. The drop-down box includes If you want to create a new Service Port, click on the Add Icon to go to the Service Port Screen and create a new Service Port. When you click on the **Save** button on the Service Port Screen you will be returned to the Create Service Screen to finish creating the Service.

Editing a Service

Click on the Service that you want to edit, then click on the Edit Icon. Edit the field(s) as described above then click on the **Edit** button. You cannot edit a Service Name. To edit a Service Name, you must delete the Service and create a new one.

Deleting a Service

To delete a Service(s), select the checkbox next to the Service(s) in the list, click on the Delete icon, then click **Yes** at the confirmation prompt.



Note

Services that are in use by policy conditions cannot be deleted. To delete these Services, remove them from the policy conditions.

10.6.9. Service Groups

The Groups Service Groups Screen displays all configured Service Groups. The screen is used to create, edit, and delete Service Groups.

Creating a Service Group

Click on the + icon. Enter a Group Name for the Service Group. Select a Service(s) and click on the Save button. If you want to create a new Service, click on the Add Icon to go to the Services Screen and create the Service. When you click on the Save button on the Services Screen you will be returned to the Create Service Group Screen to finish creating the Service Group. Note that you must enter at least one service.

Editing a Service Group

Click on the Service Group that you want to edit, then click on the Edit Icon. Add or remove Services from the group as described above then click on the **Edit** button. You cannot edit a Service Group name. To edit a Service Group name, you must delete the Service Group and create a new one.

Deleting a Service Group

To delete a Service Group(s), select the checkbox next to the group(s) in the list, click on the Delete icon, then click **Yes** at the confirmation prompt.

Note: Service Groups that are in use by policy conditions cannot be deleted. To delete these Service Groups, remove them from the policy conditions.

10.7. Default Config and Quick Entrance

All the above configurations are indirectly bound to WLAN. In order to simplify the configuration, we can directly select the default configuration when configuring WLAN. At the same time, we also provide a quick entry for authentication configuration when configuring WLAN. As shown below:

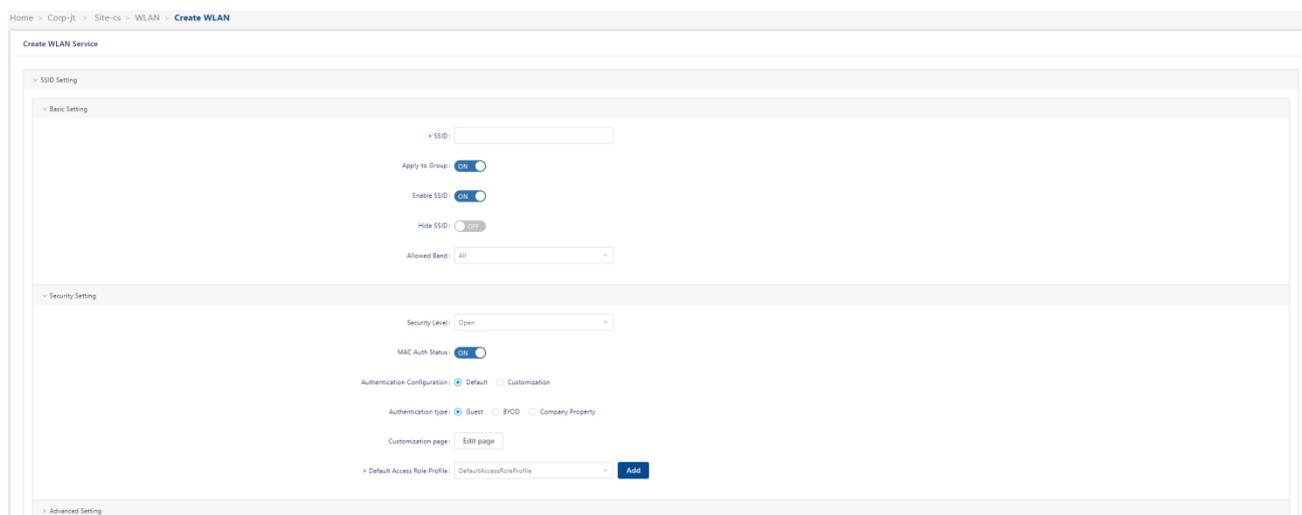


Figure 10-7-1

In WLAN configuration, if **MAC auth** is selected, a set of default authentication configurations will be selected by default. **Customization** is a shortcut for user-defined authentication. After selecting it, the configuration wizard button will appear. The configuration is consistent with the above modules and will not be repeated in this section.

When you select Default at Authentication Configuration, It will generate a set of authentication configurations automatically in the background. And you can not view or edit these configurations directly.

The default Authentication Configurations automatically generated is as follows:

1. When you select Guest for Authentication Type, an Authentication Strategy will be automatically generated, with none as the Data Source. At the same time, a Guest Access Strategy will be generated and bounded to the Authentication Strategy. You can customize the portal page in the following Customization Page settings
2. When you select Employee for Authentication Type, an Authentication Strategy will be automatically generated with none as the data source. At the same time an Employee Access Strategy will be generated and bounded to the Authentication Strategy. You can customize the portal page in the following Customization Page settings.
3. When you select Company Device for Authentication Type, an Authentication Strategy with local database as the data source will be automatically generated.
4. At last, it will generate an Access Policy with SSID as the mapping condition and with a highest

priority and bind with the Authentication Strategy Previously mentioned



Note

The configuration generated by default is bound to WLAN, and users cannot view it.

10.8. Configuration Instances for Authentication

Before introducing specific configuration instances, you should better understand the basic concepts of Authentication about DAC. Read the section of [Authentication](#) to get them.

10.8.1. Configure 802.1X Authentication in Default(simple model)

1. At the Site View, Click WLAN tab to view WLAN list.
2. Click "+" button to open Create WLAN page.
3. Fill the SSID.
4. Select **Enterprise** at **Security Level** drop down list.
5. Select Encryption Mode that you want. Click "[SSID Setting](#)" to see more information about Encryption Mode.
6. Set the Authentication Configuration to **Default**, which means it will create **Access Policy**, **Authentication Strategy** and **Employee Access Strategy** automatic (if necessary), and these Policies/Strategies are not viewable. But you can see that there are three Authentication Sources: **Local Database**, **External LDAP/AD**, **External Radius**. These Authentication Sources are export from the **Authentication Strategy** created by default. We use this method to simplify some user configurations.
7. If you select **Local Database** Authentication Source, you can add user at the page **Authentication -> Employee Access -> Employee Account**. For detailed information of **Employee Account**, you can refer to [Employee Account](#).
8. If you select **LDAP/AD** Authentication Source, you should Configure LDAP/AD at the page **Authentication -> Setting -> LDAP/AD Configuration**. For detailed information of **LDAP/AD configuration**, you can refer to [LDAP/AD Configuration](#). If you want to set a specific **Access Role Profile** to the terminal authenticated by LDAP, you can set the corresponding mapping rules in **Authentication -> Authentication -> Role Mapping for LDAP**
9. If you select **External Radius** Authentication Source, you can select an External Radius Server

at the drop down list. Or click the **Add** button to add a new External Radius Server. You can also add new External Radius Server at page **Authentication -> Setting -> External Radius**. For detailed information of **External Radius**, you can refer to [External Radius](#).

10. At the **Default Access Role Profile**, select a Profile at the drop down menu. Or you can add a new Access Role Profile by clicking the **Add** button next to it. Click "[Access Role Profile](#)" to see more information about **Access Role Profile**.

10.8.2. Configure Portal Authentication in simple model

1. At the Site View, Click WLAN tab to view WLAN list.
2. Click "+" button to open Create WLAN page.
3. Fill the SSID.
4. Select **Open** at Security Level drop down list.
5. Set the **Mac Auth** at "ON" status.
6. Select "**Default**" at the Authentication Configuration. You cannot select Authentication source for "**Guest**" or "**Employee**" at this model. It uses local databases as default.
7. Select "**Guest**" for Guest Authentication. You can add Guest Accounts at **Authentication -> Guest Access -> Guest Account**. For detailed information of **Guest Account**, you can refer to [Guest Account](#).
8. Select **Employee** for **Employee Authentication Strategy**. You can add Employee Accounts at **Authentication -> Employee Access -> Employee Account**. For detailed information of **Employee Account**, you can refer to [Employee Account](#).
9. **Company Device** authentication type is not used for Portal Authentication. There are often some devices without interactive interface in the enterprise, which cannot carry out portal authentication, but need to be connected to the wireless network, such as printers. These devices can access WLAN by entering password in personal mode or Mac authentication. You can add the MAC address of **Company Devices** in page **Authentication -> Setting -> Company Device**. For detail information of Company Device, you can refer to [Company Device](#).
10. Click **Edit Page** button to open Portal Page edit view. For detailed information of Captive Portal, you can refer to [Captive Portal](#).
11. At the **Default Access Role Profile**, select a Profile at the drop down menu. Or you can add a

new **Access Role Profile** by clicking the **Add** button next to it. For detail information of **Access Role Profile**, you can refer to [Access Role Profile](#).

