HIRSCHMANN IT

A BELDEN BRAND

User Manual

Configuration

Dragonfly Access Controller

Revision history

Revision	Date	Description
2.5	Aug-2023	Added function: SNMP and Antenna Configuration

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 to anyone.

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 manual.

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

You may get the latest version of this manual on the Internet at:

https://catalog.belden.com

Contents

Safety instructions

Safety location

The device must be placed in a certain location that is safe, stable, and reliable. The physical operators must be authorized. The operation CLI scripts should be properly kept, updated, and reviewed.

Safety channel

Hirschmann IT devices support multiple management methods, including SSH, HTTP, and HTTPS. All un-encrypted management protocols are not recommended. Hirschmann IT recommends using SSH and HTTPs to operate the devices to help ensure management traffic is encrypted.

Safety storage

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

About this manual

The “Configuration” user manual contains the information you need to start operating the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

The “Configuration” user manual is applicable to DAC 1.1.5.6005 and later versions.

About DAC

DAC is a simple, easy to deploy turnkey WLAN controlling software to manage one or more DAPs. Routable connectivity to the DAC and a self-enclosed network can be 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, then 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.

Key

The symbols used in this manual have the following meanings:

▶	List
□	Work step
■	Subheading
Link	Cross-reference with link
Note:	A note emphasizes a significant fact or draws your attention to a dependency.

1 DAC setup

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

This chapter contains the following topics:

- ▶ System requirements
- ▶ DAC installation
- ▶ DAC upgrade
- ▶ Register DAP to DAC

1.1 System requirements

DAC runs in a VM. The required resources are as follows:

AP/Clients	Configurations	HDD
50 APs + 1000 Clients	4 Cores CPU+16 GB Memory+1 TB HDD	Read: 1.7 Gbit/s Write: 134 Mbit/s
256 APs + 5000 Clients	8 Cores CPU+16 GB Memory+1 TB HDD	
500 APs + 10000 Clients	12 Cores CPU+32 GB Memory+1 TB HDD	
1000 APs + 20000 Clients	24 Cores CPU+32 GB Memory+1 TB HDD	

Table 1: Configuration requirements

For detailed system requirements, refer to Section 2.1 “Installation on the Virtual Machine” in **DAC Installation Guide**.

1.2 DAC installation

Refer to the **DAC Installation Guide** for a detailed installation process. After installation, you can log in to DAC. The default account name is **admin**, and the password is **Admin@01**. During the first login, Hirschmann IT recommends changing the default password for security concerns.

1.3 DAC upgrade

Refer to Section 4 “Installation” of the **DAC Installation Guide** for a detailed upgrade process.

1.4 Register DAP to DAC

When the DAP is connected to the wired network, it needs to register with the DAC to be managed by the DAC. There are 2 ways to register DAPs with DAC.

1.4.1 Discover DAC by DHCP options

If the AP receives Option 43, Sub-Option 1 from the DHCP server, then the AP boots up and connects 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-Option 1	Length of IP address, 0C = 12	1	9	2	.	1	6	8	.	2	2	.	1

Table 2: DHCP server configuration

1.4.2 Configuring DAC IP address from DAP website

At the DAP setup wizard, you can select the management mode of DAP: Cluster or DAC. Select DAC, then you can set the DAC IP address.

Refer to the DAP User Manual chapter Setup wizard for more information.

2 Getting started with DAC

This section describes 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

2.1 Login with default account admin

Log in to the DAC device. The default account is **admin**, and the password is **Admin@01**. Hirschmann IT recommends changing the default password for the first login.

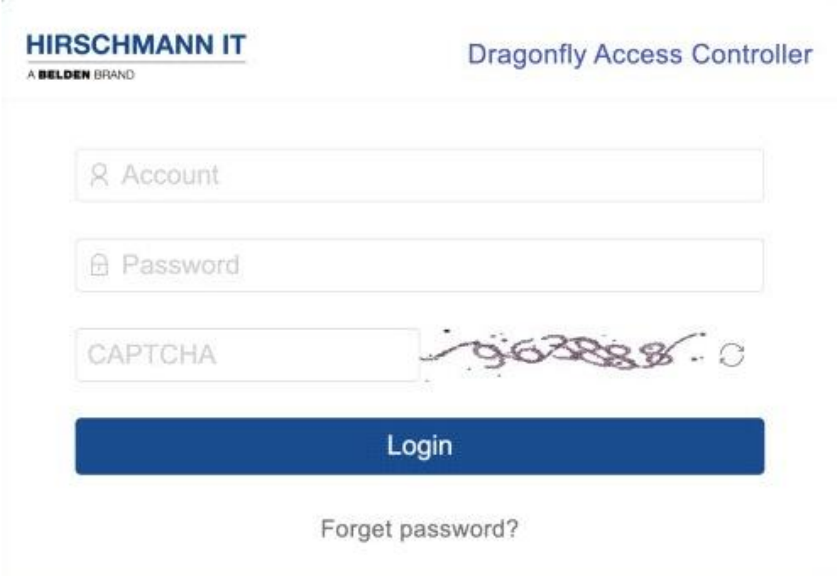
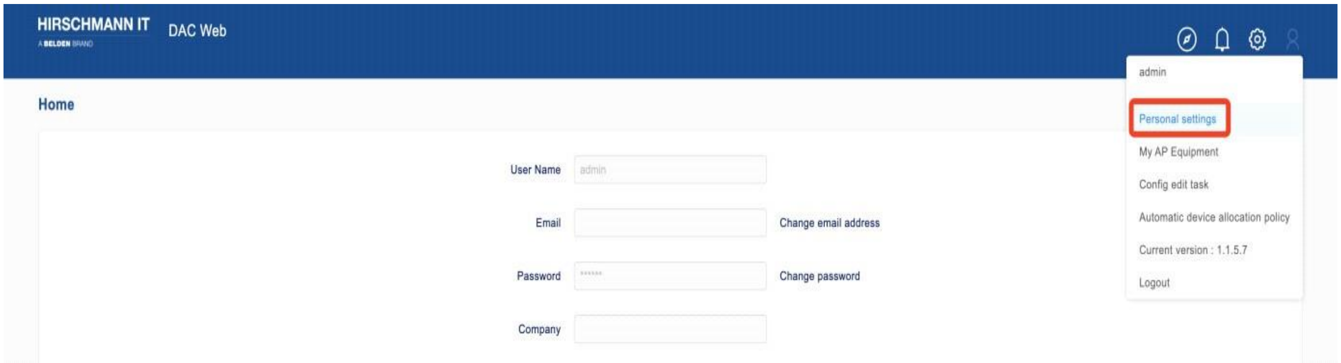


Figure 1: DAC login

2.1.1 Change default password for admin account

Log in to DAC with the admin. Click the person icon on the navigation bar, click the **“Personal settings”** item to enter the **“Personal settings”** page, and then click **“Change password”**.
The **“Change password”** dialog box opens, and you can change your password.

- **Old password**: The password that you are currently using.
- **New password:** The password that you want to change.
- **Confirm password**: Confirm the new password.



User Name admin

Email

Password ******

Company

Figure 2: Change password

2.2 Start with wizard

When you log in to DAC for the first time with the **“admin”** account, it will ask for configuration with the wizard. You can choose **“yes”** to enter the wizard or **“cancel”** to skip it. You can also click the **wizard** icon (🧭) in the navigation bar to enter the wizard. In the wizard, complete the following steps:

2.2.1 First step

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

DAC provides a three-story structure for network architecture management:

- ▶ Site (required)
- ▶ Group (optional)
- ▶ Corporate (optional)

The Site is the basic structure that provides the most abundant network configuration. At the same time, you can partially assign DAPs from the Site to Groups. While inheriting most of the configuration of the Site, Groups provide you with the ability to perform special configurations. 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 business needs. You can also 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 needs more security) to provide security isolation. For more details, refer to Network Structure.

■ Create Site (required)

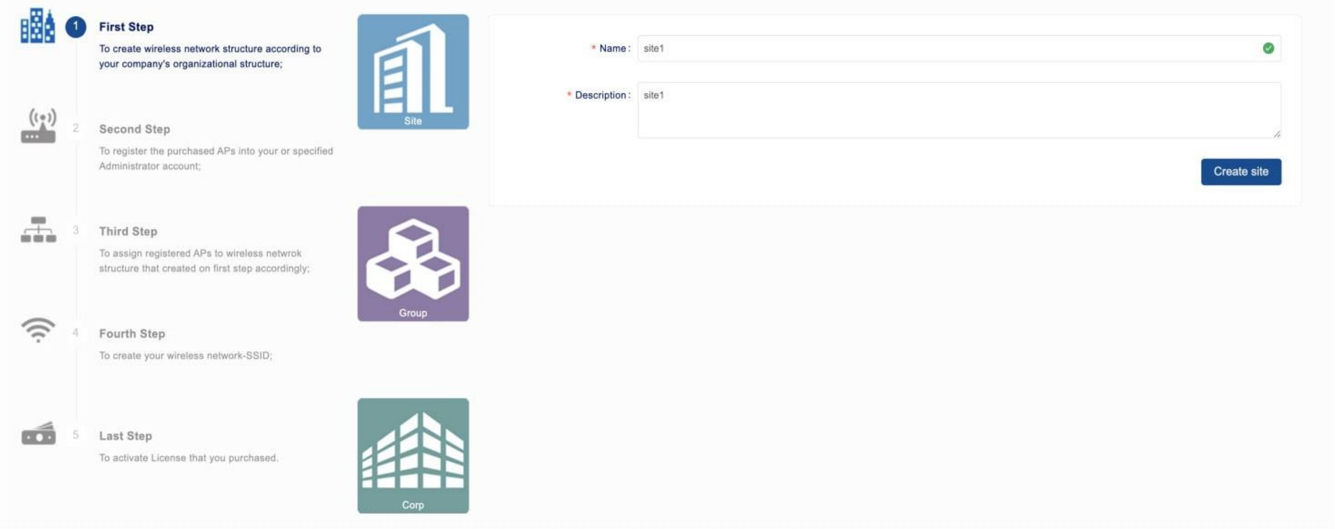
The DAC defines that customer should create a Site first. The Site is one of the distribution units in the configuration. It is an organizational structure concept, larger than a Group and smaller than a Corporate. The wireless configuration created at the Site takes effect on the AP directly under the Site and is distributed to the AP in each Group to which it belongs. First, it is necessary to create the customer’s own Site. If necessary organizational structure segmentation requirements exist, then you can continue creating Groups on the existing Site.

- **Create a Group (optional)**

Group is the smallest unit distributed by wireless configuration. The Group requires a home Site structure that can meet the needs of users. According to the design, the Group can have its own wireless configuration and inherit the wireless configuration from 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.



1 **First Step**
To create wireless network structure according to your company's organizational structure;

2 **Second Step**
To register the purchased APs into your or specified Administrator account;

3 **Third Step**
To assign registered APs to wireless netwrok structure that created on first step accordingly;

4 **Fourth Step**
To create your wireless network-SSID;

5 **Last Step**
To activate License that you purchased.

* Name: site1

* Description: site1

Figure 3: First step wizard configuration

2.2.2 Second step

To register the purchased APs into your or specified Administrator account

This step is not necessary. When DAP registers with DAC for the first time, it automatically binds to the admin account.

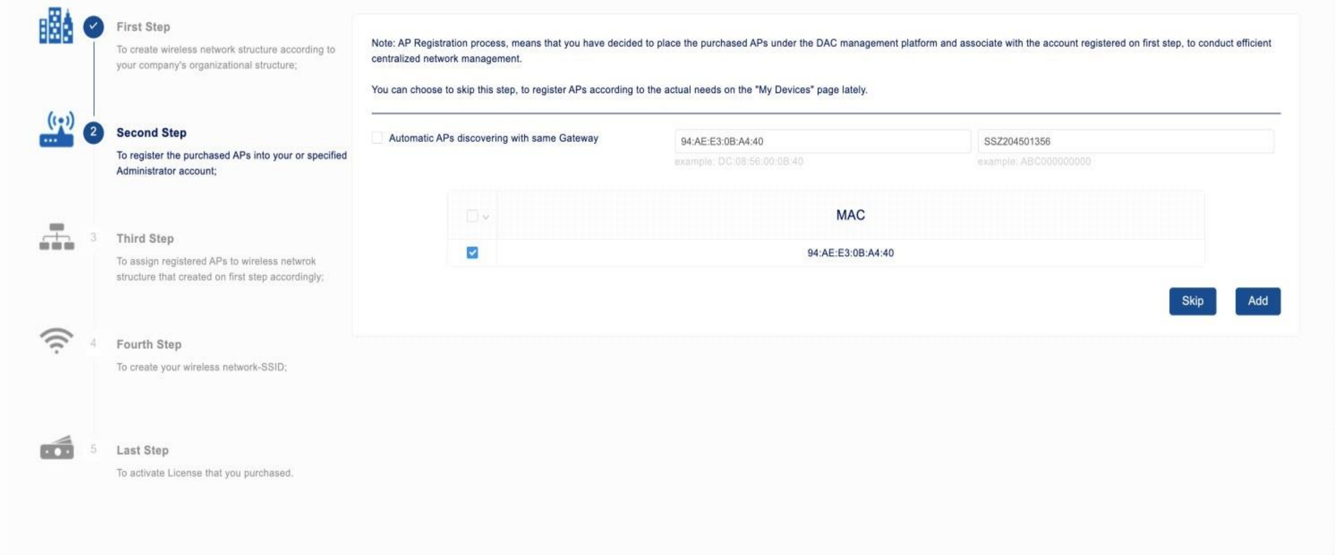
□ Select the AP to register under the account.

☐ Enter the **“MAC”** and the **“SN”** to add the AP to the account.

Note: The AP and DAC networks can communicate with each other. Additionally, we provide more convenient functions such as “Automatic entry of AP with the same gateway” and “addition with cluster”. The former is the outgoing condition of the latter function.

■ **Same gateway AP automatic entry function**

When a customer deploys AP wireless networks in batches on their own network, the AP equipment behind the fixed gateway can use this function. This function completes the entry in batches at one time and displays the AP list under the entry box.



First Step
To create wireless network structure according to your company's organizational structure;

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

3 Third Step
To assign registered APs to wireless netwrok structure that created on first step accordingly;

4 Fourth Step
To create your wireless network-SSID;

5 Last Step
To activate License that you purchased.

Note: AP Registration process, means that you have decided to place the purchased APs under the DAC management platform and associate with the account registered on first step, to conduct efficient centralized network management.

You can choose to skip this step, to register APs according to the actual needs on the "My Devices" page lately.

☐ Automatic APs discovering with same Gateway — 94:AE:E3:0B:A4:40 (example: DC:08:56:00:0B:40) — SSZ204501356 (example: ABC000000000)

☐	MAC
☑	94:AE:E3:0B:A4:40

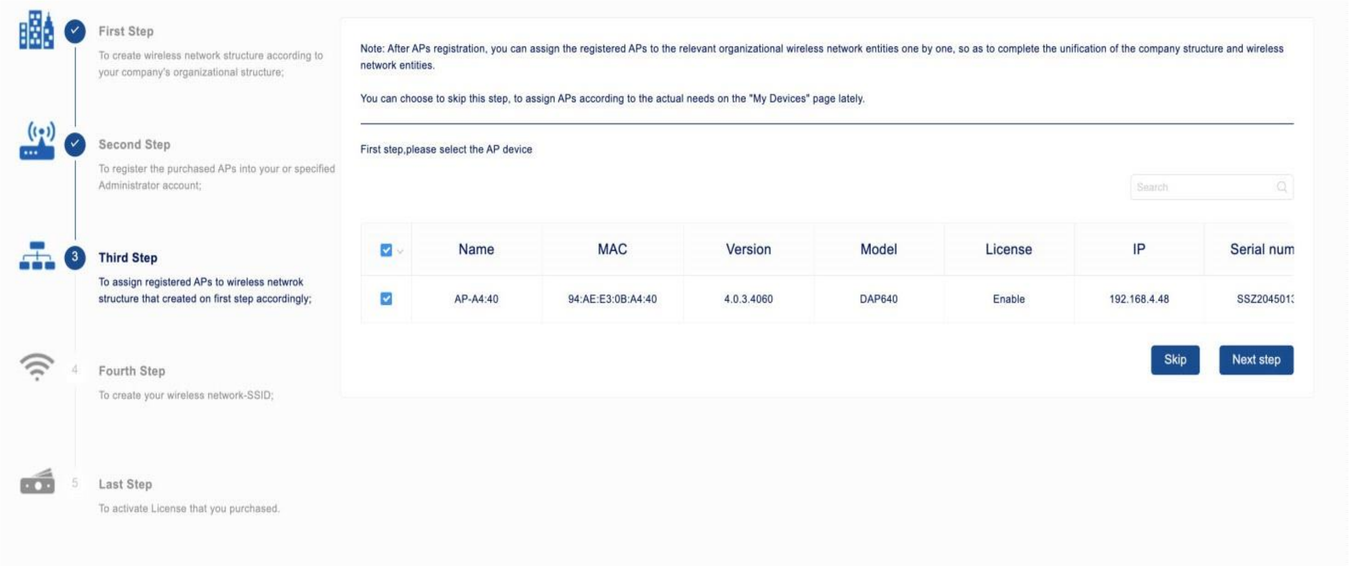
Figure 4: Second step wizard configuration

2.2.3 Third step

To assign registered APs to wireless network structure created on the first step accordingly.

☐ In the third step of the setup wizard, select the AP device for Sites or Groups under Sites.

☐ Click the **“Next step”** button.



First Step

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

Second Step

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

3 Third Step

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

4 Fourth Step

To create your wireless network-SSID;

5 Last Step

To activate License that you purchased.

Note: After APs registration, you can assign the registered APs to the relevant organizational wireless network entities one by one, so as to complete the unification of the company structure and wireless network entities.

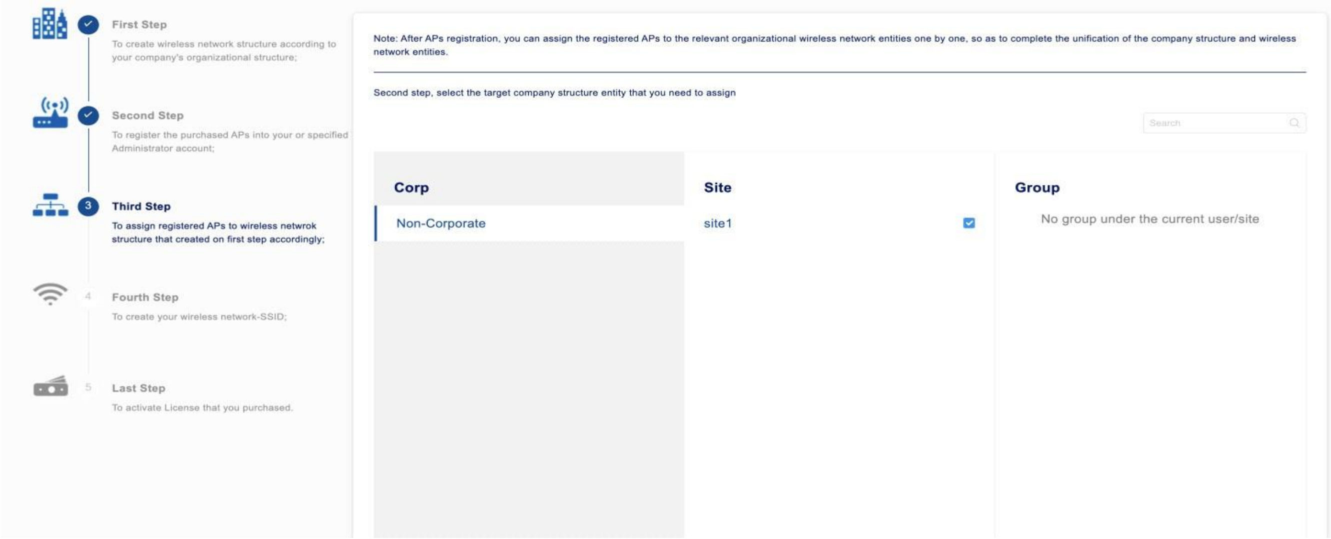
You can choose to skip this step, to assign APs according to the actual needs on the "My Devices" page lately.