10.8.3. Configure 802.1X Authentication in Customization

1. At the Site View, Click WLAN tab to view WLAN list.
2. Click "+" button to open Create WLAN page.
3. Fill the SSID.
4. Select "**Enterprise**" at Security Level drop down list.
5. Select Encryption Mode that you want. Click "[SSID Setting](#)" to see more information about **Encryption Mode**.
6. Set the Authentication Configuration to **Customization**, which means you should create Access Policy, Authentication Strategy and Employee Access Strategy by yourself.
7. Set the **Mac Auth** at "OFF" status.
8. You need click "**Effect Now**" to save WLAN and re-enter this page by edit it before continues. Otherwise you cannot select SSID in the next step.
9. Click **Configuration Wizard** button, the wizard will be shown at the right side. Based on the information in **Figure 10-3**, we need to create an **Access Policy**, an **Authentication Strategy** respectively. In this wizard, we will create these profiles in turn. Because of the reference relationship of the profile, you need to create an **Authentication Strategy** before saving the **Access Policy**. In this way, we recursively complete the creation of these profiles. Another operation way is to create an **Authentication Strategy** at **Authentication -> Authentication -> Authentication Strategy** page firstly. Then, create an **Access Policy** rule in **Authentication -> Authentication -> Access Policy** page to bind the **SSID** and **Authentication Type** to the previously created **Authentication Strategy**.
10. First, you will see the **Create Access Policy** tab, you should set a **Name** for it. For current 802.1X Authentication, you should better set the mapping conditions of **SSID** and **Authentication Type**. Select **SSID** in Mapping Condition's **Attribute** drop down list, and select the **SSID**, that you just created, at the **Value** drop down list, and then click **Add** button to add the condition. And then select Authentication Type in Mapping Condition's Attribute drop down list, and select **802.1X**. And Then you should select an **Authentication Strategy** or click **Add** button to add a new one. For detailed information of **Access Policy**, you can refer to [Access Policy](#).

11. Second, if you click the **Add** button to add a new **Authentication Strategy**, you will see the **Create Authentication Strategy** tab. You should set a **Name** for it. If you select **None** as the Authentication Source, it means that this **Authentication Strategy** is used for Mac authentication, and you should select a **Guest / Employee Access Strategy** for it. This is no use to our current use case.
 - a) If you select **Local Database** as the **Authentication Source**, you can add Employee Accounts at **Authentication -> Employee Access -> Employee Account**. You can see that **Web Authentication** can only be set as **None**, which means that this **Authentication Strategy** will be used for 802.1x authentication.
 - b) If you select **External LDAP / AD** as the Authentication Source, you can see that **Web Authentication** can only be set as **None**, which means that this Authentication Strategy will be used for 802.1x authentication. You should Configure LDAP/AD at the page **Authentication -> Setting -> LDAP / AD Configuration** page.
 - c) If you select **External Radius** as the Authentication Source, you should select one External Radius or click **Add** button to add a new External Radius. You should select Web Authentication as **None**, means you can use this **Authentication Strategy** for 802.1X authentication.

For detailed information of **Authentication Strategy**, you can refer to [Authentication Strategy](#).

12. Third, you can set parameters related to **Network Enforcement Policy**. If you set the **Default Access Role Profile**, it means that the terminal device authenticated through the **Authentication Strategy** will use this **Access Role** to authorize the terminal, instead of using **Default Access Role Profile** on WLAN. It is the same for the **Default Policy List**. If you turn on the **Session Timeout Status**, it means that the terminal that has passed the **Authentication Strategy** will automatically go offline after the **Session Timeout Interval**. If you turn on the **Account External Radius** switch, it means that when using External Radius, the Radius Accounting Interim package will be sent at the interval of **Accounting Interim Interval**.

10.8.4. Configure Web Portal Authentication

1. At the Site View, Click WLAN tab to view WLAN list.
2. Click "+" button to open Create WLAN page.
3. Fill the SSID.

4. Select **Open** at Security Level drop down list.
5. Set the **Mac Auth** at **ON** status.
6. Select **Customization** at the Authentication Configuration, which means you should create **Access Policy, Authentication Strategy** and **Employee Access Strategy** by yourself.
7. You need click **Effect Now** to save WLAN and re-enter this page by edit this WLAN before continue. Otherwise you cannot select SSID in the next step.
8. Click **Configuration Wizard** button, the wizard will be shown at the right side. Based on the information in **Figure 10-7**, we need to create an **Access Policy**, an **Authentication Strategy** and an **Employee Access Strategy** respectively. In this wizard, we will create these profiles in turn. Because of the reference relationship of the profile, you need to create an **Authentication Strategy** before saving the **Access Policy**; And you need to create an **Employee Access Strategy** before saving the **Authentication Strategy**. In this way, we recursively complete the creation of these profiles. Another operation way is to create an **Employee Access Strategy** in **Authentication -> Employee Access -> Employee Access Strategy** page firstly, and then create an **Authentication Strategy** at **Authentication -> Authentication -> Authentication Strategy** page and bind the previously created **Employee Access Strategy**. Finally, create an **Access Policy** rule in **Authentication -> Authentication -> Access Policy** page to bind the **SSID** and **Authentication Type** to the previously created **Authentication Strategy**.
13. First, you will see the **Create Access Policy** tab, you should set a **Name** for it. For current Web Portal Authentication, you should better set the mapping conditions of **SSID** and **Authentication Type**. Select **SSID** in Mapping Condition's **Attribute** drop down list, and select the **SSID**, that you just created, at the **Value** drop down list, and then click **Add** button to add the condition. And then select **Authentication Type** in Mapping Condition's **Attribute** drop down list, and select **MAC**. And Then you should select an **Authentication Strategy** or click **Add** button to add a new one. For detailed information of **Access Policy**, you can refer to [Access Policy](#).
9. Second, if you click the **Add** button to add a new **Authentication Strategy**, you will see the **Create Authentication Strategy** tab. You should set a **Name** for it. Select **None** as the **Authentication Source**, it means that this **Authentication Strategy** is used for Mac authentication, and you should select a **Guest/Employee Access Strategy** or add a new one for it. Before you select **Access Strategy**, you should check which you will use, **Guest** or **Employee**. For detailed information of **Authentication Strategy**, you can refer to [Authentication Strategy](#).
10. Third, if you select to create Guest Access Strategy, you can see that you can only use **Local**

Database as the Authentication Source. Please click [Guest Access Strategy](#) to get more information. Then you can set the **Fixed Access Role Profile**, which will be assigned to the terminal after Web Portal Authentication. The Fixed **Access Role Profile** option is not required. If you do not set this option, the terminal will use the **Default Access Role Profile** in **Authentication Strategy**. If the **Default Access Role Profile** is not set in the **Authentication Strategy**, the terminal will use the **Default Access Role Profile** set in WLAN, which must be set. If you select to create **Employee Access Strategy**, you can see that you can select **Local Database** or **External LDAP/AD** or **External Radius**.

11. Forth, you can set parameters related to **Network Enforcement Policy**. If you set the **Default Access Role Profile**, it means that the terminal device authenticated through the **Authentication Strategy** will use this **Access Role** to authorize the terminal, instead of using **Default Access Role Profile** on WLAN. It is the same for the Default Policy List. If you turn on the **Session Timeout Status**, it means that the terminal that has passed the **Authentication Strategy** will automatically offline after the **Session Timeout Interval**. If you turn on the **Account External Radius** button, it means that when using External Radius, the Radius accounting interval package will be sent at the interval of **Accounting Interim Interval**.

11. RF

The RF Management enable the user to ensure that transmit power and operating frequencies meet the requirements of global regulatory agencies and individual countries. A user can also use the profiles to adjust the wireless parameters and functions according to real network environment to improve the user experience of wireless network. You can manage RF configure for Site or a certain DAP.