First step,please select the AP device

☑	Name	MAC	Version	Model	License	IP	Serial num
☑	AP-A4:40	94:AE:E3:0B:A4:40	4.0.3.4060	DAP640	Enable	192.168.4.48	SSZ204501

Figure 5: Third step wizard configuration

☐ Select **“Site”** or **“Group”** to assign APs.



First Step

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

Second Step

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

3 Third Step

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

4 Fourth Step

To create your wireless network-SSID;

5 Last Step

To activate License that you purchased.

Note: After APs registration, you can assign the registered APs to the relevant organizational wireless network entities one by one, so as to complete the unification of the company structure and wireless network entities.

Second step, select the target company structure entity that you need to assign

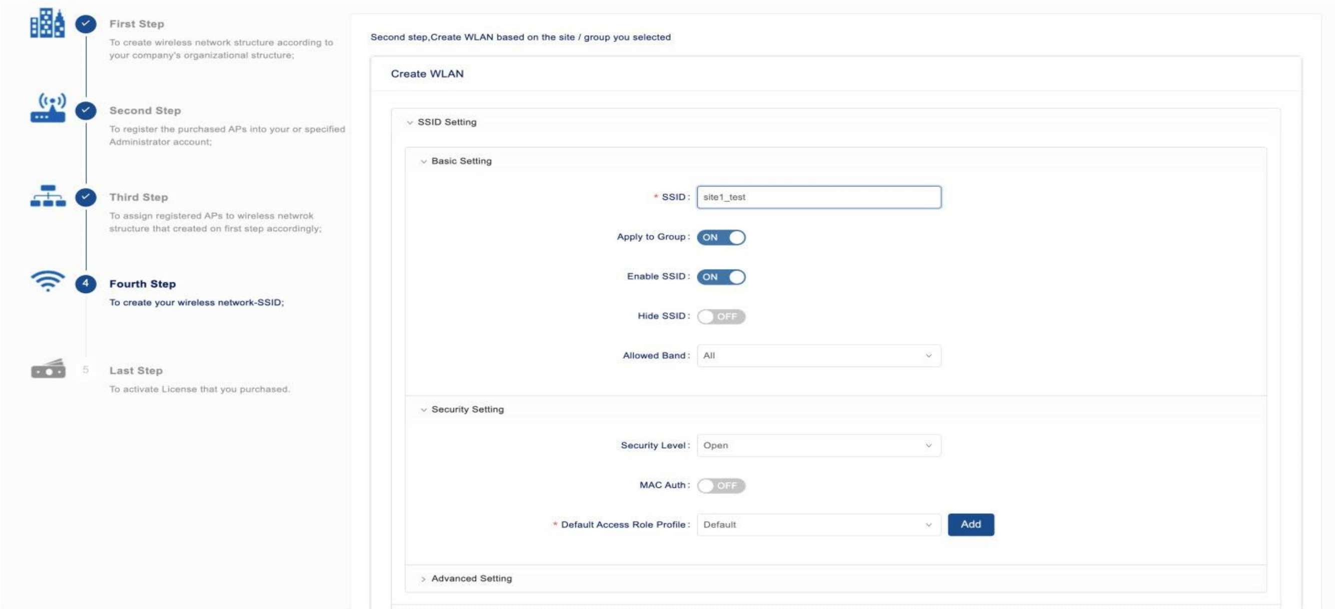
Corp	Site	Group
Non-Corporate	site1 ☑	No group under the current user/site

Figure 6: Select Site to assign AP

2.2.4 Fourth step

To create your wireless network - SSID.

Create WLAN based on the Site or Group. When creating a WLAN, you need to select the Site or Group where the WLAN needs to be created. See “WLAN” on page 87.



First Step

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

Second Step

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

Third Step

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

4 Fourth Step

To create your wireless network-SSID;

5 Last Step

To activate License that you purchased.

Second step,Create WLAN based on the site / group you selected

Create WLAN

SSID Setting

Basic Setting

* SSID : site1_test

Apply to Group : ON

Enable SSID : ON

Hide SSID : OFF

Allowed Band : All

Security Setting

Security Level : Open

MAC Auth : OFF

* Default Access Role Profile : Default

Advanced Setting

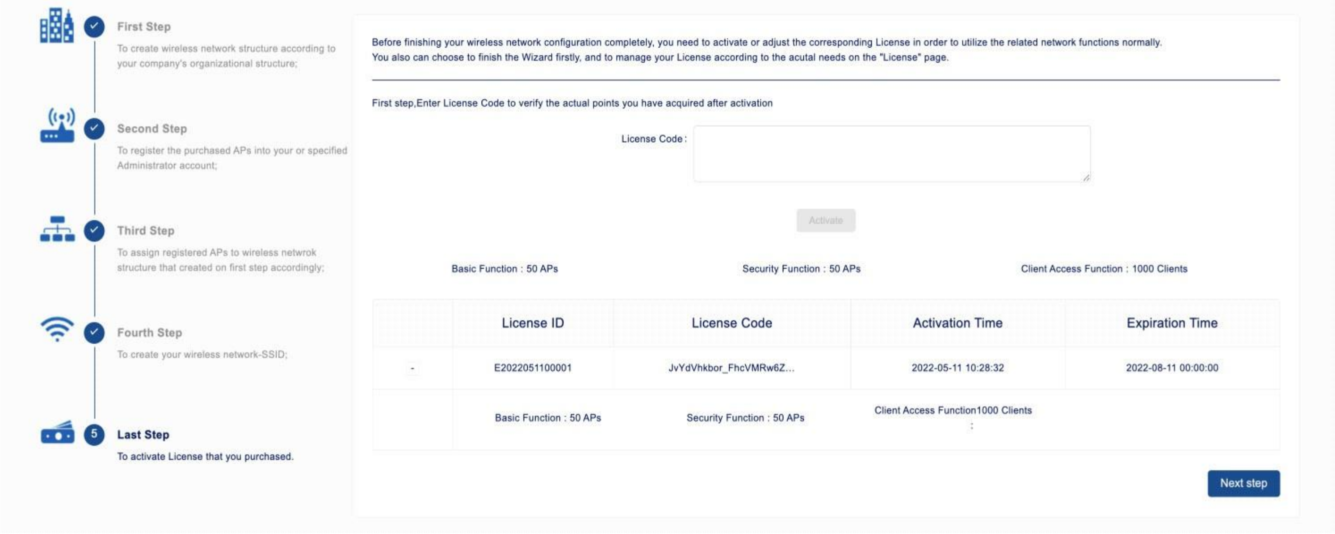
Figure 7: Fourth step wizard configuration

2.2.5 Last step

To activate License that you purchased.

In the last step of the setup wizard, activate the license.

□ Enter the License Code and click the **“Activate”** button to enable the license.



First Step

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

Second Step

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

Third Step

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

Fourth Step

To create your wireless network-SSID;

5 Last Step

To activate License that you purchased.

Before finishing your wireless network configuration completely, you need to activate or adjust the corresponding License in order to utilize the related network functions normally.
You also can choose to finish the Wizard firstly, and to manage your License according to the acutal needs on the "License" page.

First step,Enter License Code to verify the actual points you have acquired after activation

License Code :

Basic Function : 50 APs

Security Function : 50 APs

Client Access Function : 1000 Clients

	License ID	License Code	Activation Time	Expiration Time
-	E2022051100001	JvYdVhkbor_FhcVMRw6Z...	2022-05-11 10:28:32	2022-08-11 00:00:00
	Basic Function : 50 APs	Security Function : 50 APs	Client Access Function1000 Clients :	

Figure 8: Last step wizard configuration

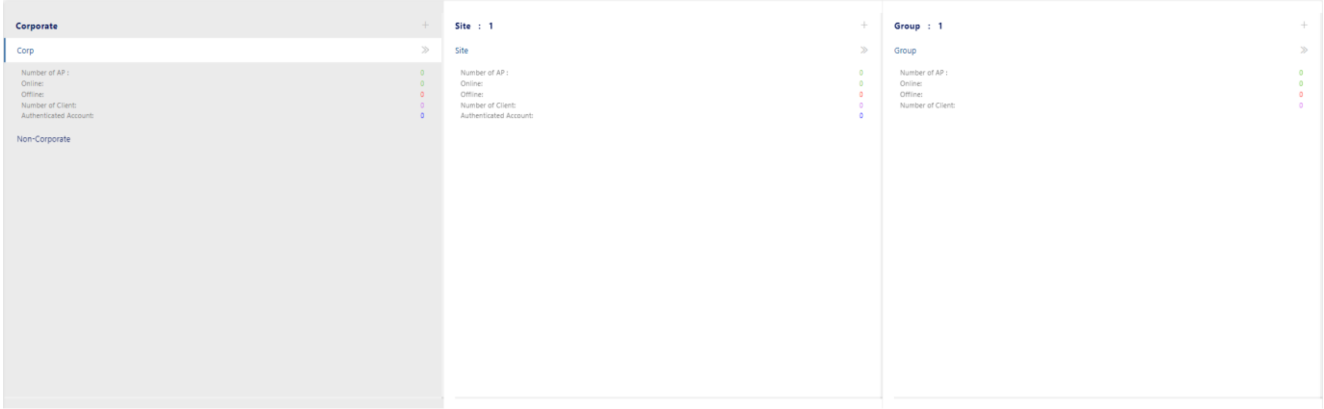
2.3 Network structure

The internal organization of an enterprise is often not completely flat and is divided into different regions or subnets. For enterprises with many branches or chain stores, it is necessary to manage the network separately. Additionally, administrators with different permissions are assigned to branches or stores. This allows them to maintain the network. DAC provides a mechanism to deal with these situations.

DAC manages the enterprise network structure through relationships at the Corporate (optional), Site (required), and Group (optional) levels. In the wizard, we already established 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 that provides the most abundant network configuration.
- **Group:** A Group belongs to a Site and is created only by a Site. While inheriting most of the configuration of the Site, Groups provide you with the ability for special configuration.
- **Corporate**: Corporate is a set of Sites. Adding Sites to Corporate can help you manage multiple Sites and allocate unified permissions.



Corporate +

Corp »

Number of AP : 0
Online: 0
Offline: 0
Number of Client: 0
Authenticated Account: 0

Non-Corporate

Site : 1 +

Site »

Number of AP : 0
Online: 0
Offline: 0
Number of Client: 0
Authenticated Account: 0

Group : 1 +

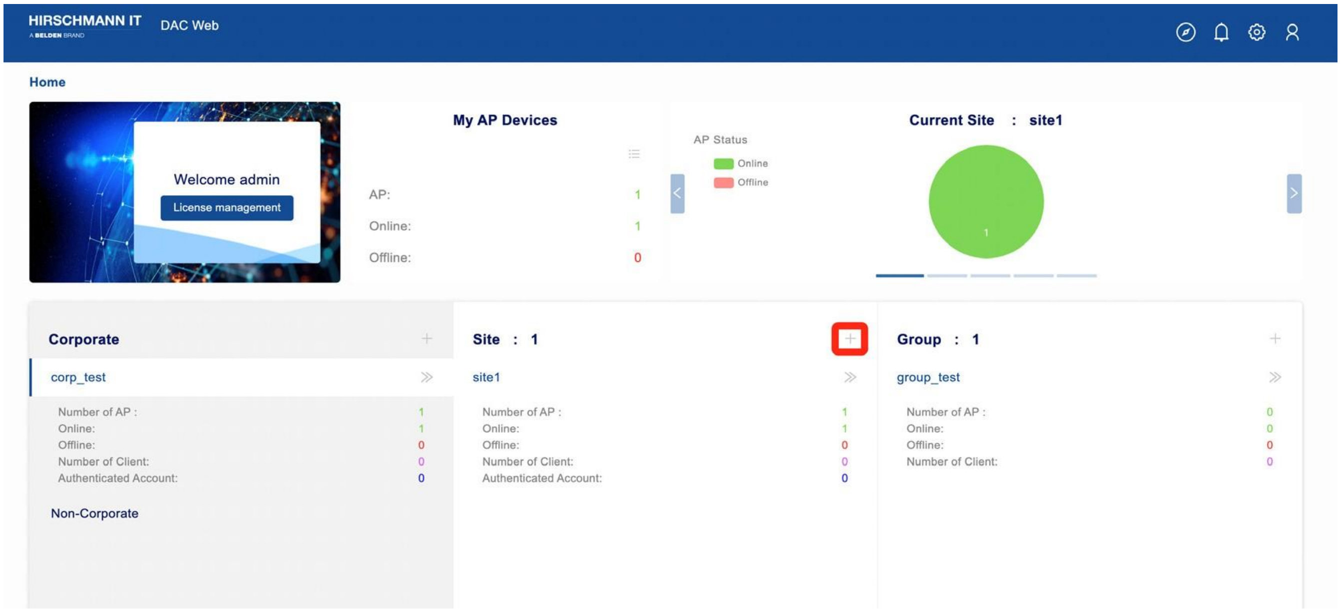
Group »

Number of AP : 0
Online: 0
Offline: 0
Number of Client: 0

Figure 9: Network Structure

2.3.1 Create a new Site

- □ On the User Dashboard page, click the **“+”** icon on the **“Site”** tab. The **“Create Site”** window appears.



My AP Devices

AP: 1
Online: 1
Offline: 0

Current Site : site1

Corporate

corp_test

Number of AP : 1
Online: 1
Offline: 0
Number of Client: 0
Authenticated Account: 0

Non-Corporate

Site : 1

site1

Number of AP : 1
Online: 1
Offline: 0
Number of Client: 0
Authenticated Account: 0

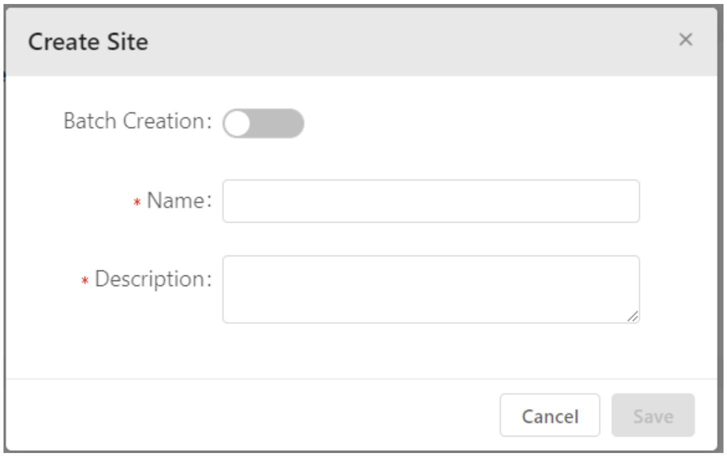
Group : 1

group_test

Number of AP : 0
Online: 0
Offline: 0
Number of Client: 0

Figure 10: Create a new Site

- □ Specify the **“Name”** and **“Description”** fields.
- □ Click the **“Save”** button to apply the settings. The newly created Site is displayed on the **“Site”** tab of the user dashboard.



Batch Creation:

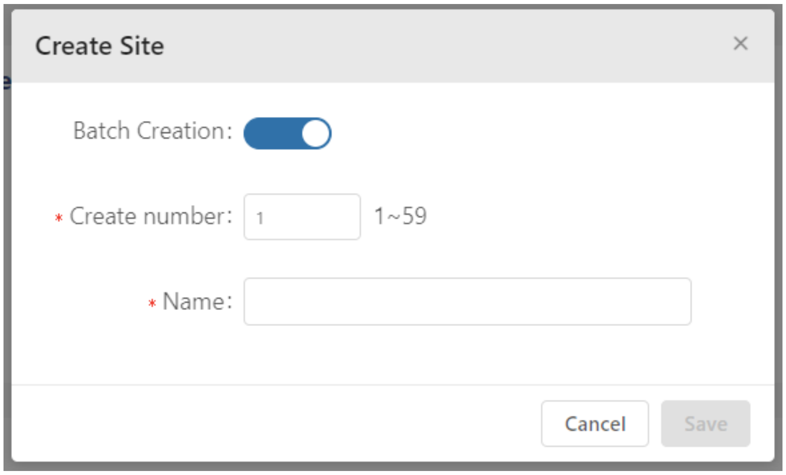
* Name:

* Description:

Figure 11: Create Site window

□ If you want to create Sites in batches, enable the **“Batch Creation”** switch.

□ Fill in the number of Sites to be created, up to 64.



Create Site

Batch Creation: ●

* Create number: 1 1~59

* Name:

Figure 12: Create Batch of Sites Window

Note: Each user can create 64 Sites at most. If you already have other Sites, then the total number of Sites for batch creation is 64 minus the number of Sites already created.

2.3.2 Create a new Group

☐ On the user dashboard page, select the Site to which you want to add a Group.

☐ Click the **“+”** icon on the **“Group”** tab.

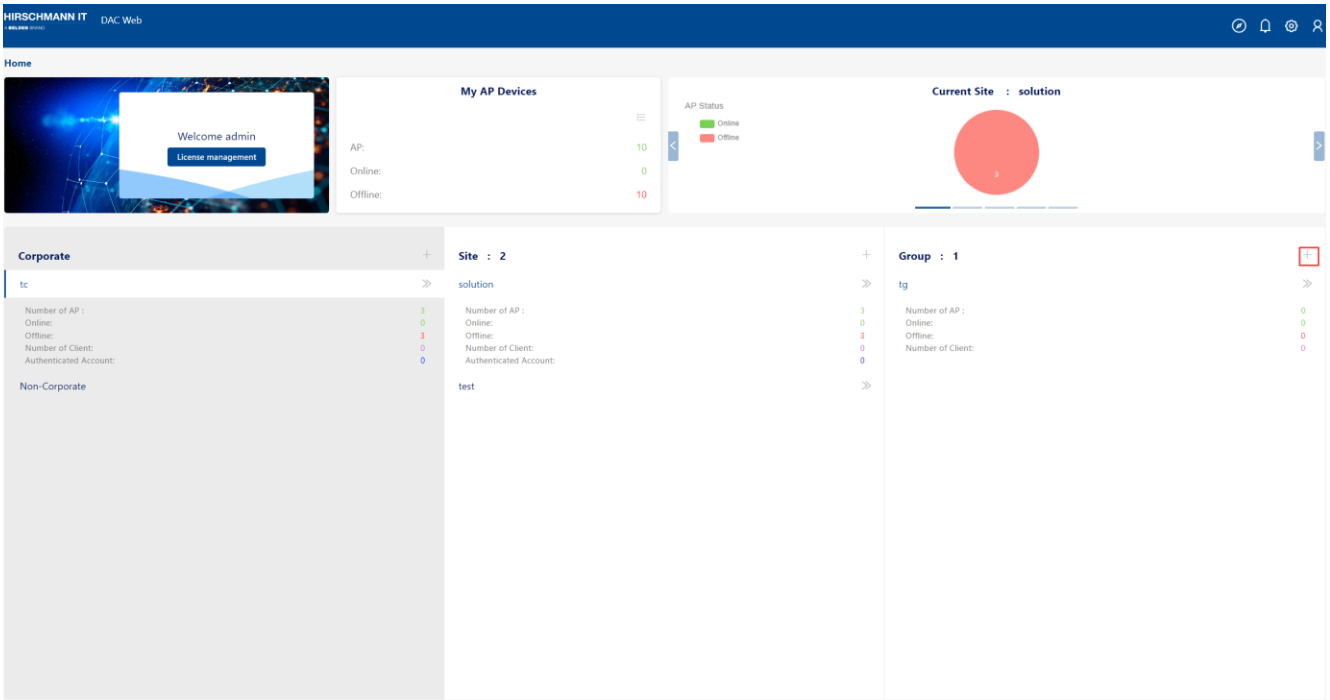


Figure 13: Create a new Group

☐ Click **“Add Group”**, the **“Create Group”** window appears.

☐ Specify the **“Name”** and **“Description”** fields.

☐ Click the **“Save”** button to apply the settings. The newly created Group is displayed on the **“Group”** tab of the user dashboard.