This chapter contains the following topics:

- [RF Overview](#)
- [Set RF configurations of Site](#)
- [Set RF configurations of a selected DAP](#)

11.1. RF Overview

The options in RF configuration can be configured as auto, and DAP will automatically set its own relevant parameters according to the surrounding signal conditions.

Here are two charts showing the distribution of equipment channels, namely. You can place the mouse over the corresponding chart to obtain the AP number of each channel and bandwidth

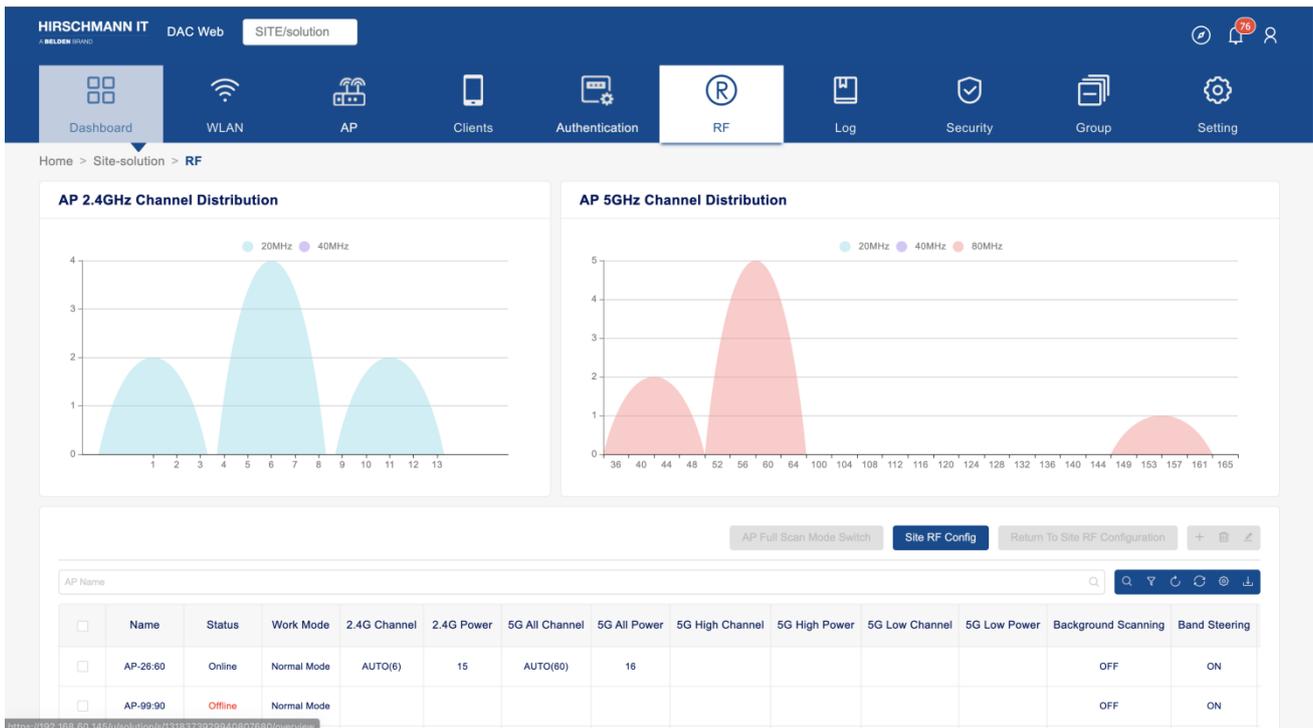


Figure 11-1-1

Below these charts is a list of detailed RF information for each AP. You can search based on AP name or use the drop menu to filter the display by AP status or AP mode.

- **Name** - AP Name
- **Location** - Location of AP
- **Status** - AP Status Online/Offline
- **Work Mode** -
 - **Normal Mode** - AP serving wireless clients
 - **Full Scan Mode** - At this mode, all radios under the AP will not broadcast SSID.
- **2.4G Channel** - Channel of 2.4G Band. If the configuration is Auto, the actual 2.4G channel of the AP will be shown.
- **2.4G Power** - Power of 2.4G Band. If the configuration is Auto, the actual 2.4G power of the AP will be shown.
- **5G All Channel** - Channel of 5G Band. If the configuration is Auto, the actual 5G channel of the AP will be shown. The optional channels vary according to the local laws of different countries or regions.

- **5G All Power** - Power of 5G All Channel Band. If the configuration is Auto, the actual 5G power of the AP will be shown.
- **5G High Channel** - Channel of 5G High. If the configuration is Auto, the actual 5G High channel of the AP will be shown.
- **5G High Power** - Power of 5G High Channel. If the configuration is Auto, the actual 5G High power of the AP will be shown.
- **5G Low Channel** - Channel of 5G Low. If the configuration is Auto, the actual 5G Low channel of the AP will be shown.
- **5G Low Power** - Power of 5G Low Channel. If the configuration is Auto, the actual 5G Low power of the AP will be shown.
- **Background Scanning** - Enables/Disables Background Scanning. Background Scanning is used to examine the radio frequency environment in which the wireless network is operating, discover neighbor APs, and identify interference and attacks. Background scanning is the basis of some advanced features such as: WIDS, WIPS etc. If want these advanced functions to be utilized, make sure it is enabled. By default, background scanning is enabled.
- **Band Steering** - Band Steering Status. Band Steering controls the behavior of dual band clients according to the utilization of a wireless channel and users connected to the AP, and guides a client accessing the network to the optimal 5GHz band or another AP.
- **Dynamic Load Balance** - Enables/disables client load balancing among APs in a group or groups in the same wireless network. The client information such as client number is synchronized in the wireless network so that an AP can know the load of its neighbor AP and decide whether or not to permit client access.

11.2. Set RF configurations of Site

Click **Site RF Config** button to enter RF edit view

11.2.1. General Information

- **Name** - Inherit from site name
- **Country/Region** - Select a Country/Region. A Country/Region is a short alphabetic or numeric geographical code that represent a country or dependent area and is used data processing and

communications. The wireless transmitting power and operating frequencies (channels) vary by country/region. Select the country/region where the APs are located.

11.2.2. Background Scanning

Background Scanning is used to examine the radio frequency environment in which the wireless network is operating, discover neighbor APs, and identify interference and attacks. Background scanning is the basis of some advanced features such as: MIPS, RDA (ACS/APC) etc. If want these advanced functions to be utilized, make sure it is enabled. By default, background scanning is enabled.

- **Background Scanning** - Enables/Disables Background Scanning.
- **Scanning Channel** -
 - **Working Channel** - AP just scan it working channel
 - **All Channel** - AP scan all channel
- **Scanning Interval** - The Background Scanning interval, in seconds.
- **Scanning Duration** - The Background Scanning duration in milliseconds. (Default = 50)

11.2.3. Smart Load Balance

Smart Load Balance (SLB) is a feature improves the user experience when accessing wireless connectivity by guiding a user's client device to connect to a free wireless channel or AP and denying access to APs with weak signal. Smart Load Balance includes:

- **Band Steering** - Enables/Disables Band Steering. Band Steering controls the behavior of dual band clients according to the utilization of a wireless channel and users connected to the AP, and guides a client accessing the network to the optimal AP.
- **Dynamic Load Balance** - Enables/disables client load balancing among APs in a group or groups in the same wireless network. The client information such as client number is synchronized in the wireless network so that an AP can know the load of its neighbor AP and decide whether or not to permit client access.
- **RSSI Threshold** - Associate RSSI Threshold. Used to set thresholds to optimize connectivity when associating with an AP by forbidding client access to networks with a weak wireless signal (RSSI). Clients with an RSSI value lower that the Association RSSI Threshold will not be allowed

to connect to the AP. By default, RSSI threshold is disabled (0). RSSI threshold can be applied to 2.4G band or 5G band separately. Recommend 2.4G (5), 5G (10). RSSI Threshold is recommended to be deployed in high density scenario.

- **Roaming RSSI** - Roaming RSSI Threshold. Used to set thresholds to optimize connectivity when roaming by forbidding client access to networks with a weak wireless signal (RSSI). Clients with an RSSI value lower than the Roaming RSSI Threshold value will be guided to roam to another AP with a better transmission signal. By default, Roaming RSSI is disabled (0). Roaming RSSI can be applied to 2.4G band or 5G band separately. Roaming RSSI is used in conjunction with 802.11k and 802.11v. Clients that support these protocols will be informed on which AP to roam to when the threshold is breached. When 802.11k and 802.11v is enabled. Recommend 2.4G (10), 5G (15).
- **Voice and Video Awareness** - Enables/Disables Voice and Video Awareness. Background scanning must be aware of existing traffic on APs. If there is an ongoing voice/video service, scanning should not be performed to ensure uninterrupted traffic; and scanning should resume there is no active voice/video session.
- **Neighbor AP Count** - Used to limit the number of neighbor APs that an AP can connect to.

11.2.4. Per Band Info

Configures the wireless setting for each radio band on an AP, such as working channel, transmit power, and short guard interval of the radio.

- **Allowed Band** - Configure the working radio for the AP.
 - **2.4G** - 2.4G band radio will be activated.
 - **5G All** - 5G band radio will be activated. Only for dual-radio devices.
 - **5G High** - 5.2G band radio will be activated. Only for three-radio devices.
 - **5G Low** - 5.8G band radio will be activated. Only for three-radio devices.
- **Channel Setting** - Configure the working channel of the radio.
 - Auto - Dynamically assigns the 2.4G working channel by ACS (Auto Channel Selection).
 - Manually specify the channel (allowed channels vary by country/region).
- **Channel Width** - Configures the channel width for 2.4 and 5G radio. Channel width is used to control how broad the signal is for transferring data. By increasing the channel width, you can

increase the speed and throughput of a wireless broadcast. However, larger channel width brings more unstable transmission in crowded areas with a lot of frequency noise and interference. The 2.4G channel width support is different from 5G.

- **2.4G** - 20MHz/40MHz
- **5G** - 20MHz/40MHz/80MHz/160MHz. Note that some high-frequency channels (e.g., 165) do not support 40MHz/80MHz/160MHz. If an AP is using these channels, a Channel Width of 40MHz/80MHz/160MHz will not be available. For example, 160MHz is only supported on channel settings 36 through 128.
- **5G High** - 20MHz/40MHz/80MHz/160MHz. Note that some high-frequency channels (e.g., 165) do not support 40MHz/80MHz/160MHz. If an AP is using these channels, a Channel Width of 40MHz/80MHz will not be available.)
- **5G Low** - 20MHz/40MHz/80MHz/160MHz.
- **Channel DRM** - Specify the channel scope for DRM. In some regions, specific unwanted channels can be scoped out automatic channel selection to avoid conflicts or law violation. Not supported on 2.4G Band.
- **Channel List** - Specify the available channel(s) that can be selected by DRM. Not supported on 2.4G Band.
- **Power Setting** - Configures the transmit power of the wireless radio. Power range varies from different radios.
 - **2.4G** - Configure the power setting for 2.4G radio.
 - **Auto** - Dynamically assigned the 2.4G transmit power by APC (Auto Power Control) Manually specify the power setting (3dBm - 20dBm)
 - **5G** - Configure the power setting for 5G radio.
 - **Auto** - Dynamically assigned the 5G transmit power by APC (Auto Power Control) Manually specify the power setting (3dBm - 23dBm)
- **Power DRM** - Specify the power range for DRM. If enable, you can select the Minimum TX Power and Maximum TX Power.
- **Minimum TX Power** - Specify the minimum transmit power for Power DRM setting. This can prevent the AP from selecting a low transmit power resulting in poor quality transmission.
- **Maximum TX Power** - Specify the maximum transmit power for Power DRM setting.

- **Short GI** - Enables/Disables Short Guard Interval. In IEEE 802.11 OFDM based communications, Guard Interval is used to ensure that distinct transmissions occur between the successive data symbols transmitted by a device. The standard symbol Guard Interval used in 802.11 OFDM is 800 nanoseconds in duration. To increase data rates, the 802.11n standard added optional support for a 400 nanoseconds guard interval (Short Guard Interval). This would provide approximately an 11% increase in data rates. However, using the Short Guard Interval will result in higher packet error rates when the delay spread of the RF channel exceeds the Short Guard Interval, or if timing synchronization between the transmitter and receiver is not precise. By Default, Short Guard Interval is disabled on the wireless radio.
- **802.11ax Radio** - Enables/Disables 802.11ax(Wi-Fi6) features. If disabled, the AP can work on 802.11ac or earlier protocols.

11.3. Set RF configurations for a selected DAP

Sometimes, we need to adjust the RF configurations of a selected AP to let users to get a better experience. Before set RF configurations for a certain AP, you must set the RF configurations of the corresponding site first. The RF configurations of AP have a higher priority over the RF Configurations of Site.

11.3.1. Single AP RF Configuration

Select a single AP, click "detail" to enter the AP details page, and then click **Config** button to set the RF configuration of the selected AP.

11.3.2. Fallback to Site RF Configuration

Selecting a single / multiple APs, click the "**Fallback to Site RF Configuration**" button, the RF configuration of these APs will be cleared, and the RF configuration of the selected APs will be consistent with the Site.

11.3.3. AP Full Scan Mode

After selecting single / multiple APS, click "**AP Full Scan Mode Switch**" button, and the selected AP will enter "full scan mode". At this mode, all radios under the AP will not broadcast SSID.



Note

Enable AP Full Scan Mode will cause the AP to close the currently working WLAN, and all terminals associated with the AP will be offline.

12. Log

Log contains two major parts: System log and Device log. The system log contains the key events of the device and the operation log of the DAC.

is log files collected from DAP. DAC provides good operation and maintenance management functions, but in some extreme cases, we need to obtain detailed logs on the device to facilitate R & D to locate problems in time.

This chapter contains the following topics:

- [System Log](#)
- [Device Log](#)

12.1. System Log

System log displays a list of current logs. You can search special message from this list.

12.1.1. Log List

The list show recently logs. You can filter logs by log type or log level or AP group.

- **Severity** - severity of log. It can be one of emergency, alert, critical, error, warning, notice, informational.
- **Type** - log type. It can be one of AP hardware, AP upgrade, wireless security, AP network, wireless authentication, operation.
- **Scene** - The log occurs at which corporate/site/group.
- **Date & Time** - The log occurs at this time.
- **Detail** - The detail information of this log.
- **AP Name** - If this log is produced by an AP, this filed will show the Name of this AP.
- **AP Location** - If this log is produced by an AP, this filed will show the Location of this AP.

12.1.2. Log Types

- **AP Hardware** - Hardware reporting information; It mainly focuses on the CPU, ram and flash performance of AP; Monitor the hot and cold start behavior of AP;
- **AP Upgrade** - Firmware upgrade information, mainly including AP upgrade behavior;
- **Wireless Security** - Wireless security information, mainly the operation information of Blocklist;
- **AP Network** - Network related reporting information, mainly the creation and deletion of layer-2 VLAN;
- **Wireless Authentication** - Authentication information, including the authentication behavior of the client and the link status information from the AP to the radius server
- **Operate** - User operation record information for DAC; Record the operation of DAC with the combination of operator and operation action;

12.1.3. Severity

- **Emergency** - System is unusable
- **Alert** - Action must be taken immediately
- **Critical** - Critical condition
- **Error** - Error condition
- **Warning** - May indicate that an error will occur if action is not taken
- **Notice** - Events that are unusual, but not error conditions
- **Informational** - Normal operational messages that require no action

12.1.4. Config of AP event log

Click **Config** button to show the config page. The current page contains the log switch or related parameters of device events. You can open the device event log which you are concerned in this page.

AP Hardware Performance

- **Cold Boot** - Cold boot is the process of starting a AP from shutdown or a powerless state and setting it to normal working condition. It is also known as hard boot, cold start or dead start.

- **Warm Boot** - A warm boot (also called a "soft boot") is the process of restarting a AP. It may be used in contrast to a cold boot.
- **CPU Overrun** - This log occurs when the AP CPU load exceeds CPU threshold.
- **CPU Threshold** - When AP CPU usage exceeds this percent, AP CPU Overrun log will occur.
- **Memory Overrun** - It occurs when the AP RAM memory usage exceeds MEM threshold.
- **Memory Threshold** - When AP memory usage exceeds this percent, AP MEM Overrun log will occur.
- **AP Flash Overrun** - It occurs when the AP Flash memory usage exceeds Flash threshold.
- **Flash threshold** - When AP Flash memory usage exceeds this percent, AP Flash overrun log will occur.
- **AP CPU Overrun Clear** - When the CPU utilization of the AP decreases from exceeding the threshold to the normal state.
- **AP MEM Overrun Clear** - When the RAM memory utilization of the AP decreases from exceeding the threshold to the normal state.
- **AP Flash Overrun Clear** - When the Flush memory utilization of the AP decreases from exceeding the threshold to the normal state.