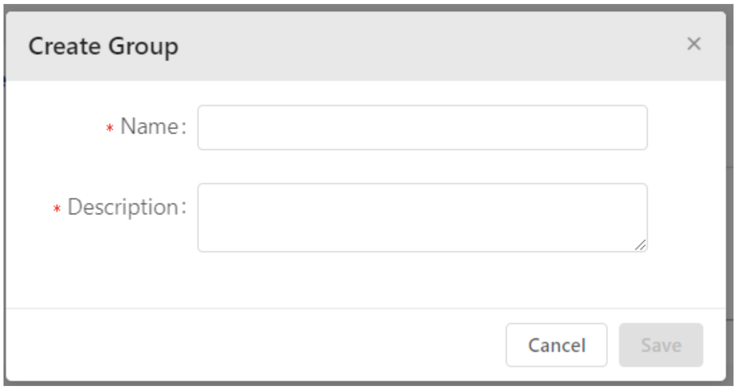


Figure 14: Create Group window

2.3.3 Create a new Corporate

- ☐ On the user dashboard page, click the **“+”** icon on the **“Corporate”** tab, which displays the **“Create Corporate”** window.

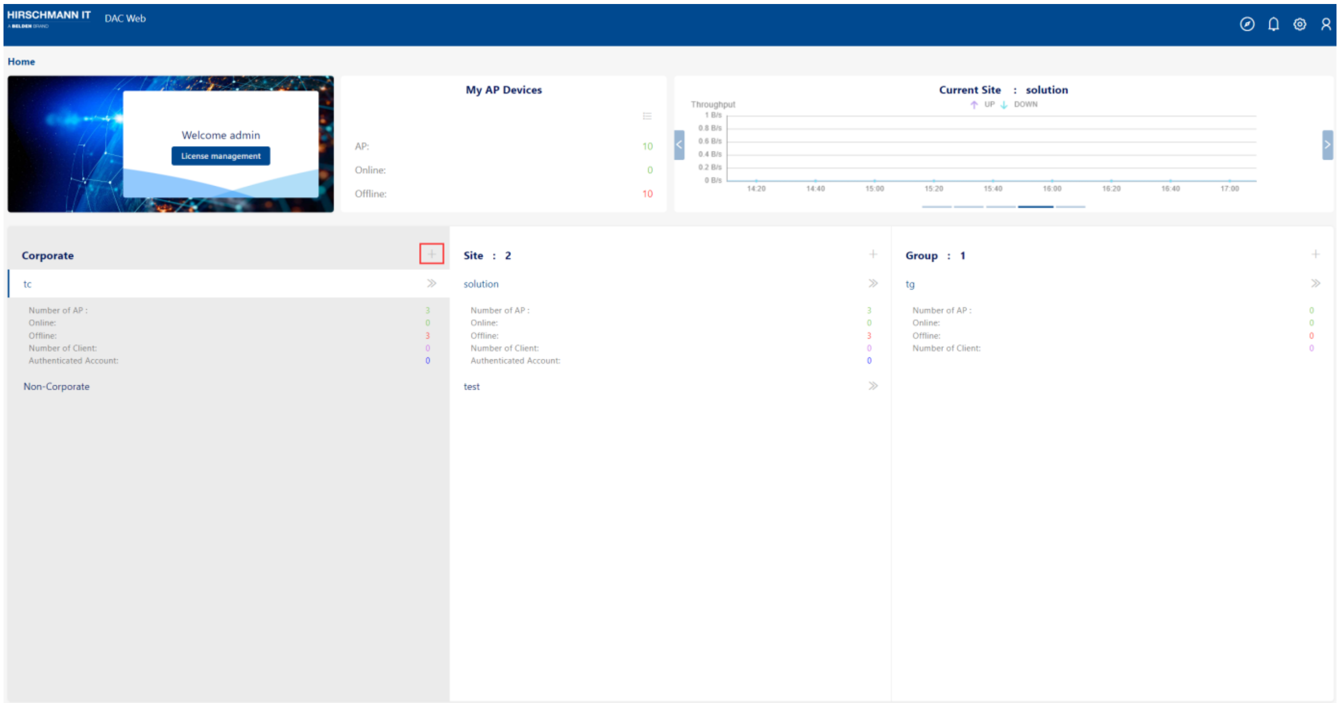


Figure 15: Create a new Corporate

- ☐ Specify the **“Name”** and **“Description”** fields.
- ☐ Click **“Save”** to apply the settings. The newly created Corporate is displayed on the **“Corporate”** tab of the user dashboard.

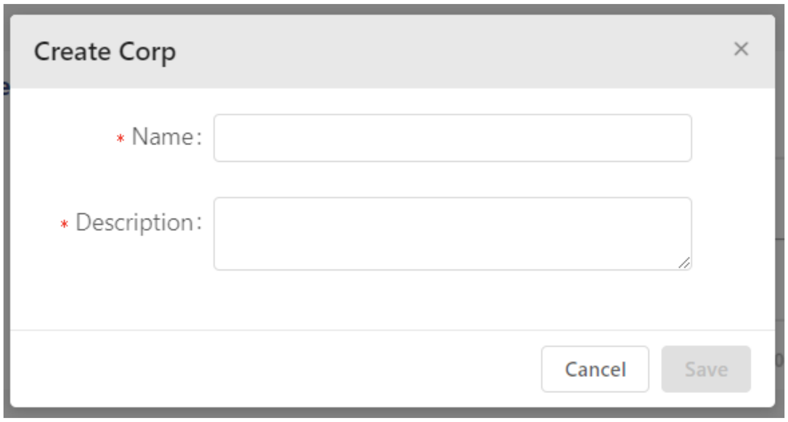


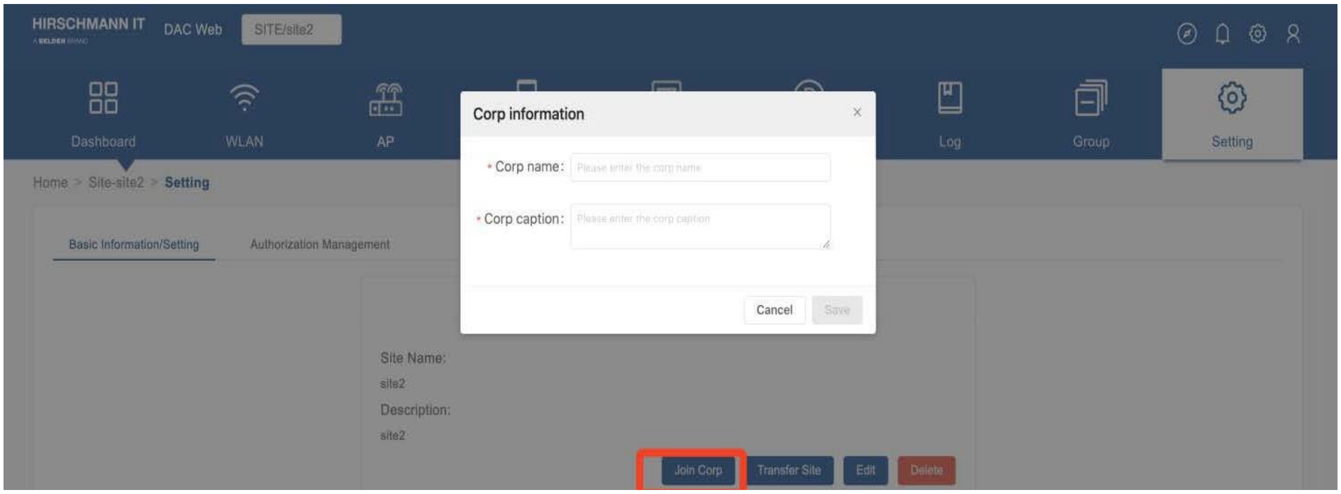
Figure 16: Create Corp window

2.3.4 Add a Site to a Corporate

A Site can only join one Corporate. If a Site is already joined into a Corporate, you should first quit it.

□ Open the **“Setting”** tab in the Site view.

□ Click the **“Join Corp”** button. The **“Corp information”** window appears.



* Corp name: Please enter the corp name

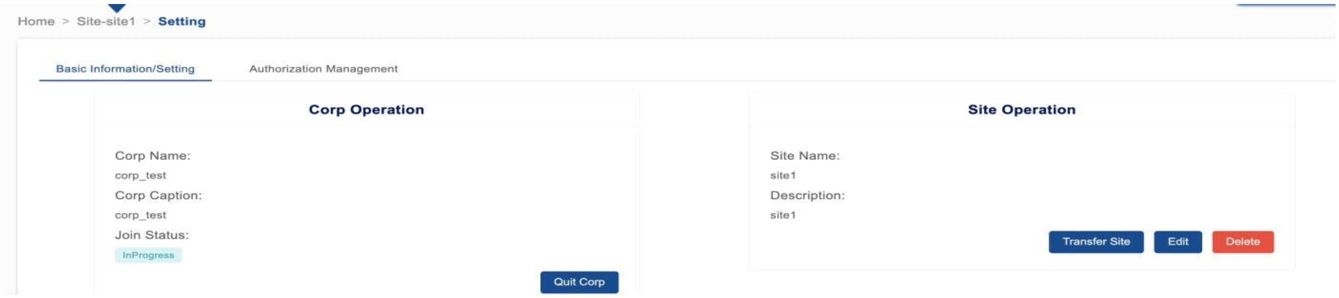
* Corp caption: Please enter the corp caption

Site Name:
site2
Description:
site2

Figure 17: Corp Information Window

□ Specify the **“Corp name”** and **“Corp caption”** fields. You need to make sure that the Corp exists.

□ Click the **“Save”** button. If successful, the **“Corp Operation”** tab in the **“Setting”** view of the Site appears and the Join Status is **“InProgress”**.



Corp Name:
corp_test
Corp Caption:
corp_test
Join Status:
InProgress

Site Name:
site1
Description:
site1

Figure 18: Corp & Site Operation Window

□ Go to **“Corp dashboard”**. The join request on the **“Monitoring Panel”** appears.

□ Click the **“Accept”** button to approve the join request or click the **“Reject”** button to deny the join request.

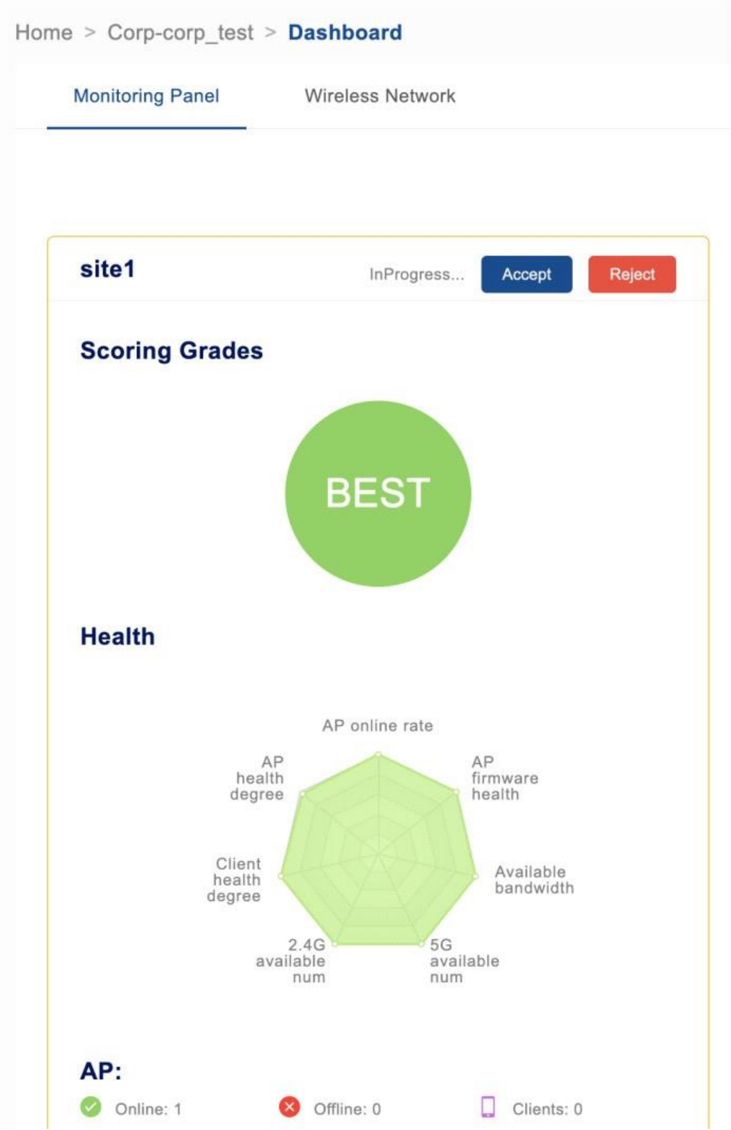


Figure 19: Corp operation window

2.4 Account management

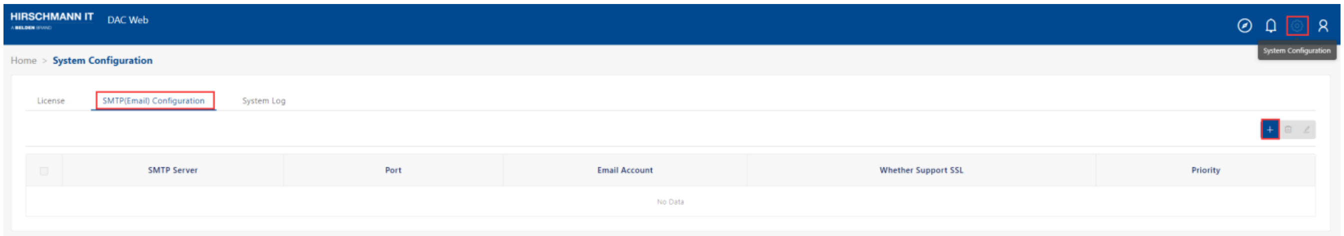
DAC is a multi-tenant system with rich and flexible authorization control. As a network administrator, you can usually use the default account **“admin”** to manage your wireless network. But in some cases, you need to make network management more flexible by creating new accounts and assigning authorization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

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

To enable the email notification for account creation and other functions of the DAC (these functions require the system to send emails externally), you first need to add at least one **SMTP Server** that can send emails from the DAC.

2.4.1 Add SMTP server

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



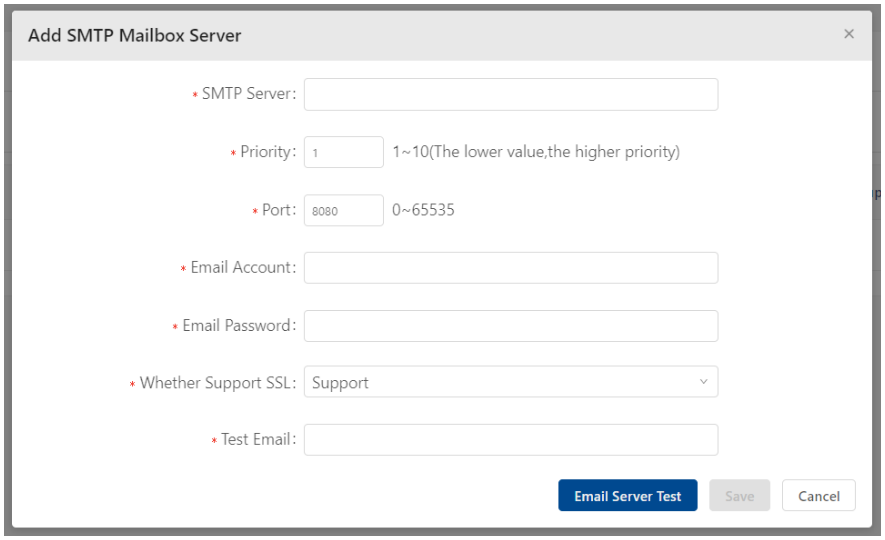
☐	SMTP Server	Port	Email Account	Whether Support SSL	Priority
			No Data		

Figure 20: SMTP configuration

- ☐ At the **Add SMTP Mailbox Server** Dialog, enter the following fields:
  - ▶ **SMTP Server:** Domain of the SMTP Server.
  - ▶ **Priority:** Priority of the SMTP Mail Server. At most 10 SMTP Mail Servers can be added. The lower the value, the higher the priority. If a working mailbox is inoperable to send mail due to a detected failure, the system tries to send mail from a lower priority working mailbox.
  - ▶ **Port:** Port of the SMTP Server.

- **Email Account:** An email account used to send mail.
- **Email Password:** Email Password.
- **Whether Support SSL:**
  - **Support:** Connect the mail server with SSL.
  - **Not Support:** Mail servers that do not support SSL will connect normally.
- **Test Email:** An email address used to receive the test email.

□ Click the **“Email Server Test”** button.
DAC will send a test email to verify the functionality. The **“Save”** button will be available only after sending Test Email successfully.
□ Click the **“Save**” button to save the working mailbox.



Add SMTP Mailbox Server ×

* SMTP Server:

* Priority: 1 1~10(The lower value,the higher priority)

* Port: 8080 0~65535

* Email Account:

* Email Password:

* Whether Support SSL: Support

* Test Email:

Figure 21: Add SMTP Mailbox Server window

2.4.2 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.

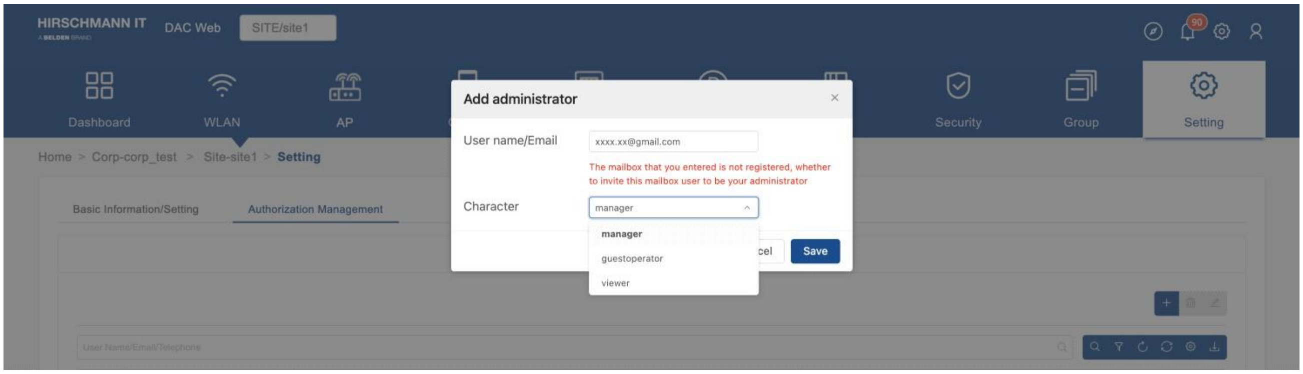
■ **Initiating email invitation**

□ Open **“Setting”** page in the view of Site.

□ Click the **“Authorization management”** tab.
□ Click the **“+”** icon and the **“Add Administrator”** window appears.
□ Enter the **“User name/Email”** of the account to register.

□ Select a **“Character”** from the drop-down list to define the role of the new account.

□ Click the **“Save”** button.



Add administrator

User name/Email: xxxx.xx@gmail.com

The mailbox that you entered is not registered, whether to invite this mailbox user to be your administrator

Character: manager

manager
guestoperator
viewer

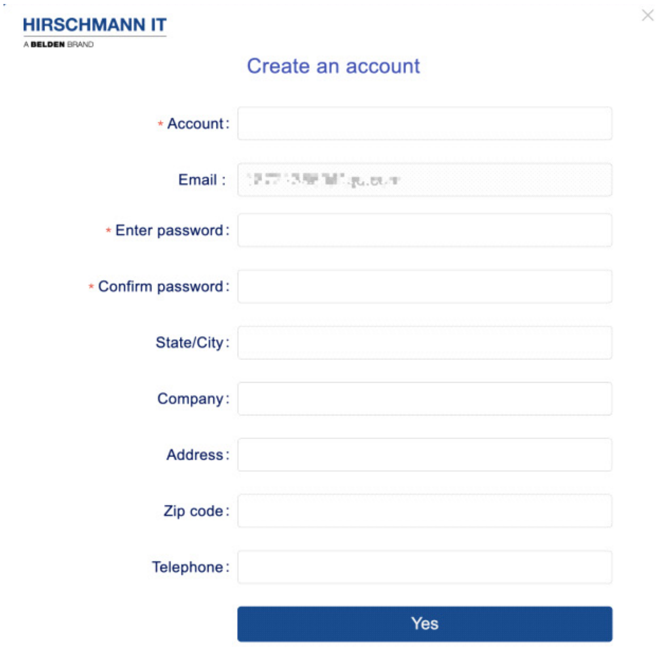
cel
Save

Figure 22: Initiating email invitation

■ Create account

□ Log in to the configured mailbox.