AP Upgrade

- **AP Upgrade** - Logs of AP Upgrade

Wireless Security

- **AP Add Client to Blocklist** - Log of a client is added to blocklist by the WIPS policy dynamically or manually.

AP Network

- **AP VLAN Creation** - AP VLAN creation log
- **AP VLAN Deletion** - AP VLAN deletion log

Wireless Authentication

- **AP Client Authentication Successful** - Log of client authenticate successful.

- **AP Client Authentication Failed** - Log of client authenticate failed.
- **AP Radius Auth Server No Connection** - Log of authentication server unreachable
- **AP Radius Auth Server No Connection Clear** - Log of authentication server recover to reachable
- **AP Radius Acct Server No Connection** - Log of accounting server unreachable
- **AP Radius Acct Server No Connection Clear** - Log of accounting server recover to reachable

12.2. Device Log

After the AP restarts abnormally, it reconnects to the DAC platform, and the platform will collect the log files of the AP. In the Device Log view, you can see the list of logs that have been collected.

- **File Name** - File Name
- **AP MAC** - AP MAC of this log file.
- **AP Name** - AP Name of this log file.
- **AP IP** - AP IP Address
- **Status** - Success/failed. The file upload status.
- **Log Generation Time** - This file is generated at this time.
- **File Size** - File size of this log File

Select a log file, click **File Download** button to download this file.

13. Security

An 802.11 network is open and borderless, making it vulnerable to attack (e.g., Rogue APs, unauthorized clients, DoS attacks). The Wireless Intrusion Protection System (WIPS) application monitors the wireless radio spectrum for the presence of unsafe access points and clients and can take countermeasures to mitigate the impact of foreign intrusions. WIPS provides an overview of wireless network threats/intrusions for DAPs, and enables users to set up policies to detect threats and take countermeasures.

WIDS:

DAC provides comprehensive security function to ensure customer wireless cyber security. The system identifies rogue APs by means of following policy and criteria.

- To detect when APs' signal strength threshold exceeds the value defined by administrator;
- To detect if APs' SSID name is valid according to system definition;
- To detect by defined key words (defined by administrator) within SSID name of APs;
- To detect by defined OUI (Organizational Unique Identifier within first six digits of MAC address) of APs, refer to Blacklist mechanism;
- To detect by defined legal OUI, refer to Whitelist mechanism; DAC is also able to detect following cyber-attack behaviors from potential rogue APs or clients:
- APs: AP Spoofing, Broadcast de-authentication, Broadcast disassociation, Ad-hoc network with SSID being used in current infrastructure, invalid long SSID, AP impersonation, Omerta attack, Null probe response, invalid address combination, invalid reason code of de-authentication, invalid reason code of dis-association;
- Clients: Valid Client mis-association, Omerta Attack, Unencrypted Valid Clients, 802.11 40MHz bandwidth intolerance setting, Active 802.11n Greenfield Mode, DHCP client ID, DHCP conflict, DHCP name change, Frequent authentication, long SSID (client), Malformed
- Frame-Assoc request, invalid reason code of de-authentication, invalid reason code of dis-association;

WISP:

In cooperate with WIDS, DAC provides WIPS to implement relevant security policies:

- Security policy to suppress rogue APs to mitigate destructive impacts, by preventing clients from connecting to rogue APs;
- Security policy to suppress rogue clients (active/passive) to mitigate negative effects, by means of blacklist mechanism (static or dynamic);
- Security policy to protect legal equipment by providing whitelist mechanism.

The home page provides two charts to facilitate you to understand the current overall situation.

- **Rogue Client/AP** - Line chart of Rogue client / AP quantity.
- **Blocklist** - Line chart of blocklist quantity.

This chapter contains the following topics:

- [Security Config](#)
- [AP Record](#)
- [Client Record](#)
- [Blocklist](#)
- [Attack Ranking](#)

13.1. Security Config

The Security Config Screen is used to configure policies for Rogue AP and wireless attacks on the network. When an attack is detected based on the policy, the detected device is banned from the network and is displayed on the Rogue AP Record or Rogue Client Record for review. Click **Config** button, edit policy as described below, click on the **Save** button to activate the policy for the site wireless network.

13.1.1. Rogue AP Policy

A Rogue AP is an unauthorized AP connected to the wired side of the network, that is considered a security threat to the wireless network. An interfering AP is an AP seen in the wireless environment but not connected to the wired network, which is not considered a direct security threat. However, some interfering APs may have an impact on network quality and can interfere with valid client access

to the network. Complete the fields below to configure rules to classify interfering APs as Rogue APs.

- **Signal Strength Threshold** - If enabled, an interfering AP with greater RSSI than the setting value will be classified as Rogue (Range = 50 - 95). By default, the RSSI matching rule is disabled.
- **Detect Valid SSID** - If enabled, a other AP broadcasting the same SSID with valid DAC network SSIDs will be classified as Rogue. By default, the Detected Valid SSID rule is enabled.
- **Detect Rogue SSID Keyword** - If enabled, an interfering AP broadcasting and SSID that matches the characteristic specified by the user will be classified as Rogue. The matching condition can be equal to or contain the configured keyword.
- **Rogue OUI** - If enabled, interfering APs matching this MAC OUI will be classified as Rogue.
- **Valid OUI** - An AP classified as interfering or Rogue can be trusted to be a "Valid" AP by entering the MAC OUI of the AP - essentially creating a Vendor "Whitelist". These interfering APs will never be classified as Rogue.
- **Rogue AP Containment** - If enabled, the Rogue AP containment function reduces the impact of the Rogue AP on valid clients.

13.1.2. Wireless Attack Detection Policy

A Rogue AP is not the only threat to the wireless network, other wireless attacks can be detected and mitigated for both APs and Clients. To create Wireless Attack Policies, you must enable **Wireless Detection**. When configuring a policy, each detection policy can be set to one of the following levels. When a level is selected, all detection policies included in that level are displayed and selected.

- **High** - Enables all applicable detection mechanisms, including all the options of low and medium level settings.
- **Medium** - Enables important detection mechanisms. This includes all the options of the low-level settings.
- **Low (Default)** - Enables only the most critical detection mechanisms.
- **Customization** - Enables only the selected detection mechanisms. When this level is selected, all detection mechanisms are displayed. Select the ones you want to include in the policy.

The sections below describe each of the Wireless Attack Policies.

AP Attack Detection Policy

An AP Attack Detection Policy detects multiple attacks originating from foreign APs. The following detection methods are available depending on the level selected.

- **Detect AP Spoofing** - An AP Spoofing attack involves an intruder sending forged frames that are made to look like they are from a valid AP.
- **Detect Broadcast De-authentication** - A de-authentication broadcast attempts to disconnect all clients in range. Rather than sending a spoofed de-authentication frame to a specific MAC address, this attack sends the frame to a broadcast address.
- **Detect Broadcast Disassociation** - By sending disassociation frames to the broadcast address (FF:FF:FF:FF:FF:FF), an intruder can disconnect all stations on a network for a widespread DoS.
- **Detect Adhoc Networks using VALID SSID** - If an unauthorized adhoc network is using the same SSID as an authorized network, a valid client may be tricked into connecting to the wrong network. If a client connects to a malicious adhoc network, security breaches or attacks can occur.
- **Detect Long SSID** - Detects long SSIDs with more than 32 characters in the name.
- **Detect AP Impersonation** - In AP impersonation attacks, an AP assumes the BSSID and ESSID of a valid AP. AP impersonation attacks can be done for man-in-the-middle attacks, a Rogue AP attempting to bypass detection, or a Honeypot attack.
- **Detect Adhoc Networks** - An ad hoc network is a collection of wireless clients that form a network among themselves without the use of an AP. If the ad hoc network does not use encryption, it may expose sensitive data to outside eavesdroppers. If a device is connected to a wired network and has bridging enabled, an ad-hoc network may also function like a Rogue AP. Additionally, ad-hoc networks can expose client devices to viruses and other security vulnerabilities.
- **Detect Wireless Bridge** - Wireless bridges are normally used to connect multiple buildings together. However, an intruder could place (or have an authorized person place) a wireless bridge inside the network that would extend the corporate network somewhere outside the building. Wireless bridges are somewhat different from Rogue APs in that they do not use beacons and have no concept of association. Most networks do not use bridges. In these networks, the presence of a bridge is a signal that a security problem exists.
- **Detect Null Probe Response** - A null probe response attack has the potential to crash or lock up the firmware of many 802.11 NICs. In this attack, a client probe-request frame will be answered by a probe response containing a null SSID. Many popular NIC cards will lock up upon receiving

such a probe response.

- **Detect Invalid Address Combination** - In this attack, an intruder can cause an AP to transmit de-authentication and disassociation frames to its clients. Triggers that can cause this condition include the use of broadcast or multicast MAC address in the source address field.
- **Detect Reason Code Invalid of De-authentication** - De-authentication packets with invalid reason code will be classified as an attack.
- **Detect Reason Code Invalid of Disassociation** - Disassociation packets with invalid reason code will be classified as an attack.

You can quickly select the corresponding level to complete the detection AP Attack Detection Policy

- **Low**
 - Detect AP Spoofing
 - Detect Broadcast De-authentication
 - Detect Broadcast Disassociation
- **Medium**
 - Detect AP Spoofing
 - Detect Broadcast De-authentication
 - Detect Broadcast Disassociation
 - Detect Adhoc Network Using Valid SSID
 - Detect Long SSID
- **High** - The flow items will all be used
 - Detect AP Spoofing
 - Detect Broadcast De-authentication
 - Detect Broadcast Disassociation
 - Detect Adhoc Network Using Valid SSID
 - Detect Long SSID
 - Detect AP Impersonation
 - Detect Omerta Attack
 - Detect Null Probe Response

- Detect Invalid Address Combination
- Detect Reason Code Invalid of De-authentication
- Detect Reason Code Invalid of Disassociation
- **Customization** - You can select the attack detection policies that you care about from flow.
 - Detect AP Spoofing
 - Detect Broadcast De-authentication
 - Detect Broadcast Disassociation
 - Detect Adhoc Network Using Valid SSID
 - Detect Long SSID
 - Detect AP Impersonation
 - Detect Omerta Attack
 - Detect Null Probe Response
 - Detect Invalid Address Combination
 - Detect Reason Code Invalid of De-authentication
 - Detect Reason Code Invalid of Disassociation

Client Attack Detection Policy

A Client Attack Detection Policy detects attacks originating from wireless clients. The following detection methods are available depending on the level selected.

- **Detect Valid Station Misassociation** - This feature does not detect attacks, but rather monitors valid wireless clients and their association within the network. Valid client misassociation is potentially dangerous to network security. The four types of misassociation monitored are:
 - **Valid Client Associated to a Rogue** - A valid client that is associated to a Rogue AP
 - **Valid Client Associated to an Interfering AP** - A valid client that is associated to an interfering AP
 - **Valid Client Associated to a Honeypot AP** - A honeypot is an AP that is not valid but is using an SSID that has been designated as valid
 - **Valid Client in Ad Hoc Connection Mode** - A valid client that has joined an ad hoc network

- **Detect Omerta Attack** - Omerta is an 802.11 DoS tool that sends disassociation frames to all clients on a channel in response to data frames. The Omerta attack is characterized by disassociation frames with a reason code of 0x01. This reason code is "unspecified" and is not be used under normal circumstances.
- **Detect Unencrypted Valid Client** - A valid client that is passing traffic in unencrypted mode is a security risk. An intruder can sniff unencrypted traffic (also known as packet capture) with software tools known as sniffers. These packets are then reassembled to produce the original message.
- **Detect 802.11 40MHZ Intolerance Setting** - When a client sets the HT capability "intolerant bit" to indicate that it is unable to participate in a 40MHz BSS, the AP must use lower data rates with all of its clients. Network administrators often want to know if there are devices that are advertising 40MHz intolerance, as this can impact the performance of the network.
- **Detect Active 802.11n Greenfield Mode** - When 802.11 devices use the HT operating mode, they can't share the same channel as 802.11a/b/g clients. Not only can they not communicate with legacy devices, the way they use the transmission medium is different, which would cause collisions, errors and retransmissions.
- **Detect DHCP Client ID** - A client which sends a DHCP DISCOVER packet containing a Client-ID tag (Tag 61) which doesn't match the source MAC of the packet may be doing a DHCP denial-of-service to exhaust the DHCP pool.
- **Detect DHCP Conflict** - Clients which receive a DHCP address and continue to use a different IP address may indicate a miss-configured or spoofed client.
- **Detect DHCP Name Change** - The DHCP configuration protocol allows clients to optionally put the hostname in the DHCP Discover packet. This value should only change if the client has changed drastically (such as a dual-boot system). Changing values can often indicate a client spoofing/MAC cloning attack.
- **Detect Frequent Certification** - Client which attempts to connect to DAP but fails to pass the authentication for too many times, indicating an attack client.
- **Detect Long SSID at Client** - Detect long SSID in the wireless environment based on packets sent by clients.
- **Detect Malformed Frame-Assoc Request** - Some wireless drivers used in access points do not correctly parse the SSID information element tag contained in association request frames. A malicious association request with a null SSID can trigger a DoS or potential code execution

condition on the targeted device.

- **Detect Reason Code Invalid of De-authentication** - De-authentication packets with invalid reason code will be classified as an attack.
- **Detect Reason Code Invalid of Disassociation** - Disassociation packets with invalid reason code will be classified as an attack.

You can quickly select the corresponding level to complete the Client Attack Detection Policy

- **Low**
 - Detect Valid Client Misassociation
 - Detect Too Many Auth Failure Client
- **Medium**
 - Detect Valid Client Misassociation
 - Detect Omerta Attack
 - Detect Unencrypted Valid Clients
 - Detect Too Many Auth Failure Client
 - Detect Long SSID At Client
 - Detect Malformed Frame-Assoc Request
- **High**
 - Detect Valid Client Misassociation
 - Detect Omerta Attack
 - Detect Unencrypted Valid Clients
 - Detect 802.11 40MHZ Intolerance Setting
 - Detect Active 802.11n Greenfield Mode
 - Detect DHCP Client ID
 - Detect DHCP Conflict
 - Detect DHCP Name Change
 - Detect Too Many Auth Failure Client
 - Detect Long SSID At Client

- Detect Malformed Frame-Assoc Request
- Detect Reason Code Invalid of De-authentication
- Detect Reason Code Invalid of Disassociation
- **Customization** - You can select the attack detection policies that you care about from flow.
 - Detect Valid Client Misassociation
 - Detect Omerta Attack
 - Detect Unencrypted Valid Clients
 - Detect 802.11 40MHZ Intolerance Setting
 - Detect Active 802.11n Greenfield Mode
 - Detect DHCP Client ID
 - Detect DHCP Conflict
 - Detect DHCP Name Change
 - Detect Too Many Auth Failure Client
 - Detect Long SSID At Client
 - Detect Malformed Frame-Assoc Request
 - Detect Reason Code Invalid of De-authentication
 - Detect Reason Code Invalid of Disassociation

Client Blocklist Policy

There are two sources for the Client Blocklist: created manually by user or added dynamically by system. If the Dynamic Client Blocklist is enabled, intruders discovered by WIPS are dynamically added into the Client Blocklist and prevented from associating with the network. The following detected items are added to the Client Blocklist by system: List of Client Attack Detection, ad hoc clients, Clients associated to Rogue AP.

- **Aging Time** - Aging time for the Client Blocklist. Once expired, a client will be removed from the blocklist and allowed to be associated to the valid network until it is detected as a threat again. (Range = 1 hour to 365 days, Default = 1 Day).
- **Max Auth Failure Times** - Authentication failure times threshold. When a client fails to pass the authentication in the associated phase for too many times in a brief period, it will be classified as

an attack and added into the Client Blocklist. (Range = 3 - 10 times per 5 - 3600 seconds, Default = 10 times per 60 seconds.

13.2. AP Record

The Security -> AP Screen list APs on the network including Interfering APs, Rogue APs, Valid APs.

- **AP MAC** - BSSID of the interfering/Rogue AP.
- **Encryption Type** - Encryption method of ESSID broadcast by the Rogue AP.
- **Collection Time** - The latest time that the Rogue AP was seen by the detecting AP
- **Device Network Type** - Encryption method of the SSID to which the Rogue client is associated.
- **Signal Strength** - RSSI of the Rogue AP.
- **WLAN Name** - SSID of Rogue AP broadcast.
- **Client Number** – Client count associated to the Rogue/interfering/Valid AP
- **Channel** - Working channel of the radio frequency on the Rogue AP.
- **Attack Item** - The Attack Detection Policy used (e.g., Detect Valid Station Misassociation)
- **Device Type**
 - Interfering AP
 - Rogue AP
 - Valid AP
- **Scanning AP** - MAC address of the valid AP that detected the Rogue AP.