□ Click the registration connection, then go to the **“Invitation Registration”** page.



Create an account

* Account:	
Email :	[redacted]
* Enter password:	
* Confirm password:	
State/City:	
Company:	
Address:	
Zip code:	
Telephone:	

Yes

Figure 23: Create account

□ Enter the following fields to create an account:

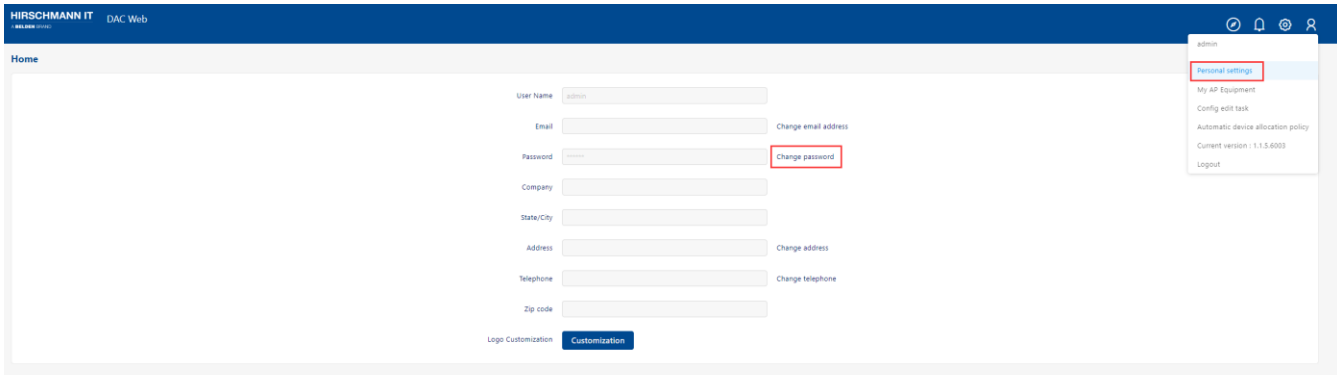
- **Account:** Account.
- **Email:** The email used for login.

- ▶ **Enter Password:** The password used for login.
- ▶ **Confirm Password:** Confirm the password.
- ▶ **State/City:** State/City.
- ▶ **Company:** The name of your company.
- ▶ **Address:** The address of your company.
- ▶ **Zip code:** The zip code of your company.
- ▶ **Telephone:** Your telephone number.

2.4.3 Change password

After logging in to the device, you can change the password.

- ☐ Click the personal icon on the navigation bar.
- ☐ Click the **“Personal settings”** item to enter the **“Personal setting”** page.
- ☐ Click the **“Change password”** and the **“Change password”** dialog box opens.



User Name: admin
Email:
Password:
Company:
State/City:
Address:
Telephone:
Zip code:
Logo Customization:

Figure 24: Personal settings

- ☐ Enter the following fields to change your password:
  - ▶ **Old password**: The password that you use currently.
  - ▶ **New password:** The password that you want to change to.
  - ▶ **Confirm password:** Confirm the new password.

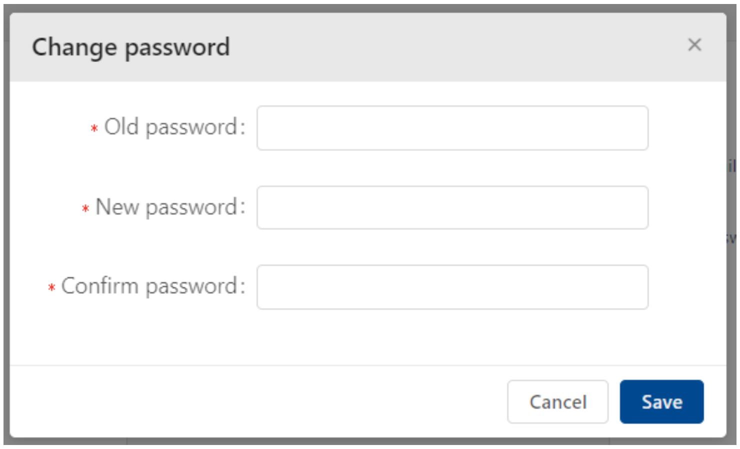


Figure 25: Change password window

2.4.4 Forget password

If you forget your password, you can recover your account.

- □ Click the **"Forgot password"** link on the login page. The **"Recover your account"** page appears.
- □ Enter the following fields to recover your account:
  - ▶ **Email / Account**: Enter your email or account.
  - ▶ **Verification code**: Once you enter the correct email or account, click the **"Get Code"** button. Then you receive a Verification Code in your email.
  - ▶ **New password**: Input the password that you want to set.
  - ▶ **Confirm password**: Confirm the password.

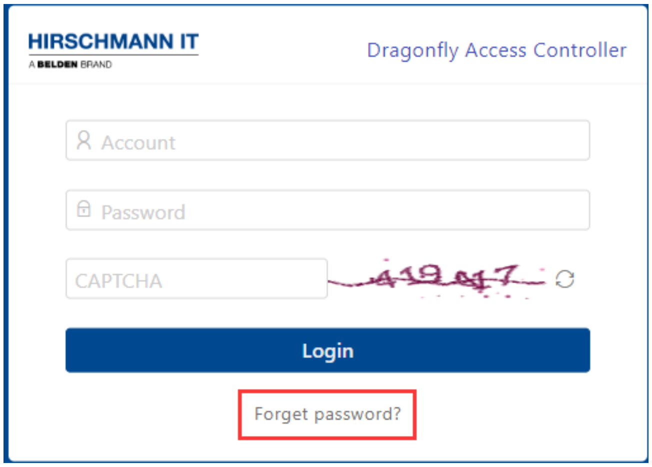
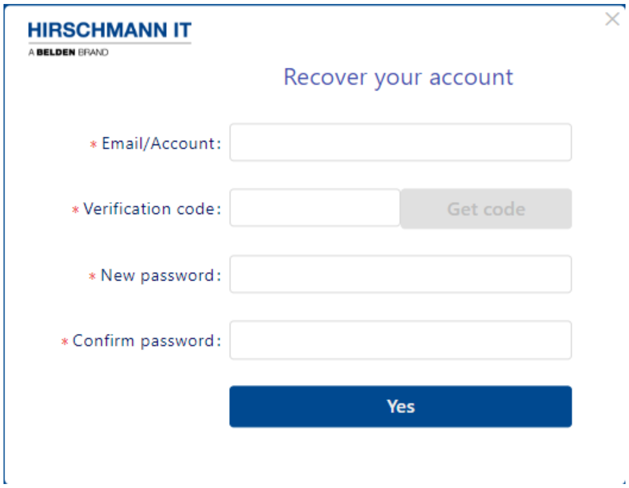


Figure 26: Forget password button



Recover your account

* Email/Account:

* Verification code:

* New password:

* Confirm password:

Figure 27: Recover your account window

2.5 Administrator privileges

The **“admin”** account is the main user of DAC. It owns AP devices, Licenses, and 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 all AP devices and licenses. ▶ Create network structures and assign AP to Site. Use the management and monitoring functions. ▶ Invite other users to manage and monitor the network based on the network organization structure.
Other users	Manager	▶ The manager of the network, not the owner of the device and license. ▶ Use the management and monitoring functions.
	Viewer	▶ The observer of the network, rather than the manager of the network. ▶ It has privileges for the 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 3: DAC Administrators

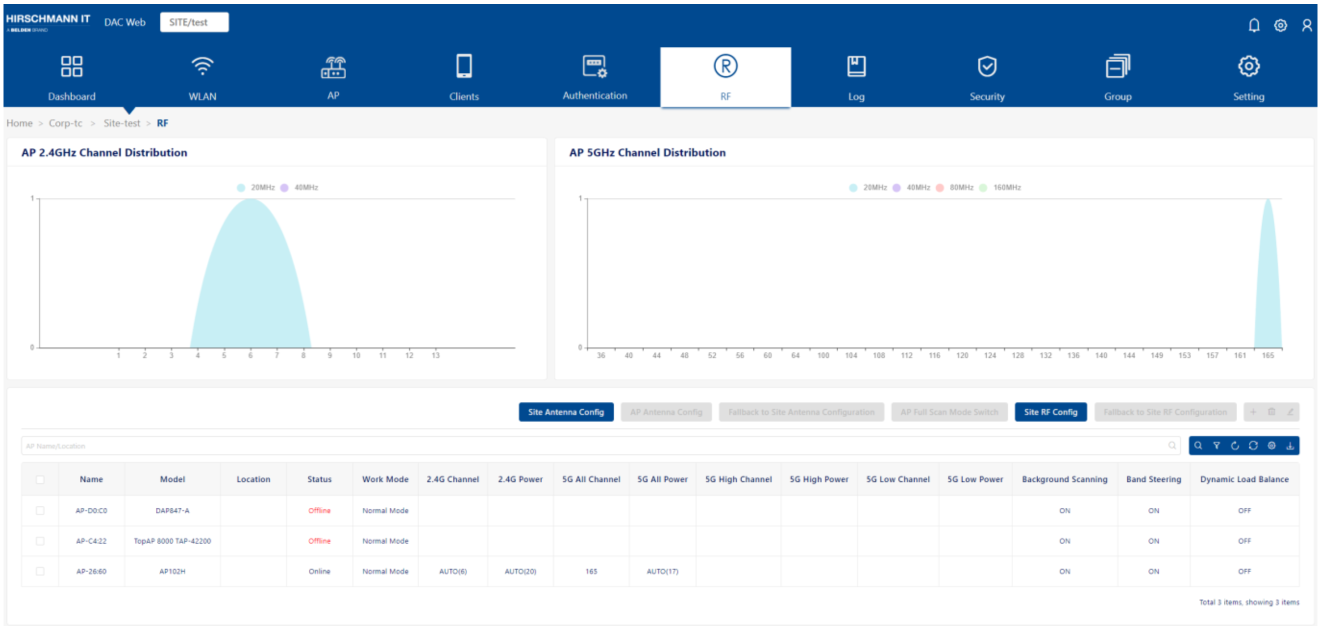
■ Admin

- ▶ The **“admin”** account owns the network, including the AP devices and licenses.
- ▶ The **“admin”** account can create new network structures (Site, Group, and Corporate). The account can also assign APs to these network structures excluding Corporate, and authorize the management of Site and Group to the other accounts.

- The **“admin”** account has privileges for the management and monitoring functions.
- The **“admin”** account can initiate an invitation for other people to register an account. Only the email address 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.

Manager

If a user has manager privileges on a Site, they can use the management and monitoring functions of the Site.



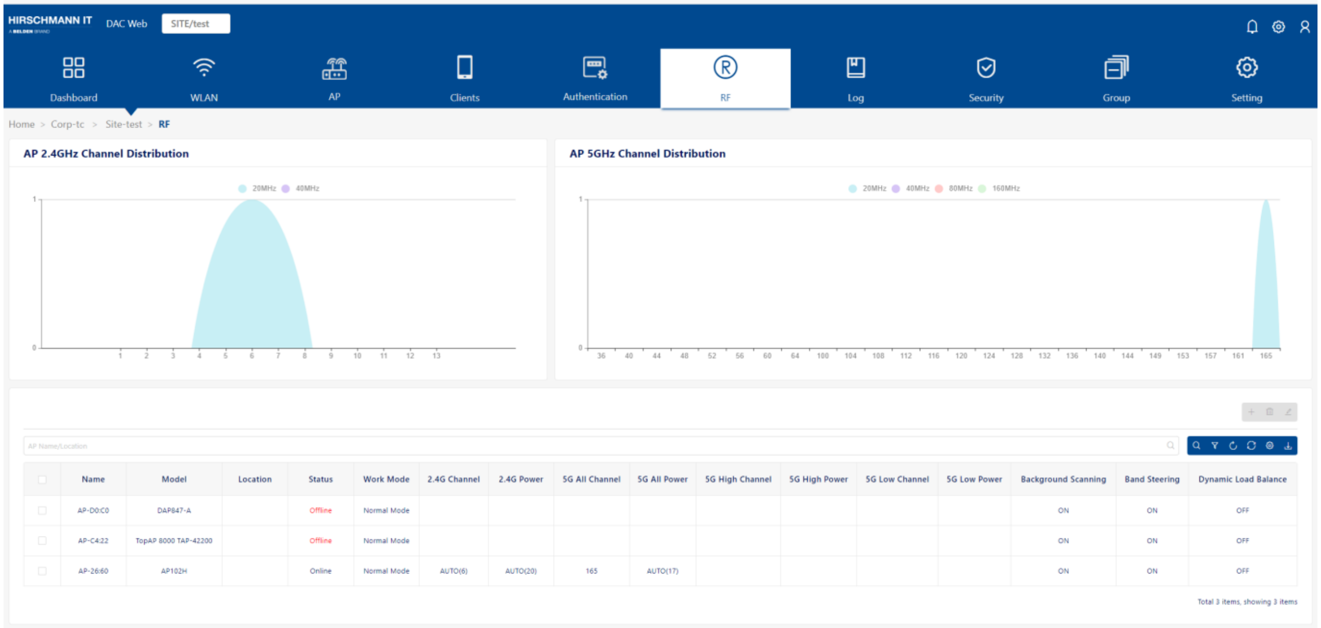
□	Name	Model	Location	Status	Work Mode	2.4G Channel	2.4G Power	5G All Channel	5G All Power	5G High Channel	5G High Power	5G Low Channel	5G Low Power	Background Scanning	Band Steering	Dynamic Load Balance
□	AP-D0:C0	DAP847-A		Offline	Normal Mode									ON	ON	OFF
□	AP-C4:22	TopAP 8000 TAP-42200		Offline	Normal Mode									ON	ON	OFF
□	AP-26:60	AP102H		Online	Normal Mode	AUTO(6)	AUTO(20)	165	AUTO(17)					ON	ON	OFF

Total 3 items, showing 3 items

Figure 28: RF page for Manager

Viewer

If a user has viewer privileges on a Site, they can view the Site configuration and monitor the running status of the Site, but they cannot add or modify the Site’s configuration.



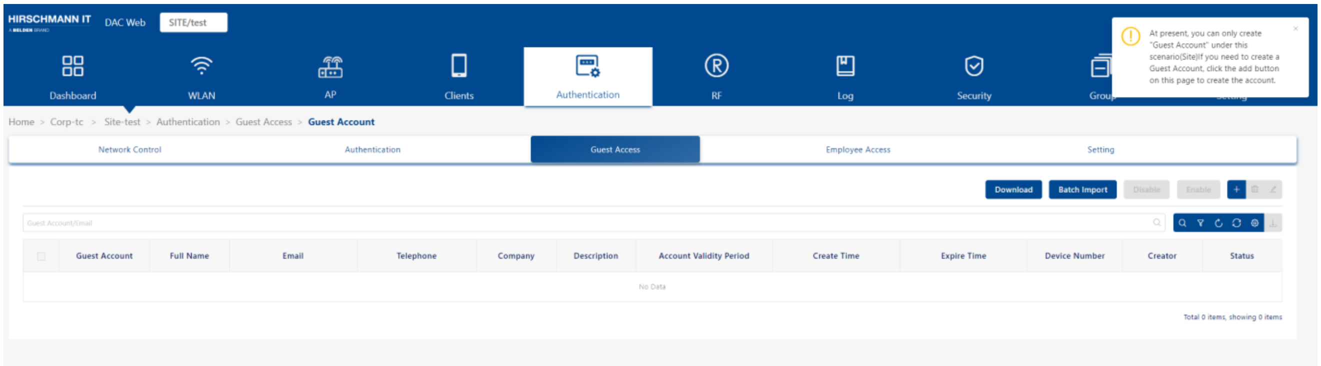
□	Name	Model	Location	Status	Work Mode	2.4G Channel	2.4G Power	5G All Channel	5G All Power	5G High Channel	5G High Power	5G Low Channel	5G Low Power	Background Scanning	Band Steering	Dynamic Load Balance
□	AP-D0:C0	DAP847-A		Offline	Normal Mode									ON	ON	OFF
□	AP-C4:22	TopAP 8000 TAP-42200		Offline	Normal Mode									ON	ON	OFF
□	AP-26:60	AP102H		Online	Normal Mode	AUTO(6)	AUTO(20)	165	AUTO(17)					ON	ON	OFF

Total 3 items, showing 3 items

Figure 29: RF page for Viewer

- **Guest operator**

If a user has Guest Operator privileges on a Site, they only have the permission to manage guest accounts of the Site.



At present, you can only create "Guest Account" under this scenario(Site)If you need to create a Guest Account, click the add button on this page to create the account.

□	Guest Account	Full Name	Email	Telephone	Company	Description	Account Validity Period	Create Time	Expire Time	Device Number	Creator	Status
	No Data											

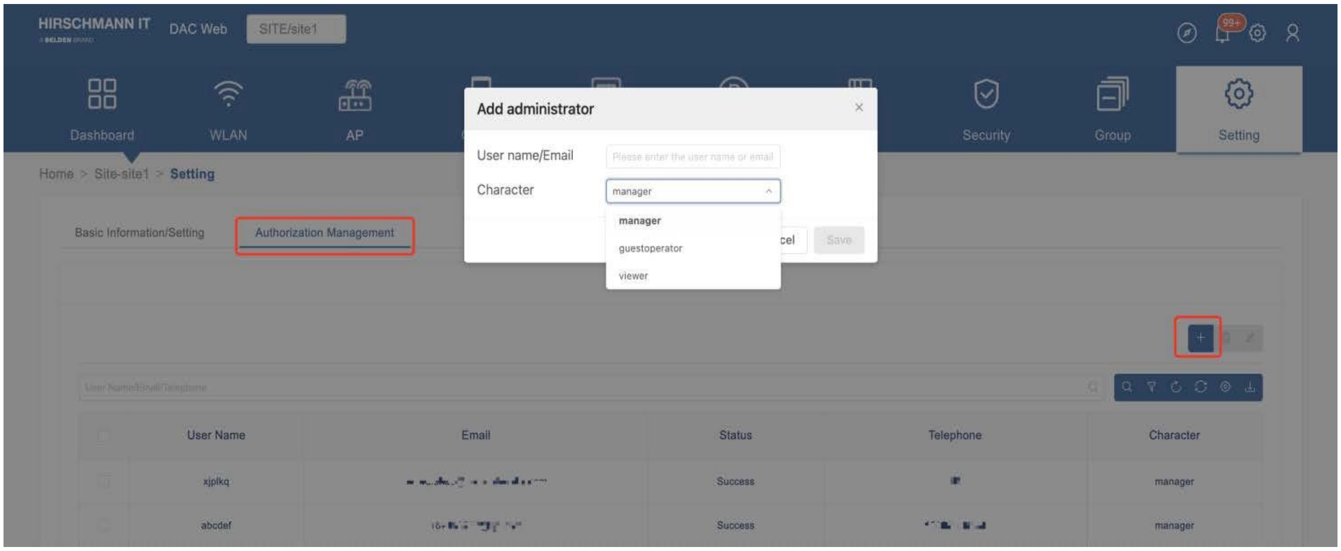
Total 0 items, showing 0 items

Figure 30: Guest operator management page

2.5.1 Add Administrator for Site

- ☐ Click the **“Authorization Management”** tab on the **“Setting”** page of the Site.
- ☐ Click the **“+”** icon. The **“Add administrator”** window opens.
- ☐ Specify the **“User name/Email”** field. The User name should exist.
- ☐ Select **“Character”** from the drop-down list. You can also invite a new user to manage the current Site. See “Create account” on page 33 .

□ Click the **“Save”** button to complete authorization.



User name/Email: Please enter the user name or email

Character: manager

User Name	Email	Status	Telephone	Character
xjplkq	[redacted]	Success	[redacted]	manager
abcdef	[redacted]	Success	[redacted]	manager

Figure 31: Add administrator for site

2.5.2 Remove Administrator for Site

□ Select the user from **“Authorization Management”** that you want to remove from the list.

□ Click the **“Delete”** icon.

□ Click **“Yes”** on the confirmation prompt.

3 DAC user interface introduction

This chapter introduces the basic operations 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

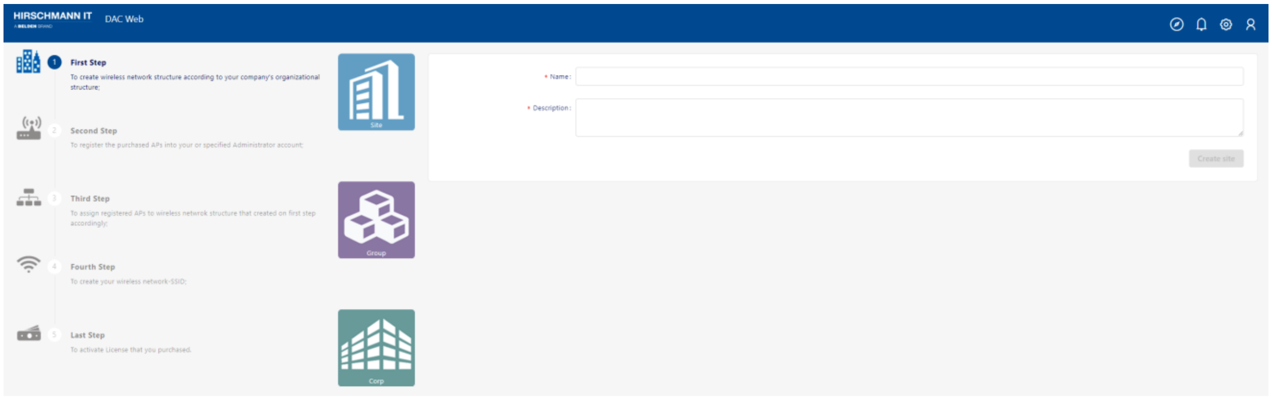
3.1 Banner tools

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

Table 4: Banner tools

▶ Wizard

- Quick access to the wizard mode. You can configure the relevant network structure and its corresponding license activation. See “Start with wizard” on page 20.



1 First Step
To create wireless network structure according to your company's organizational structure;

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

3 Third Step
To assign registered APs to wireless netwrok structure that created on first step accordingly;

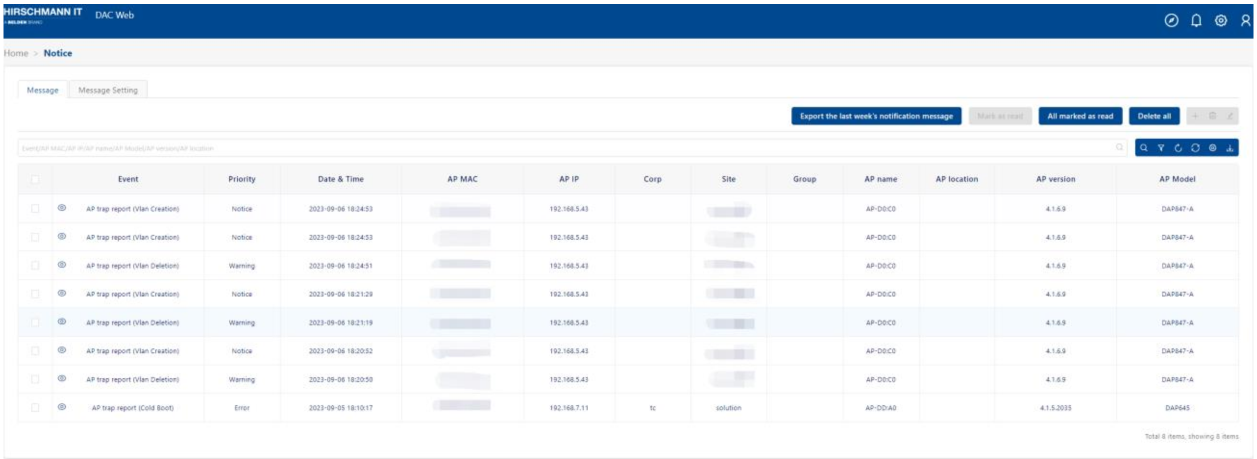
4 Fourth Step
To create your wireless network-SSID;

5 Last Step
To activate License that you purchased.

Figure 32: Wizard

▶ Notice

- Click to enter the message **notification** based on the user level.
- **Message:** Displays message notifications based on the account dimension.
- **Message Setting:** Configure whether to receive relevant messages or send email notifications for message options.



HIRSCHMANN IT
DAC Web
Home > Notice
Message
Message Setting
Export the last week's notification message
Mark as read
All marked as read
Delete all
Event/AP MAC/AP IP/AP name/AP Model/AP version/AP location

	Event	Priority	Date & Time	AP MAC	AP IP	Corp	Site	Group	AP name	AP location	AP version	AP Model
□	AP trap report (Vlan Creation)	Notice	2023-09-06 18:24:53	[redacted]	192.168.5.43		[redacted]		AP-D0:C0		4.1.6.9	DAP847-A
□	AP trap report (Vlan Creation)	Notice	2023-09-06 18:24:53	[redacted]	192.168.5.43		[redacted]		AP-D0:C0		4.1.6.9	DAP847-A
□	AP trap report (Vlan Deletion)	Warning	2023-09-06 18:24:51	[redacted]	192.168.5.43		[redacted]		AP-D0:C0		4.1.6.9	DAP847-A
□	AP trap report (Vlan Creation)	Notice	2023-09-06 18:21:29	[redacted]	192.168.5.43		[redacted]		AP-D0:C0		4.1.6.9	DAP847-A
□	AP trap report (Vlan Deletion)	Warning	2023-09-06 18:21:19	[redacted]	192.168.5.43		[redacted]		AP-D0:C0		4.1.6.9	DAP847-A
□	AP trap report (Vlan Creation)	Notice	2023-09-06 18:20:52	[redacted]	192.168.5.43		[redacted]		AP-D0:C0		4.1.6.9	DAP847-A
□	AP trap report (Vlan Deletion)	Warning	2023-09-06 18:20:50	[redacted]	192.168.5.43		[redacted]		AP-D0:C0		4.1.6.9	DAP847-A
□	AP trap report (Cold Boot)	Error	2023-09-05 18:10:17	[redacted]	192.168.7.11	tc	solution		AP-DD:A0		4.1.5.2035	DAP645

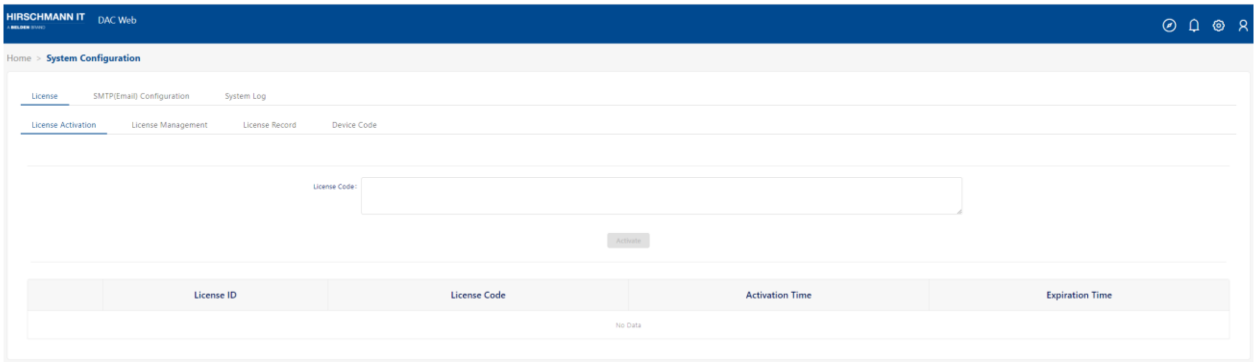
Total 8 items, showing 8 items

Figure 33: Notice

Note: If relevant messages are configured, the corresponding message information is generated only when 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** here.



License ID	License Code	Activation Time	Expiration Time

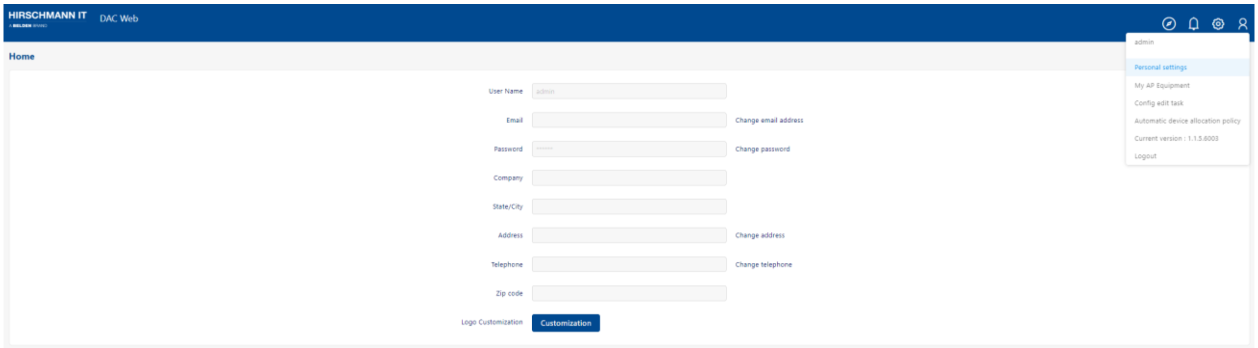
No Data

Figure 34: System Configuration

▶ Common Information

- **Personal settings:** Click to enter the personal information modification page. You can modify email, password, address, and telephone number.
- **My AP Equipment:** Click to enter my device page.

- **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 configure the binding policy of the subnet and the Site. The corresponding Site automatically assigns the AP.
- **Current version:** Click to view the DAC Release Note.
- **Logout:** Click to log out of the current account.



User Name: admin
Email:
Password: ******
Company:
State/City:
Address:
Telephone:
Zip code:
Logo Customization

Figure 35: Common Information

3.2 Configuration/Display icons

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

Configuration Icons/Buttons	
+	**Add** Click the **“Add”** icon to create a new entry within the configuration screen.
✎	**Edit** To edit an existing entry, select the entry in the configuration screen and click the **“Edit”** icon.
🗑	**Delete** To delete an entry, select the entry and click the **“Delete”** icon.
🧭	**Wizard** Click to quickly enter wizard mode. You can configure the relevant network structure and its corresponding license activation.
🔔	**Notice** Click to enter the message notification based on the user level.
⚙	**System Configuration** You can enter **License**, **SMTP (Email) Configuration**, and **System Log** from here.
👤	**Common Information** Quick access to personal configuration and its common functions.
?	**Help** Click the **“help”** button to load the corresponding prompt.

Table Icons/Buttons	
🔍	**Search** Click the **“Search”** button and enter search criteria in the "Search..." field to display specific entries in the table.
▽	**Filter** Users can check the corresponding filter field for the table to display specific data.
↻	**Reset** Click the **“Reset”** button after filtering a table to return to the original display.
🔄	**Refresh** The **“Refresh”** button loads the latest data for an application table, chart, or list.
⚙	**Settings** Used to configure the column headings to display in a table. Click the **“Settings”** button and select the column headings you want to display.

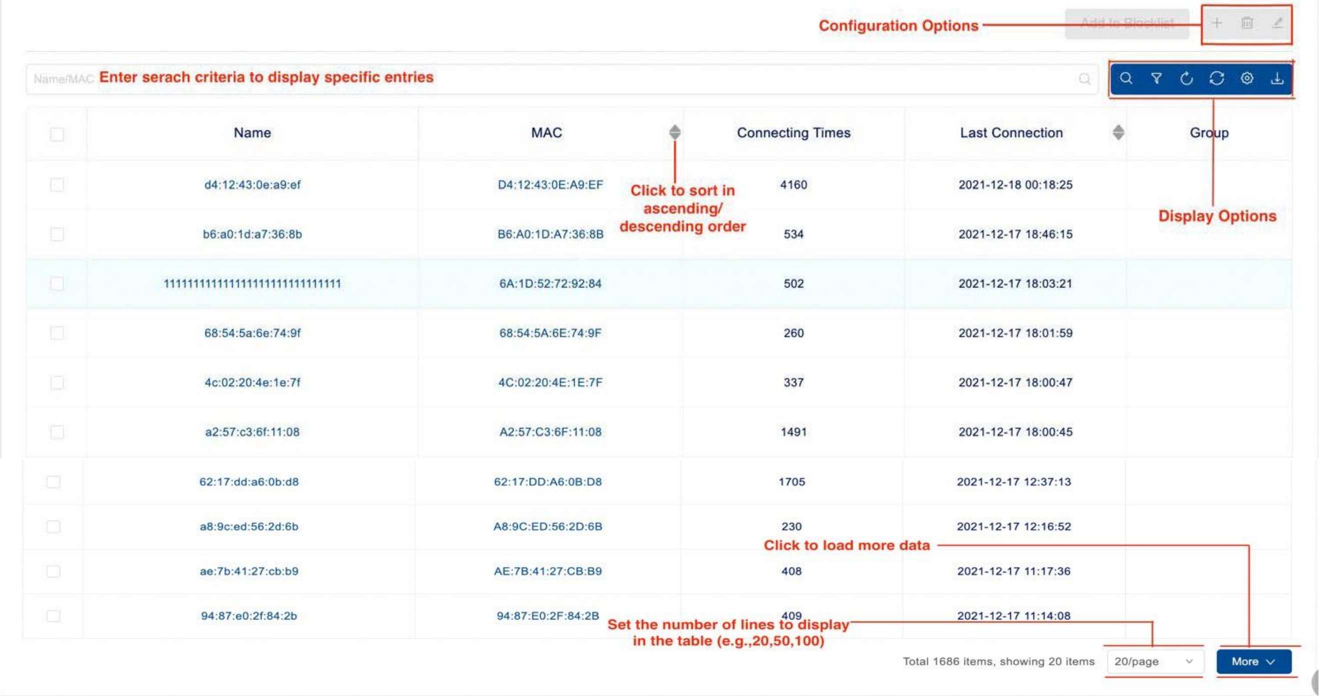
Table Icons/Buttons	
⤓	**Export to CSV** Click the **“CSV”** button to download the information displayed in Table View to a CSV (spreadsheet) file.
▲▼	**Sort** The information displayed in List View may be sorted in alphabetical order, either ascending or descending, by clicking the **“Sort”** button. You can also click 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.

Table 5: Configuration/display icons

3.3 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.


Configuration Options
Add to Blacklist
Name/MAC
Enter serach criteria to display specific entries
Click to sort in ascending/ descending order
Display Options
Click to load more data
Set the number of lines to display in the table (e.g.,20,50,100)
20/page
More

□	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	
□	111111111111111111111111111111	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	

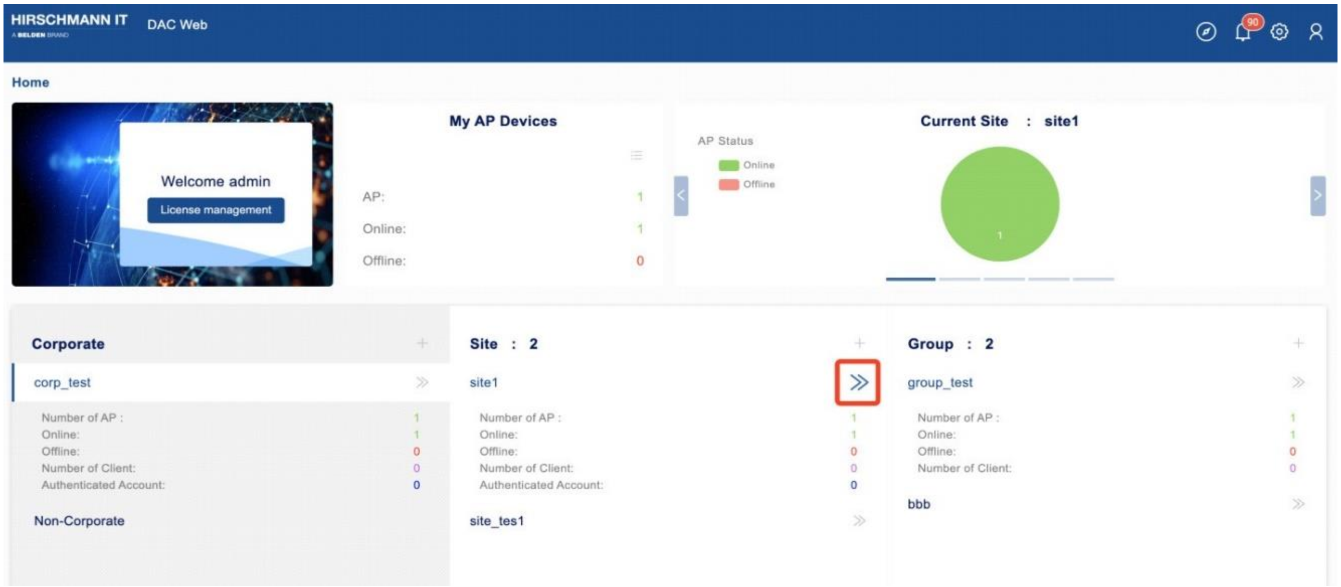
Total 1686 items, showing 20 items

Figure 36: DAC information in table format

- ▶ **Configuration Options:** Used to create, edit, and delete entries (e.g., create, edit, and 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, set the columns you want to display, and refresh the data in the table. Details for each button are provided in the Configuration/ Display icons section.
- ▶ **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 list at the bottom right corner of the page.

3.4 User home page

The user home page includes Corporate, Site, Group, Device list, License, and other information.



HIRSCHMANN IT
A BELDEN BRAND
DAC Web

Home

Welcome admin
License management

My AP Devices

AP: 1
Online: 1
Offline: 0

AP Status
🟩 Online
🟥 Offline

Current Site : site1

Corporate
corp_test
Number of AP : 1
Online: 1
Offline: 0
Number of Client: 0
Authenticated Account: 0
Non-Corporate

Site : 2
site1
Number of AP : 1
Online: 1
Offline: 0
Number of Client: 0
Authenticated Account: 0
site_tes1

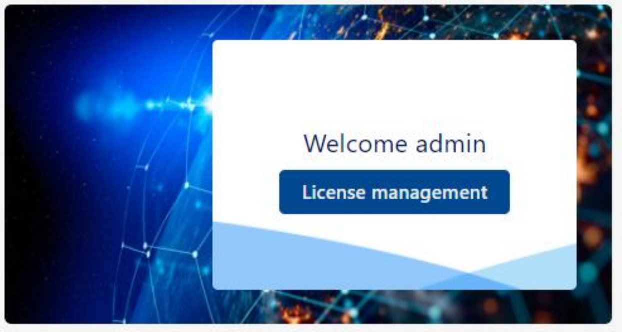
Group : 2
group_test
Number of AP : 1
Online: 1
Offline: 0
Number of Client: 0
bbb

Figure 37: User home page

3.4.1 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 for **"License management"** function.

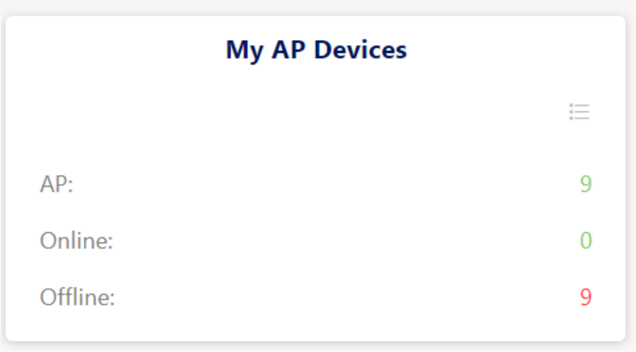


Welcome admin
License management

Figure 38: 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 to quickly enter the My Device screen.