13.3. Client Record

- **Client MAC** - MAC address of the interfering/Rogue client.
- **Scanning Client MAC** - Scanning Client MAC
- **Association AP MAC** - MAC address of the interfering/Rogue AP to which the client is associated.
- **Attack Item** - The Attack Detection Policy used (e.g., Detect Valid Station Misassociation)
- **Collection Time** - The latest time that the Rogue client was seen by the detecting AP.

- **Device Network Type** - Encryption method of the SSID to which the Rogue client is associated.
- **Signal Strength** - RSSI of the Rogue client
- **Client IP** - IP address of client.
- **Device Type**
 - Clients Associated to a Rogue AP
 - Clients Associated to an Interfering AP

13.4. Blocklist

Blocklist focus on the basic access control mechanism for users connecting to SSID based on the client level; those clients on the Blocklist are denied associating to the DAP, once a client is in the Blocklist, it cannot connect to any WLAN of any security level (Enterprise/Personal/Open). You can add/delete the Blocklist based on client's MAC address.

The Wireless Blocklist Page show information about all clients that have been blocked. It is also used to manually add clients to the blocklist.

- **Client MAC** - MAC address of the client in the Blocklist.
- **Start Time** - The starting time for the block. During the duration, the client is not allowed to access to the wireless network.
- **Expiry time** - The expiry time for the Blocklist. The client can access the wireless network after the expiry time.
- **Type** - The reason why the client was added to blocklist.
 - **manual** - Added into the Blocklist by the user.
 - **auto** - Dynamically added by the WIPS policy.
- **Status** - Indicates whether the Blocklist policy effective date has expired.

13.4.1. Adding a Client to The Blocklist

Click on the **+** icon to bring up the **Add to Blocklist** module window. Enter the client's MAC address, then click on the **Save** button. Repeat to add additional clients. You should set an Expire time for the client. That means the client can connect to SSID of this Site again after Expire time.

13.4.2. Deleting a Client from The Blocklist

Select the client(s) in the Blocklist and click on the Delete icon. Click **Yes** at the confirmation prompt.

13.5. Attack Ranking

Count the number of attacks respectively

- **Attack Item** - The Attack Detection Policy used (e.g., Detect Valid Station Misassociation)
- **Attack times** - Count of this attack item.

14. Captive Portal

Captive Portal authentication is mechanism by which user credentials are obtained through Web pages and authenticated through a RADIUS server. If the authentication is successful, the RADIUS server may return a role (policy list) that is applied to traffic from the user device. Captive Portal provides a secondary level of authentication that is used to apply a new role (QoS policy list) to the user. An external, guest Captive Portal authentication mechanism is provided through the employee feature.

This chapter contains the following topics:

- [Entry to Portal Page Editor](#)
- [Portal Editor View](#)
- [Select Template](#)
- [Page Selector](#)
- [Page View](#)
- [Component Attributes](#)

14.1. Entry to Portal Page Editor

Portal Page is binding to **Guest Access Strategy** or **Employee Access Strategy**. To use Portal authentication, you should set **MAC Auth** ON. When you select default Authentication Configuration, you can entry portal editor by click "**Edit page**" button.

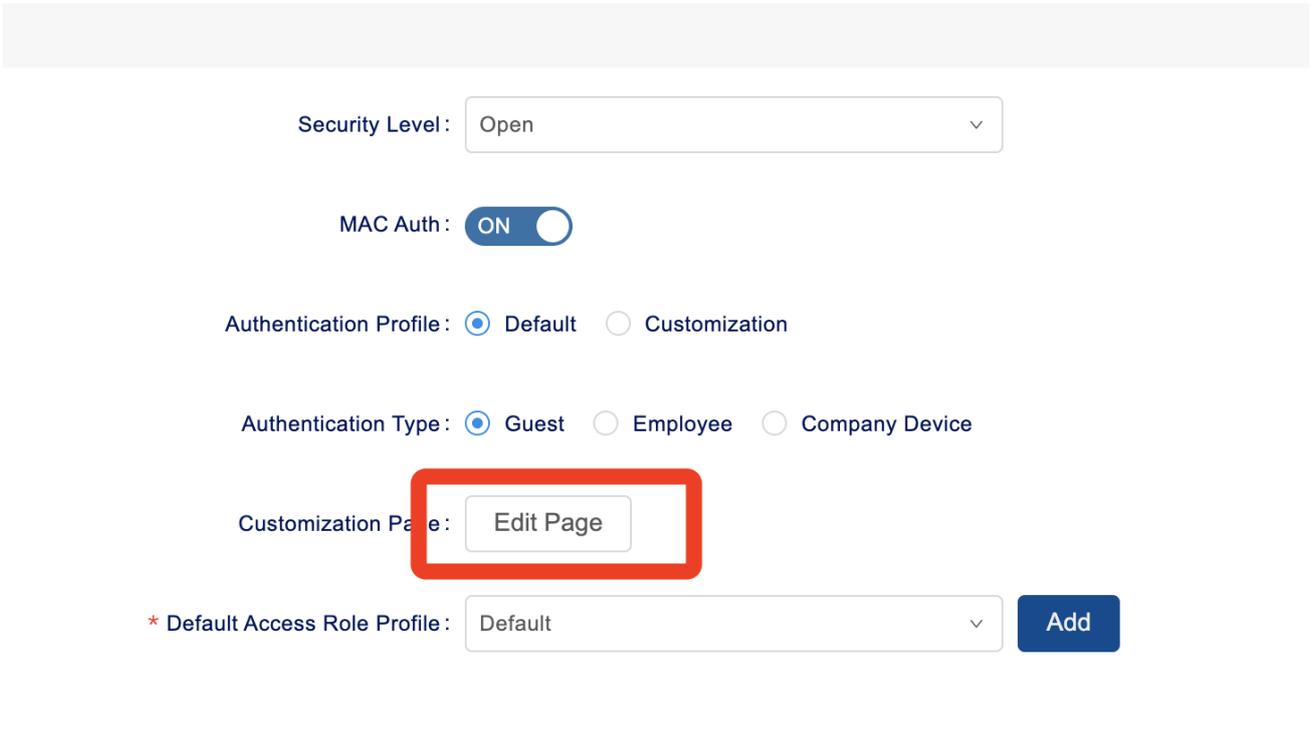


Figure 14-1-1

If you select Customization for Authentication Profile, you can find the entrance of Portal editor in the page of Guest Access Strategy (Authentication -> Guest Access -> Guest Access Strategy) or Employee Access Strategy (Authentication -> Employee Access -> Employee Access Strategy).

14.2. Portal Editor View

The layout of portal customized page is shown in the Figure 14-2-1. From left to right, it can be divided into the following functional blocks:

- **Page selector** - It usually includes three HTML page: index, success and fail. You can select one of them to edit.
- **Page view** - Dynamic display portal page that you select. When you edit the component attributes, it will update and display the modification results in real time here.
- **Page attributes view** - View and setting the attributes of HTML Component.