My AP Devices

AP: 9

Online: 0

Offline: 9

Figure 39: My AP Devices

- ▶ **Current Site:**

- **AP Status:** Pie Chart of AP Status (Online or Offline Number).

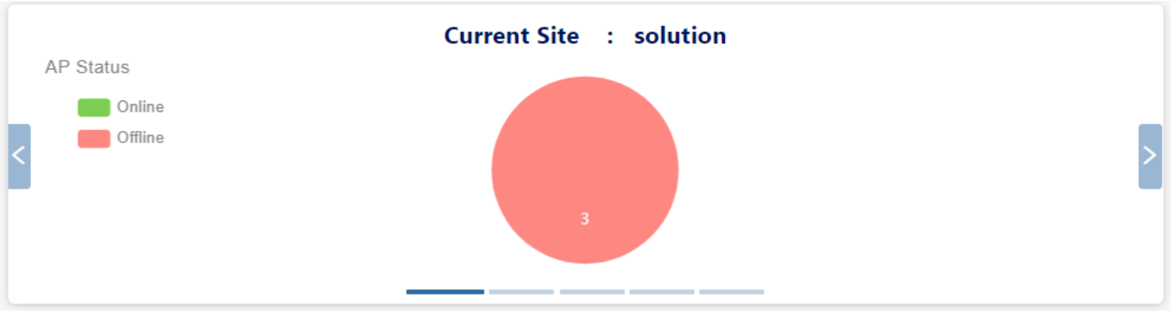


Figure 40: Current Site - AP Status

- **AP Model:** Model and quantity of AP device.

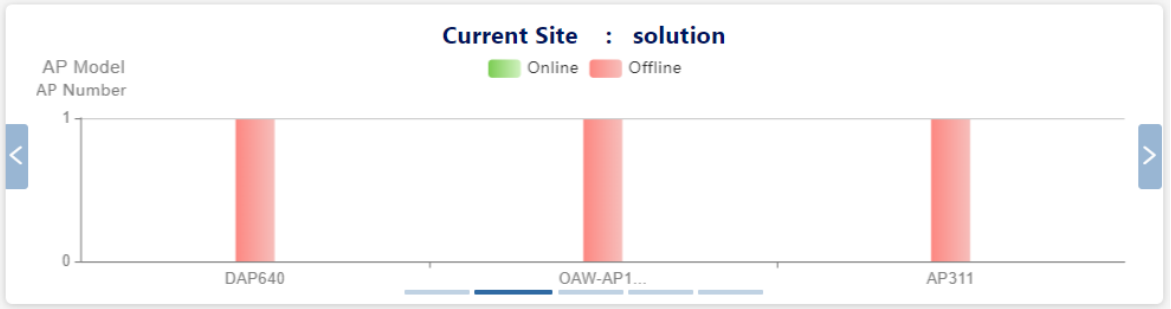


Figure 41: Current Site - AP Model and AP Number

- **Client Number:** Statistics of clients.

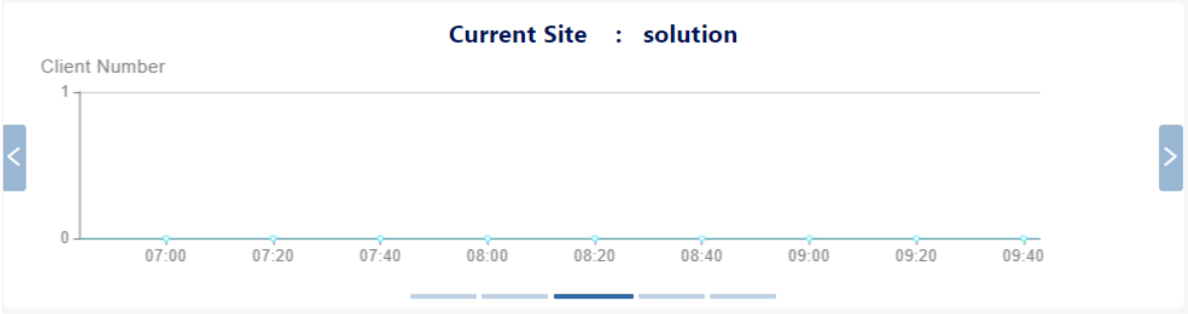


Figure 42: Current Site - Client Number

- **Throughput:** Line chart of bandwidth.

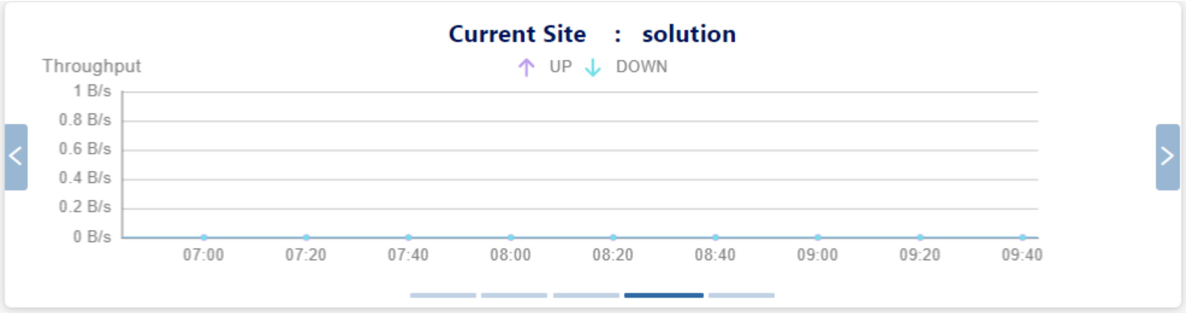


Figure 43: Current Site - Throughput

- **Total Traffic:** Flow Histogram of Traffic.

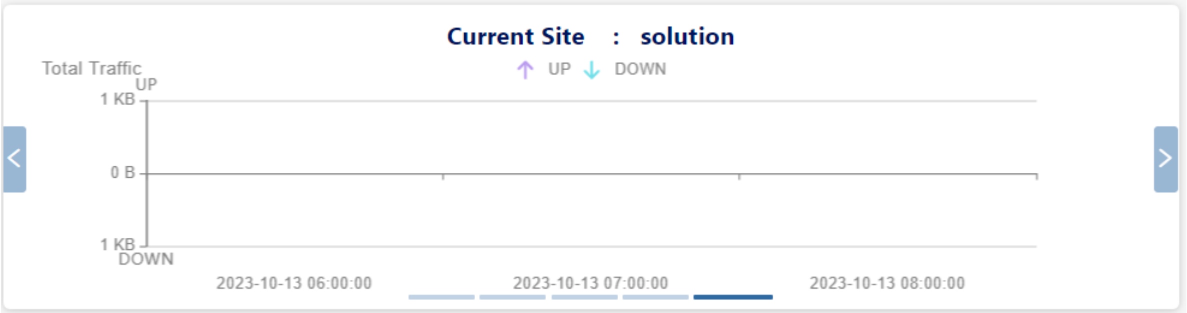


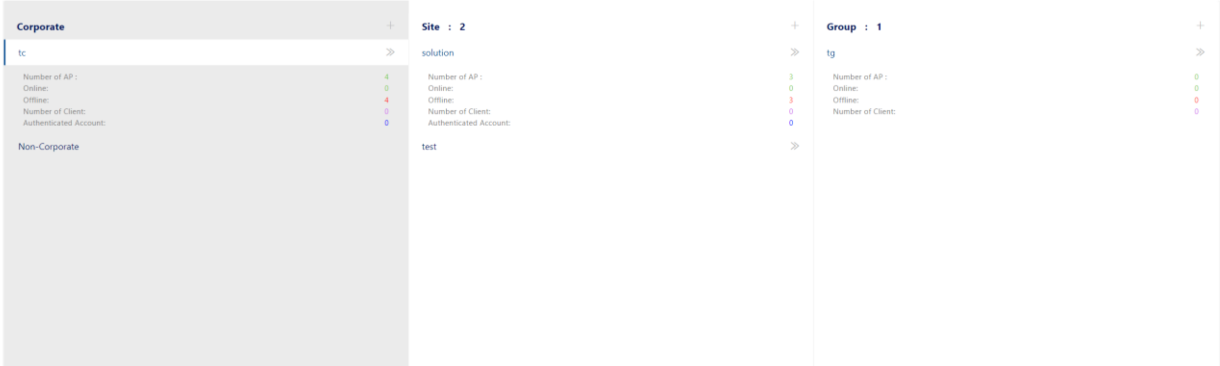
Figure 44: Current Site - Total Traffic

▶ **Network structure**:

The customer network structure panel is divided into:

- Corporate
- Site
- Group

The three-tier network structure adopts the progressive display method in its design. If the customer has more than one Corporate or Site, the corresponding Site or Group will be displayed when clicking **“Corporate”** or **“Site”**.



Corporate

tc

Number of AP : 4
Online: 0
Offline: 4
Number of Client: 0
Authenticated Account: 0

Non-Corporate

Site : 2

solution

Number of AP : 3
Online: 0
Offline: 3
Number of Client: 0
Authenticated Account: 0

test

Group : 1

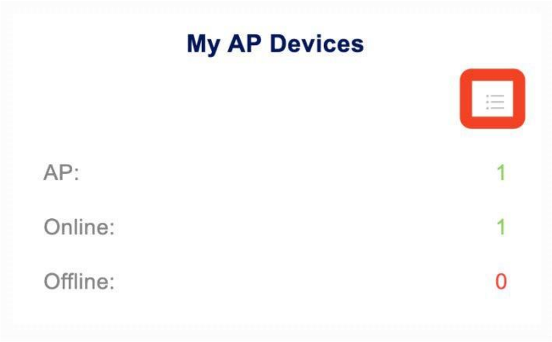
tg

Number of AP : 0
Online: 0
Offline: 0
Number of Client: 0

Figure 45: Network Structure

3.4.2 My device

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



My AP Devices

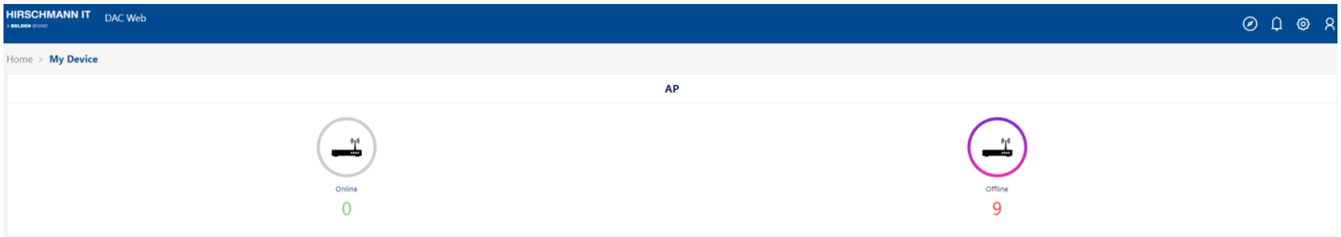
AP: 1

Online: 1

Offline: 0

Figure 46: My device panel

On the **My Device** screen, the top prominent positions are **“count of online APs (green number)”** and **“count of offline APs (red number)”**.



Online
0

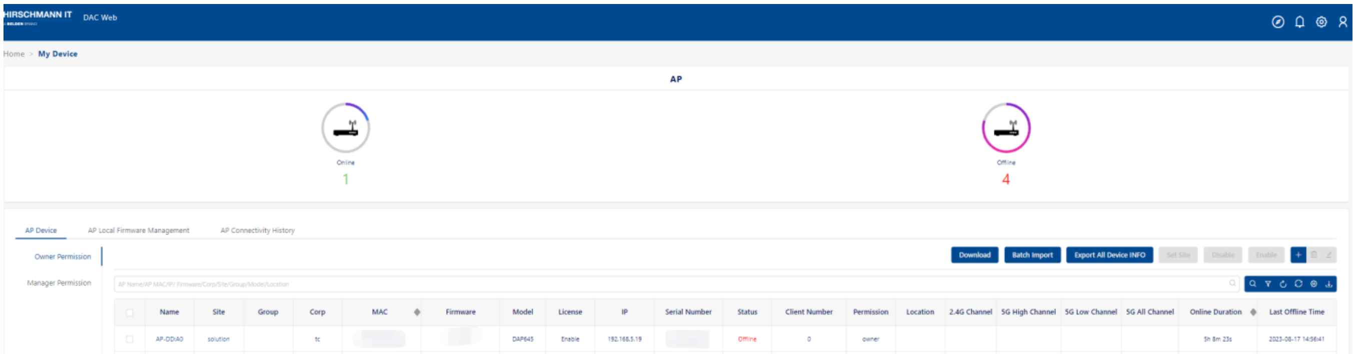
Offline
9

Figure 47: My Device screen

3.4.3 AP device

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

- **Name:** AP device name. You can change the name of the AP to find it quickly. Click it to enter the AP detail view.
- **Site:** The Site that AP belongs to. Click it to enter the Site view.
- **Group:** The Group that AP was assigned to. Click it to enter Group view.
- **Corp:** The Corp that AP belongs to.
- **MAC:** The MAC Address of the AP.
- **Firmware:** Firmware version of AP.
- **Model:** Hardware type of AP.
- **License:** License Status of AP can enable or disable. If license is disabled, AP will not broadcast the SSID.
- **IP:** IP Address of the AP.
- **Serial Number:** Serial Number of the AP.
- **Status:** Online or offline status of AP.
- **Client Number:** Number of clients on AP currently.
- **Permission:** The managing permission to AP of the current user.
- **Location:** Location of the AP device.
- **2.4G Channel:** The 2.4G channel used for DAP.
- **5G High Channel:** The high band 5G is used for DAP.
- **5G Low Channel:** The low band 5G is used for DAP.
- **5G All Channel:** The 5G channel used for DAP.
- **Online Duration:** The duration of DAP connects to DAC.
- **Last Offline Time:** The latest time of the DAP latest disconnect from the DAC.

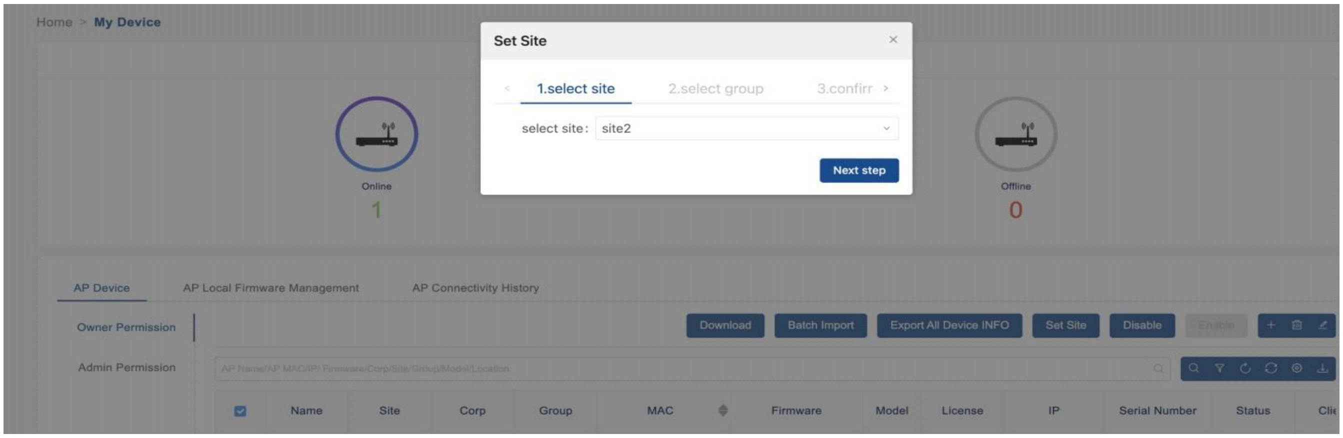


	Name	Site	Group	Corp	MAC	Firmware	Model	License	IP	Serial Number	Status	Client Number	Permission	Location	2.4G Channel	5G High Channel	5G Low Channel	5G All Channel	Online Duration	Last Offline Time
□	AP-DD:A0	solution		tc	[redacted]	[redacted]	DAP645	Enable	192.168.5.19	[redacted]	Offline	0	owner						5h 8m 23s	2023-08-17 14:56:41

Figure 48: AP Devices List

3.4.4 Assigning DAPs to a Site or a Group

- ☐ Go to **Home** → **My Device** Page. Click the **“AP Device”** tab.
- ☐ Select the APs that you want to assign to the Site or Group.
- ☐ Click the **“Set Site”** button.
- ☐ Click the **“Yes”** button on the confirmation prompt. The **“Set Site”** screen appears.
- ☐ Select a Site from the drop-down list and click the **“Next step”** button.
- ☐ Select a Group or do not set Group and click the **“Next step”** button.
- ☐ Click the “Save” button to confirm the information.



select site : site2

Figure 49: Set Site screen

3.4.5 AP local firmware management

- ☐ Go to **Home** → **My Device** Page and click the **“AP Local Firmware Management”** tab to manage local AP firmware.

  Usually, the DAC downloads the firmware of the AP from the cloud. However, in some cases, we need to import the firmware of the DAP from the DAC management page. The imported firmware is a compressed package that you can get from your supplier.

- □ Click the **“+”** icon to open the **“Upload”** window.
- □ Click the **“Upload”** button and select the AP firmware package you obtained from the vendor. The uploaded file appears in the list.
  - ▶ **Firmware Version**: Version of the DAP Firmware.
  - ▶ **Firmware Description**: Firmware Description.
  - ▶ **Upload Time:** Time taken to upload the firmware.

And then, you can upgrade the firmware of AP devices on the AP device list page of Site view. See “Firmware upgrade” on page 111 .

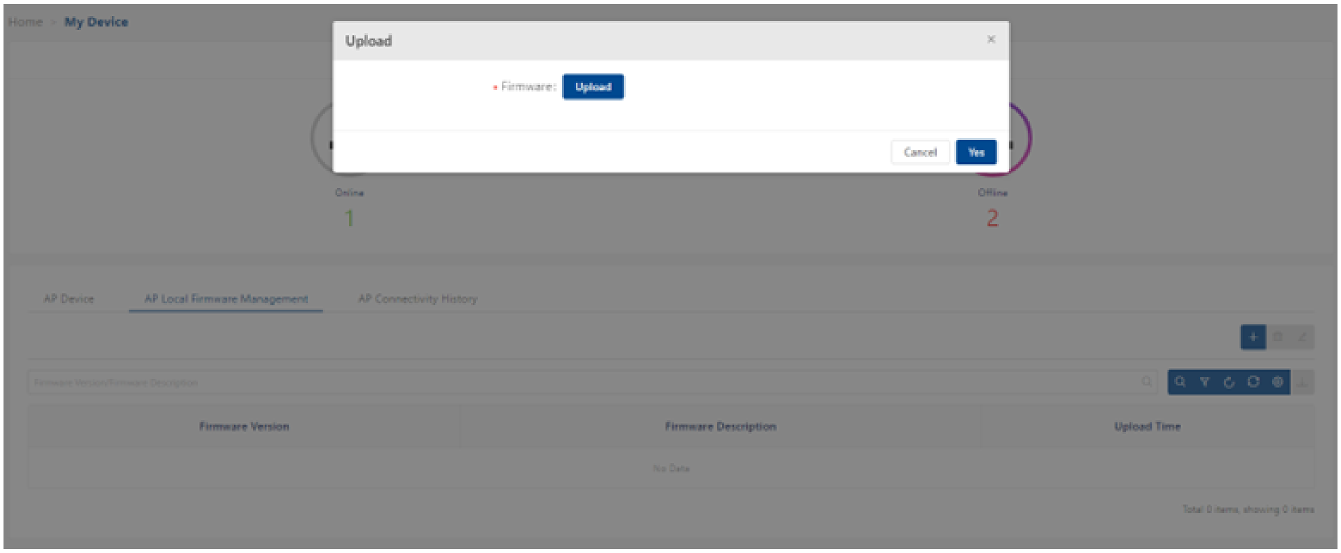
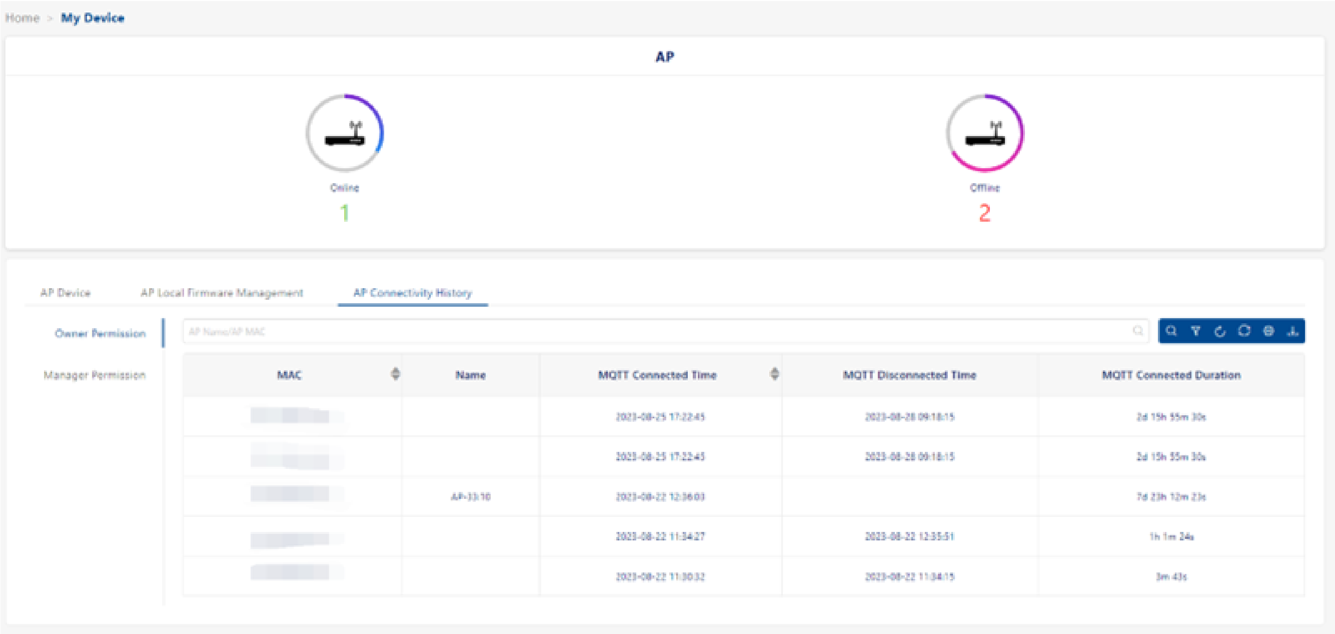


Figure 50: AP Local Firmware Management

3.4.6 AP connectivity history

AP connects and disconnects records.

- ▶ **MAC:** MAC Address of the AP device.
- ▶ **Name:** Name of the AP device.
- ▶ **MQTT Connected Time:** MQTT connect time of the AP device.
- ▶ **MQTT Disconnected Time:** MQTT disconnect time of the AP device.
- ▶ **MQTT Connected Duration:** MQTT connection duration of the AP device.



MAC	Name	MQTT Connected Time	MQTT Disconnected Time	MQTT Connected Duration
[redacted]		2023-08-25 17:22:45	2023-08-28 09:18:15	2d 15h 55m 30s
[redacted]		2023-08-25 17:22:45	2023-08-28 09:18:15	2d 15h 55m 30s
[redacted]	AP-33:10	2023-08-22 12:36:03		7d 23h 12m 23s
[redacted]		2023-08-22 11:34:27	2023-08-22 12:35:51	1h 1m 24s
[redacted]		2023-08-22 11:30:32	2023-08-22 11:34:15	3m 43s

Figure 51: AP Connectivity History

3.5 Site view

Click **"Site"** on the Home Page to view the Site information.

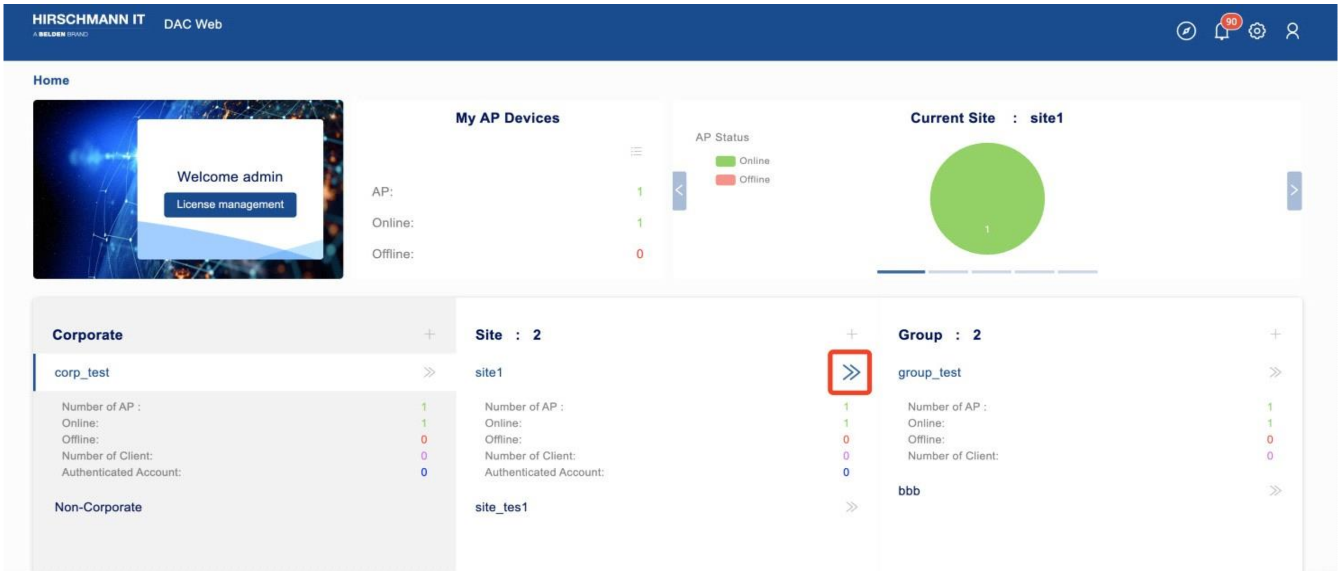


Figure 52: Home page

In Site view, you can see the tabs Dashboard, WLAN, AP, Clients, Authentication, RF, Log, Security, Group, and Setting.

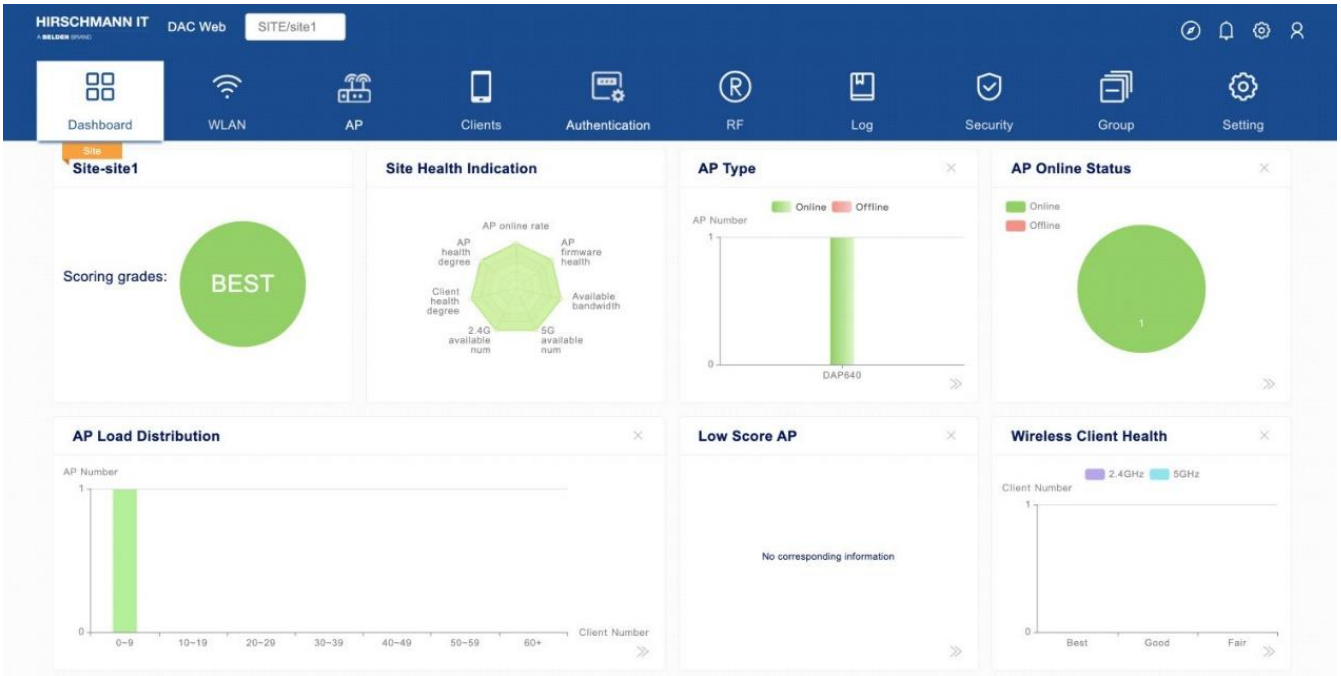
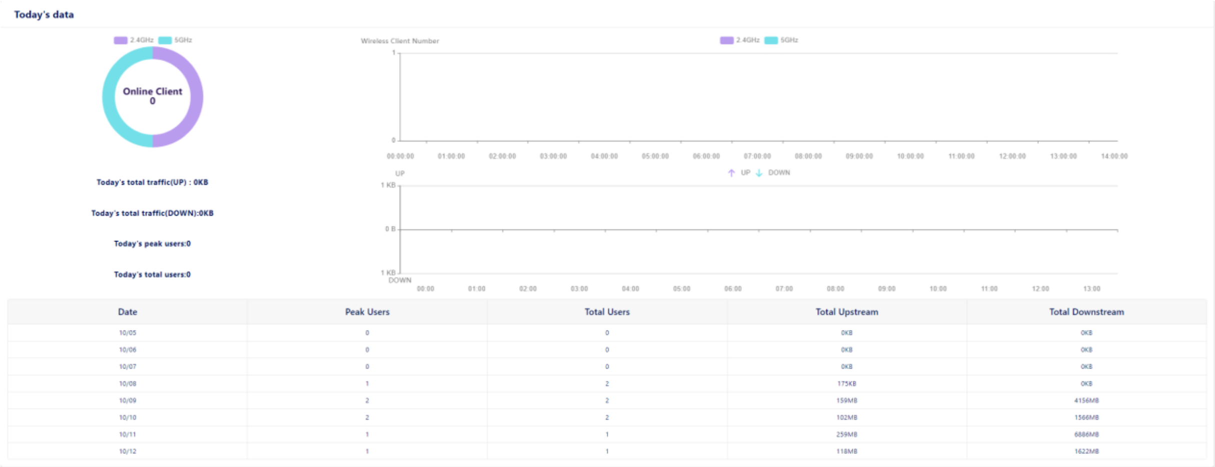


Figure 53: Site view page

3.5.1 Dashboard

- **Today's data:** Display the current number of real-time terminals, the number of historical terminals for the day and traffic, the peak number of users counted by day within the past 8 days, cumulative users, uplink traffic statistics, and downlink traffic statistics.



Today's data

Today's total traffic(UP) : 0KB

Today's total traffic(DOWN):0KB

Today's peak users:0

Today's total users:0

Date	Peak Users	Total Users	Total Upstream	Total Downstream
10/05	0	0	0KB	0KB
10/06	0	0	0KB	0KB
10/07	0	0	0KB	0KB
10/08	1	2	175KB	0KB
10/09	2	2	159MB	4156MB
10/10	2	2	102MB	1566MB
10/11	1	1	259MB	6886MB
10/12	1	1	118MB	1622MB

Figure 54: Site Dashboard - Today’s data

- **Scoring grades:** Show the current Site health level (best, good, fair, or N/A).

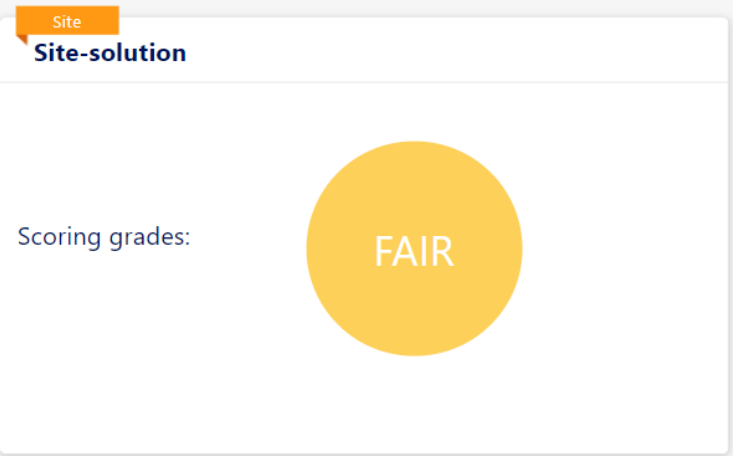


Figure 55: Site Dashboard - Scoring grades

- **Site Health Indication:** Display the specific health level details of all AP, terminal, or bandwidth dimensions of the current field. The health level can be divided into three grades: best, good, and fair.
  - **AP online rate:** Determined by the percentage of online APs to all APs in the site.

    Best: percentage>80%; Good: 60%<percentage<80%;

Fair: percentage<60%

- **AP firmware health:**

  Best: when all APs in the site are the latest version.

  Good: when all the AP versions in the site are the same but not the latest.

  Fair: when the AP versions in the site are different.

- **Available bandwidth:** Determined by the ratio of the average available bandwidth to the total bandwidth of each AP in the site.

  Best: ratio>80%; Good: 60%<ratio<80%; Fair: ratio<60%

- **5G available num:** Determined by the average number of clients in the 5G band of online APs in the site.

  Best: average<8; Good: 8<average<16; Fair: average>16

- **2.4G available num:** Determined by the average number of clients in the 2.4G band of online APs in the site.

  Best: average<8; Good: 8<average<16; Fair: average>16

- **Client health degree:** Determined by the percentage of health clients to all clients in the site.

  Best: percentage>80%; Good: 60%<percentage<80%;

  Fair: percentage<60%

  Note: Whether a client is a healthy client is determined by its RSSI.

- **AP health degree:** Determined by the average CPU usage of the online AP in the site.

  Best: average<20%; Good: 20%<average<40%;

  Fair: average>40%

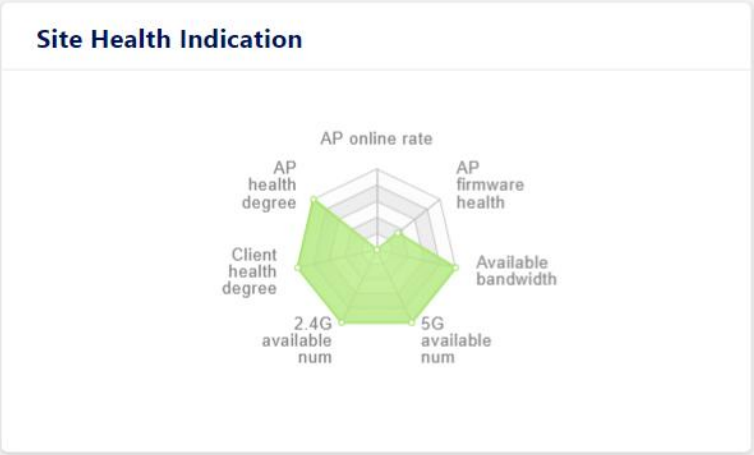


Figure 56: Site Dashboard - Site Health Indication

- **AP Type:** The specific model of AP and the corresponding histogram of the number of this model in the **“Site”**. The horizontal axis represents the AP model, and the vertical axis represents the number of corresponding models.

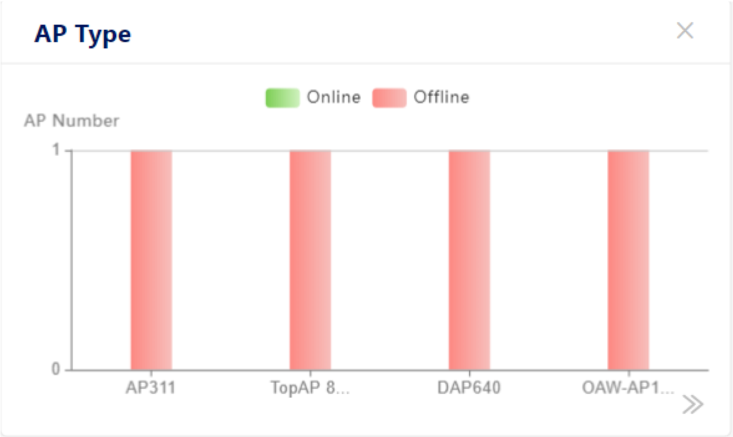


Figure 57: Site Dashboard - AP Type

- **AP Online Status:** Pie chart percentage of AP online and offline.

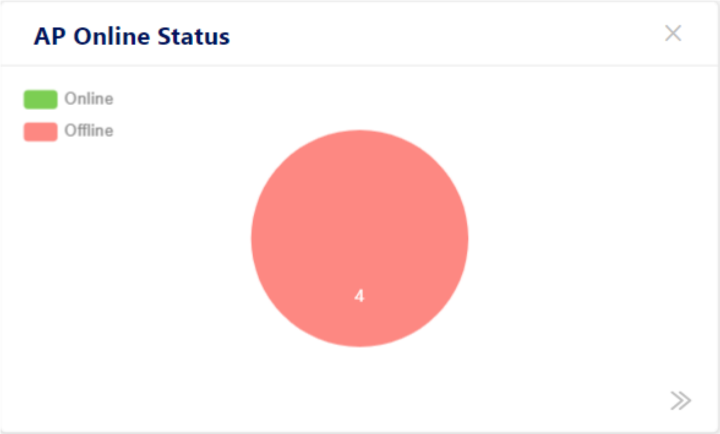


Figure 58: Site Dashboard - AP Online Status

- **AP Load Distribution:** Load balance in AP. A bar chart depicts the number of connected terminals in a site of different APs.
  - The number of connected terminals of APs is divided into 7 ranges and plotted on the horizontal axis, which are: 0-9, 10-19, 20-29, 30-39, 40-49, 50-59, 60+.
  - The vertical axis represents the number of APs corresponding to the number of connected terminals.