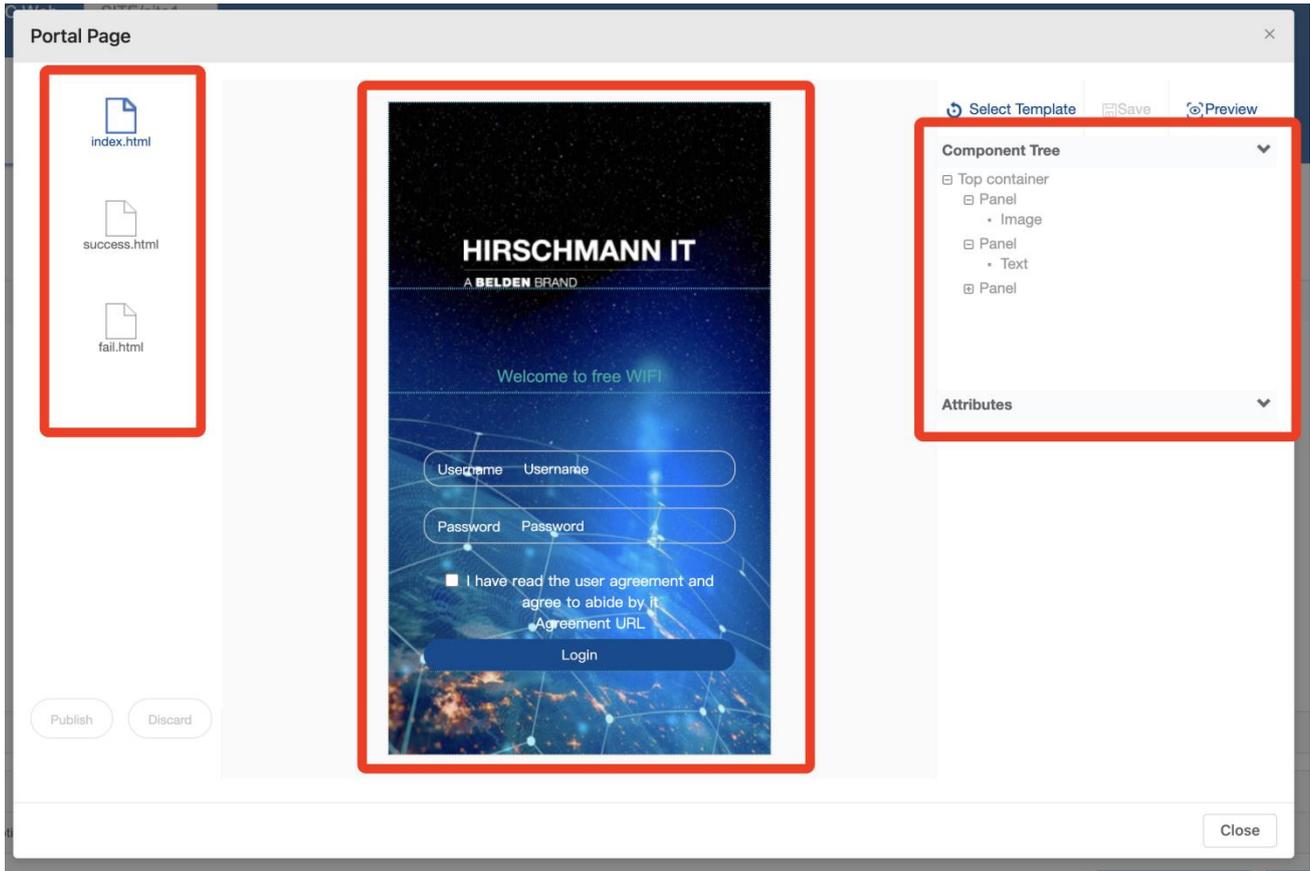


Figure 14-2-1

14.3. Select Template

Click the "**Select Template**" button which is at the top of page attributes view. On the Prompt Message window, click **confirm** button. There are three templates that you can select:

- **Login by Account** - From this Portal template, user can login with Account and Password. Account and Password can be added at Authentication Profile -> Guest Access -> Guest Account for Guest or Authentication Profile -> Employee Access -> Employee Account for Employee.
- **AccessCode** - This Portal just can be used for guest access. And Access Code can be added at Create Guest Account page, select Access Code as the Guest Type.
- **Scan QRCode by Employee** - This Portal is used for guest access. When the guest is associated with the WLAN using this template, he will get a portal page containing a QR code. Any employee can scan the QR code with his certified mobile phone to authorize the guest.
- **SMS Login** - From this Portal template, user can login with mobile number.

14.4. Page Selector

Each portal template usually contains three pages: index, success and failed. The index page contains the login form. When the user logs in successfully, he will see the success page. When the user fails to log in, he will see the failed page.

Click on the page, then you can edit it.

14.5. Page View

Each page contains several components. These components may be a picture, a piece of text, or a form. You can click the page element or select the corresponding component from the component tree and edit it. So as to change the display content and visual effect of page.

14.6. Component Attributes

Each component has several attributes, which can be modified to change the content displayed on the page.

14.6.1. Image Component

- **Image** - You can replace the current image by modifying the attribute.
- **Width** - Width of image.
- **Height** - Height of image. If the width and height are not the same scale of the original image, the image will stretch and deform.
- **Link Address** - Hyperlink, which will open when the user clicks on the component. If the current page is displayed before the user logs in, you need to ensure that the IP address of the hyperlink is in the allowed IP.

14.6.2. Text Component

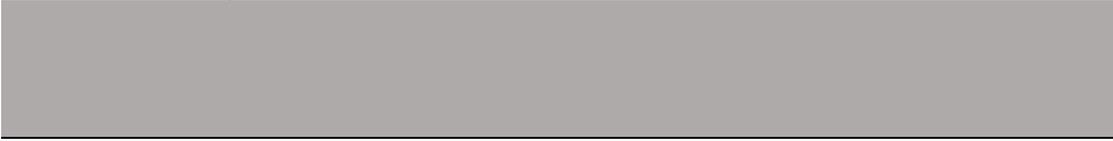
- **Font Family** - Font family of the text.
- **Font Size** - Font size of the text.

- **Content** - Content of the text component. You can customize personalized information here.
- **Link Address** - When click the text, open the URL. If the current page is not a successful page, you need to ensure that the IP address of this URL is in the allowed IP.
- **Color** - Font color of the text.
- **Action** - The action of click the text. It can be one of the values none, back or forward. If link address is configured, it should not work here.

14.6.3. Form Component

- **Login Success Redirect URL** - Redirect to the URL when login successful. This means that the success page in the template will not be used. You can set it as the home page of the enterprise or other promotion pages.
- **Login Failed Redirect URL** - When login fails, redirect to the URL. This means that the failed page in the template will not be used. You need to make sure that there is a prompt of "login failure" on this page. Because the user does not have access to the network, you need to ensure that the IP where the URL is located is in the allowed IP.
- **"User Protocol Link" whether or not show** - Show or Hide the User Protocol Link text.
- **"User Protocol Link" Font Color** - Font Color of the User Protocol Link text.
- **"User Protocol Link" whether to add Underline** - Show or Hide underline on the User Protocol Link text.
- **Agreement Detail** - User Protocol Agreement Detail information.
- **Button Text** - Text content on the button.
- **Button Font Color** - Color of the text on the button.
- **Button Background Color** - Color of the Button.
- **Material Width** - Only appears in scan QR-Code by employee template. The width of QR-Code can be the number of pixels or percent

15. Glossary

	
ACL	Access Control List
ACS	Automatic Channel Selection
APC	Automatic Power Control
ARP	Address Resolution Protocol
BLE	Bluetooth Low Energy
BSSID	Basic Service Set Identifier
CLI	Command-Line Interface
DAC	Dragonfly Access Controller
DAP	Dragonfly Access Point
DCM	Dynamic Client Management

DNS	Domain Name System
DRM	Dynamic Radio Management: automatically manage DAP working channel and transmitting power
DHCP	Dynamic Host Configuration Protocol
DSCP	Differentiated Services Code Point
ESSID	Extended Service Set Identifier
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
IDS	Intrusion Detection System
IG	Installation Guide
IGMP	Internet Group Management Protocol
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control

MIMO Multiple-Input Multiple-Output

MQTT Message Queuing Telemetry Transport.

MTU Maximum Transmission Unit

MU-MIMO Multi-User Multiple-Input Multiple-Out

NAT Network Address Translation

NTP Network Time Protocol

OKC Opportunistic Key Caching

OUI Organizationally unique identifier

PMD Post Mortem Dump

PMF Protected Management Frames

POE Power over Ethernet

PPPOE Point-to-Point Protocol over Ethernet

PVM	Primary Virtual Manager: the virtual manager selected from DAPs according to the defined priority will be responsible for an internal portal server, AP and client management and monitoring
------------	--

QoS	Quality of Service
------------	--------------------

QSG	Quick Start Guide
------------	-------------------

RF	Radio Frequency
-----------	-----------------

RSSI	Received Signal Strength Indicator
-------------	------------------------------------

SNMP	Simple Network Management Protocol
-------------	------------------------------------

SSID	Service Set Identifier
-------------	------------------------

SVM	Secondary Virtual Manager: the second highest priority in the cluster. When the PVM fails to respond due to an unexpected error or issues, the SVM will automatically upgrade to act as the PVM
------------	---

TCP	Transmission Control Protocol
------------	-------------------------------

TLS	Transport Layer Security
------------	--------------------------

UDP	User Datagram Protocol
------------	------------------------

VLAN Virtual Local Area Network

WBM Web Based Management

WIDS Wireless Intrusion Detection System

WIPS Wireless Intrusion Prevention System

WLAN Wireless Local Area Network

WMM Wi-Fi Multimedia (WMM)

WPA Wi-Fi Protected Access

WPA2 Wi-Fi Protected Access 2

WPA3 Wi-Fi Protected Access 3