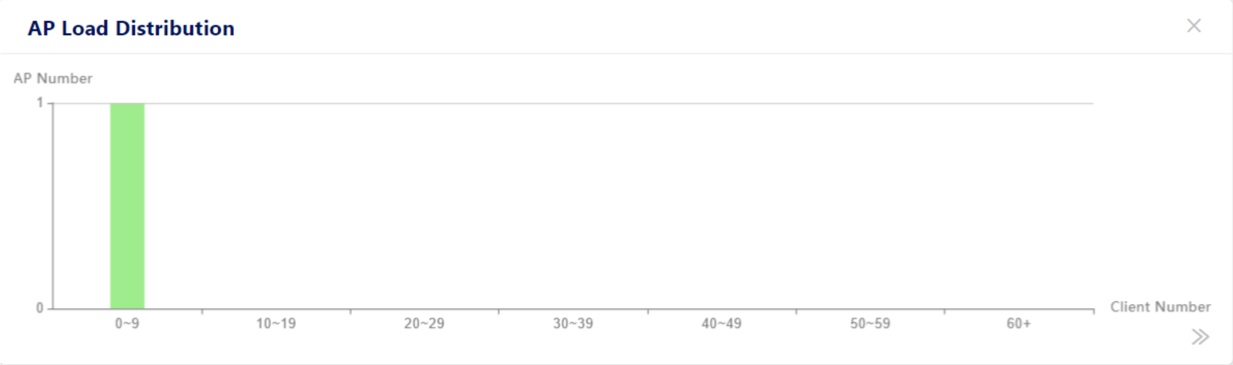
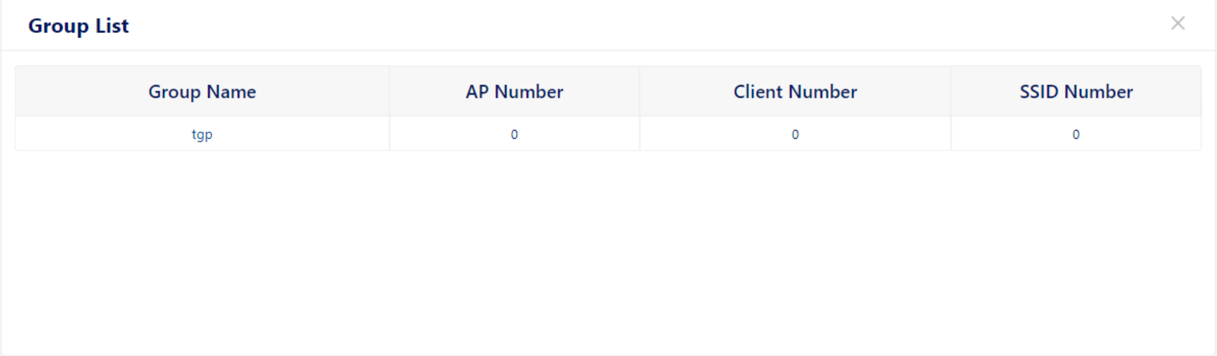


Figure 59: Site Dashboard - AP Load Distribution

- **Low Score AP:** Provide a list of APs whose scores are lower than the threshold standard. Remind customers to focus on the specific operation status and version information of APs. The AP list in the low-split AP tab is dynamic. If the AP indicators do not meet the threshold requirements, the AP is displayed in the tab. Customers can click directly to 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 automatically disappears from the tab.

  AP threshold indicators are judged by the following 5 aspects:
  - AP CPU utilization
  - AP memory utilization
  - AP flash memory utilization
  - Number of terminal accesses
  - AP used bandwidth

- **Group List:** Show the list of groups under the Site.
  - **Group Name:** Names of all groups included in the Site**.** You can click the name to enter the **"Group"** view.
  - **AP Number:** Count of APs in the Group.
  - **Client Number:** Count of clients in the Group.
  - **SSID Number:** Count of SSIDs created in the Group.

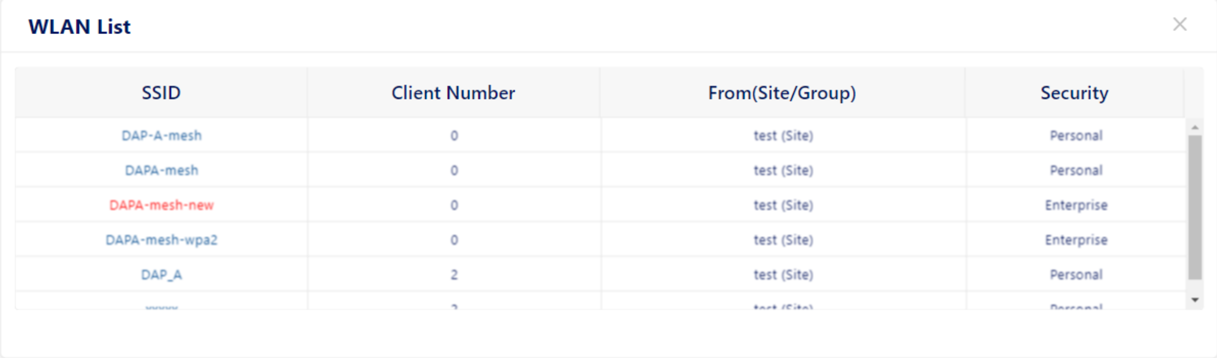


Group List

Group Name	AP Number	Client Number	SSID Number
tgp	0	0	0

Figure 60: Site Dashboard - Group List

- **WLAN List:** Show the SSID list on the Site.
  - **SSID:** SSID name of a wireless network
  - **Client Number:** Client Count associated with the SSID
  - **From(Site/Group):** Site or Group, which means the SSID is created from the Site or Group.
  - **Security:** Wireless security levels, can be Open, Personal, or Enterprise.



WLAN List

SSID	Client Number	From(Site/Group)	Security
DAP-A-mesh	0	test (Site)	Personal
DAPA-mesh	0	test (Site)	Personal
DAPA-mesh-new	0	test (Site)	Enterprise
DAPA-mesh-wpa2	0	test (Site)	Enterprise
DAP_A	2	test (Site)	Personal

Figure 61: Site Dashboard - WLAN List

- **Wireless Client Health:** In the tab of terminal health, according to the signal strength (RSSI stands for Received Signals Strength Indicators) of the terminal signal uplink to the AP, we provide 3 levels of access health:
  - The terminal meeting the best RSSI threshold is classified as **“best”** level.
  - The terminal meeting the good RSSI threshold is classified as **“good”** level.
  - 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.

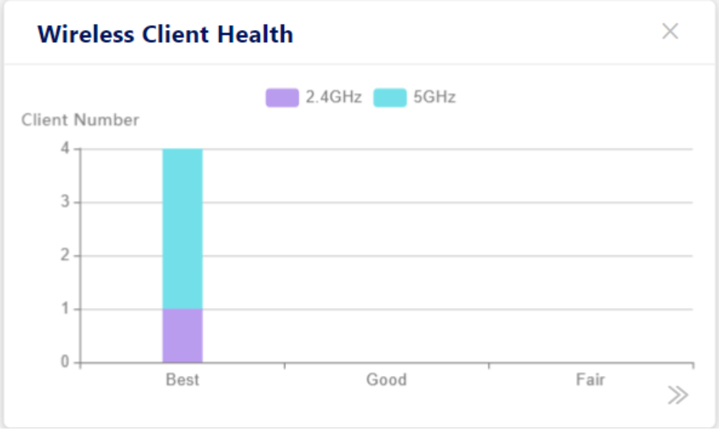


Figure 62: Site Dashboard - Wireless Client Health

- **Client Type:** The current hardware types of access terminals include computers, mobile devices, and others.

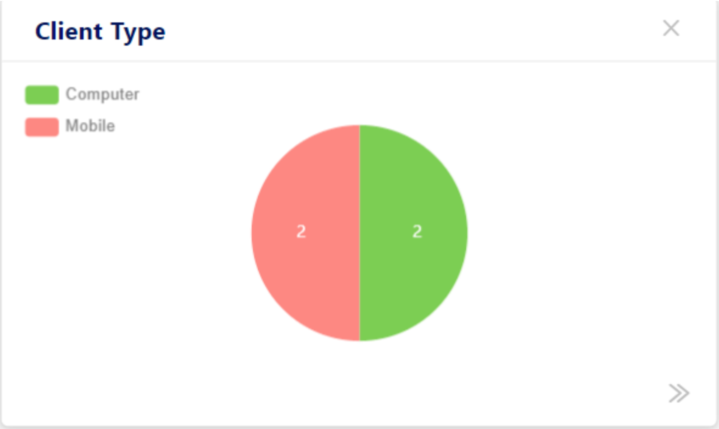


Figure 63: Site Dashboard - Client Type

- **Operating System:** The operating system type of the access terminal is intuitively given in the form of a pie chart.

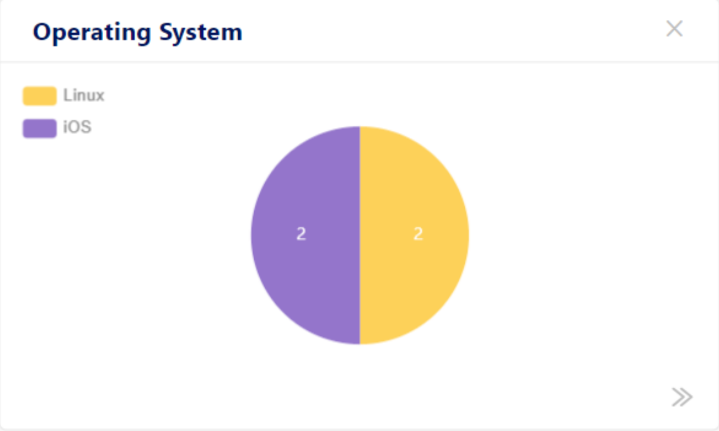
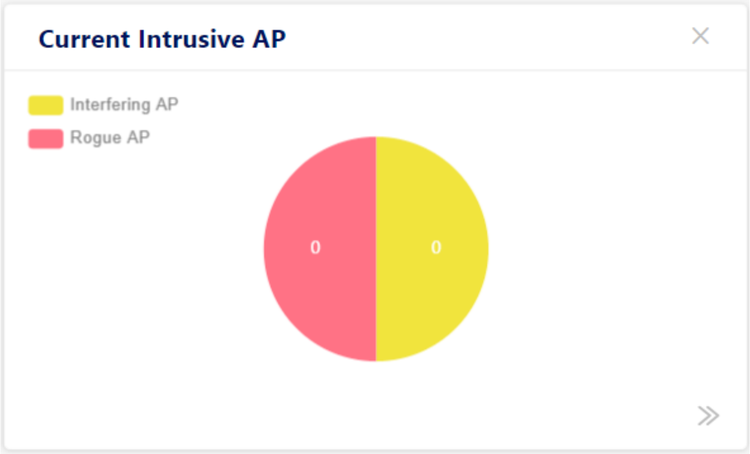


Figure 64: Site Dashboard - Operation System

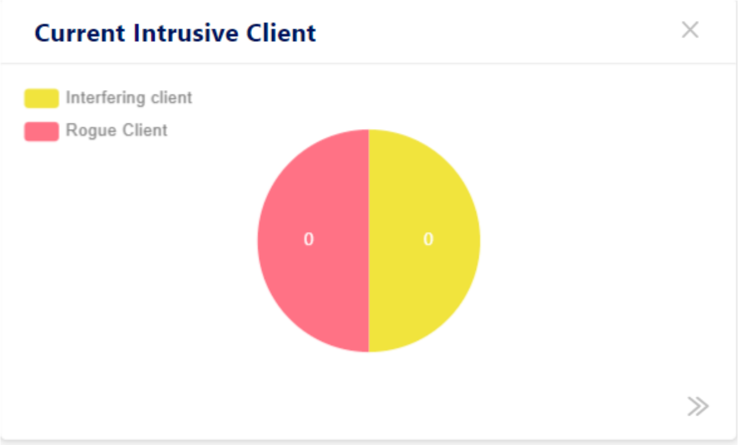
- **Current Intrusive AP:** Show the proportion of interference AP and Rogue AP in the form of a pie chart.


Current Intrusive AP

🟨 Interfering AP
🟥 Rogue AP

Figure 65: Site Dashboard - Current Intrusive AP

- **Current Intrusive Client:** Show the proportion of interference client and Rogue client in the form of a pie chart.


Current Intrusive Client

🟨 Interfering client
🟥 Rogue Client

Figure 66: Site Dashboard - Current Intrusive Client

- **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 for the Site
  - **Traffic:** Histogram of Traffic

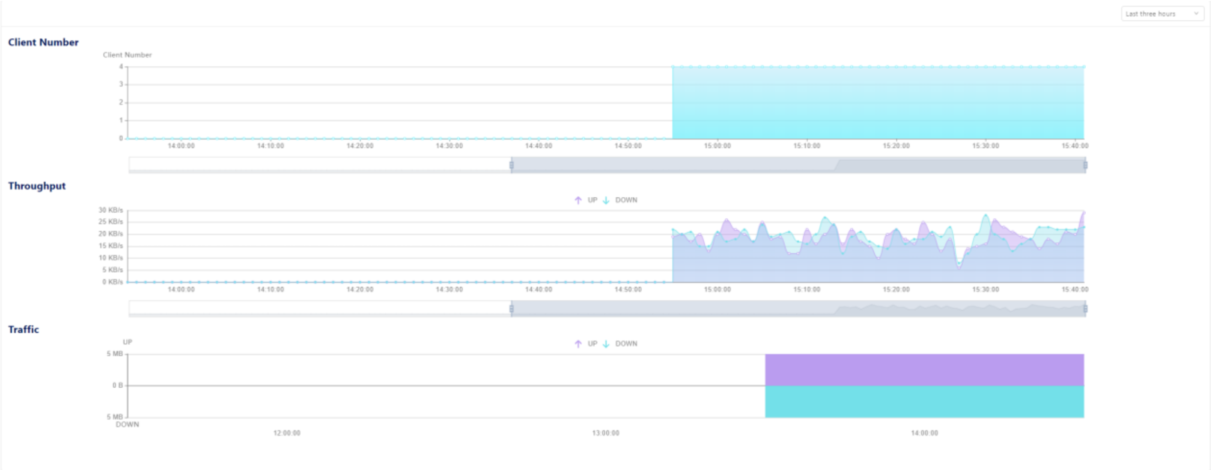


Figure 67: Site Dashboard – Historical Statistics

3.5.2 WLAN

Create, modify, and delete SSIDs for the Site. See "WLAN" on page 87.

3.5.3 AP

Provide management and monitoring of the 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" on page 106.

3.5.4 Clients

Provide terminal management and monitoring. Management includes Blocklist processing for terminals with abnormal behavior. Monitoring includes type statistics of terminals, OS type statistics, and queries of various parameters of terminals attached to the network. See "Clients" on page 131.

3.5.5 Authentication

Create, modify, and delete authentication and other related policy configurations. See "Authentication" on page 139.

3.5.6 RF

Show the AP RF configuration. Set the RF configuration based on the Site. Set the RF configuration based on a single AP (with a higher priority than the Site configuration). See “RF” on page 211.

3.5.7 Log

Log of the system or log of the device. See “Log” on page 224.

3.5.8 Security

Configure the Rogue AP strategy and wireless attack detection strategy. The wireless attack detection strategy includes an AP attack detection strategy, a terminal attack detection strategy, and a Blocklist strategy. Statistics of illegal AP records, including interference AP, Rogue AP, attack AP, and invalid AP. Statistics of jamming terminal records include terminals associated with jamming AP, terminals associated with Rogue AP, terminals detected by the terminal attack, and terminals that entered Blocklist. Attack ranking statistics are available. See “Security” on page 231.

3.5.9 Group

The entrance of the Group belonging to the Site. You can see all Group on this Site, and each Group is shown on a card.

- **Scoring Grades:** Show the Group health level (best, good, fair, or N/A).
- **Health:** Display the specific health level details of all AP, terminal, and bandwidth dimensions of the current field.
- **AP:** Online and offline numbers.

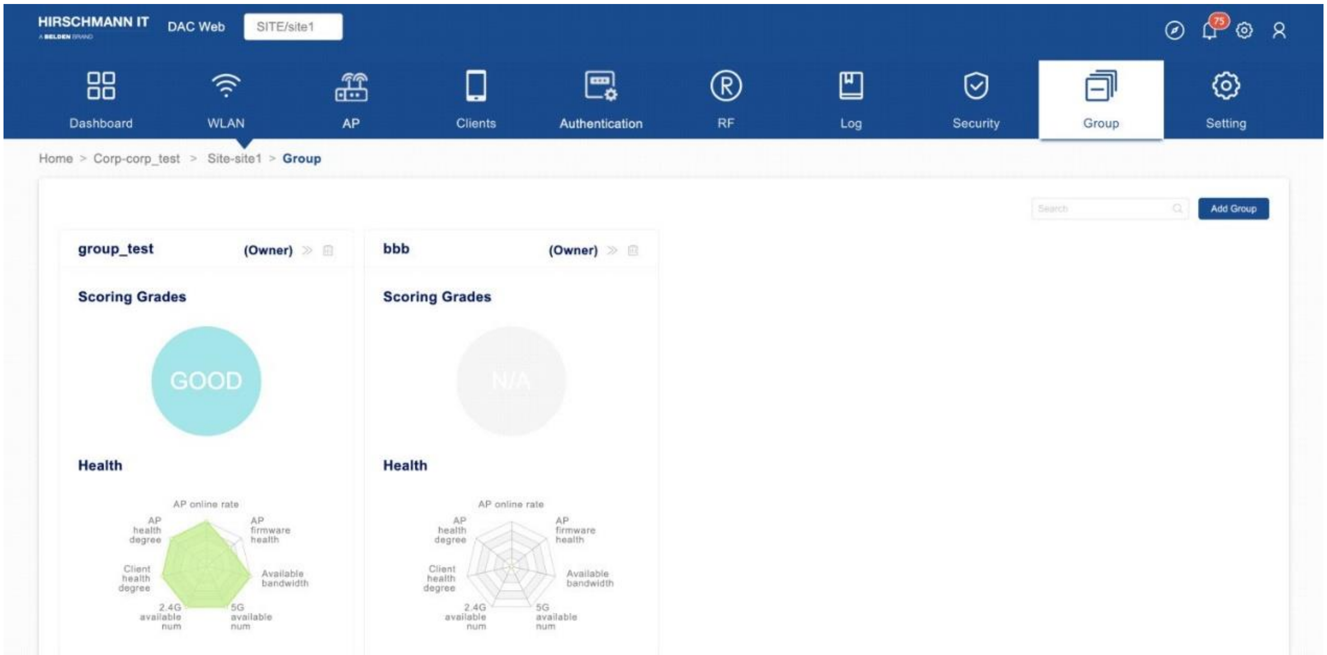


Figure 68: Group window

■ **Create A Group**

☐ Click the **“Add Group”** button. The **“Create Group”** window appears.

☐ Specify the **“Name”** and **“Description”**.

☐ Click the **“Save”** button to save the Group. You can see the new Group added on the Group page.

■ **Delete A Group**

☐ Click the **Delete** icon in the Group card.

☐ Click the **“Yes”** button on the confirmation prompt.

3.5.10 Setting

It shows the settings of the Site.

■ **Basic information/setting**

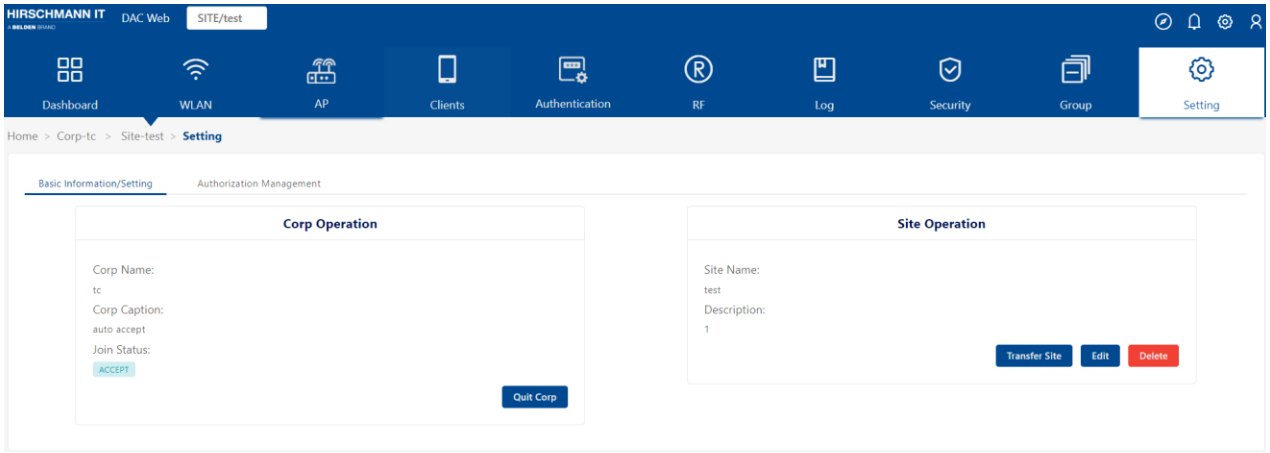
▶ **Corporate Operation:** Display after assigning the Site to a Corporate.

- **Quit Corp:** Remove the current Site from Corporate.

▶ **Site Operation:**

- **Transfer Site:** Transfer Site owner permissions to other users.

- **Edit:** Change the Site **“Name”** or **“Description”**.
- **Delete:** Delete the Site.
- **Join Corporate:** Assign the Site to a Corporate.



Corp Operation

Corp Name:
tc
Corp Caption:
auto accept
Join Status:
ACCEPT

Site Operation

Site Name:
test
Description:
1

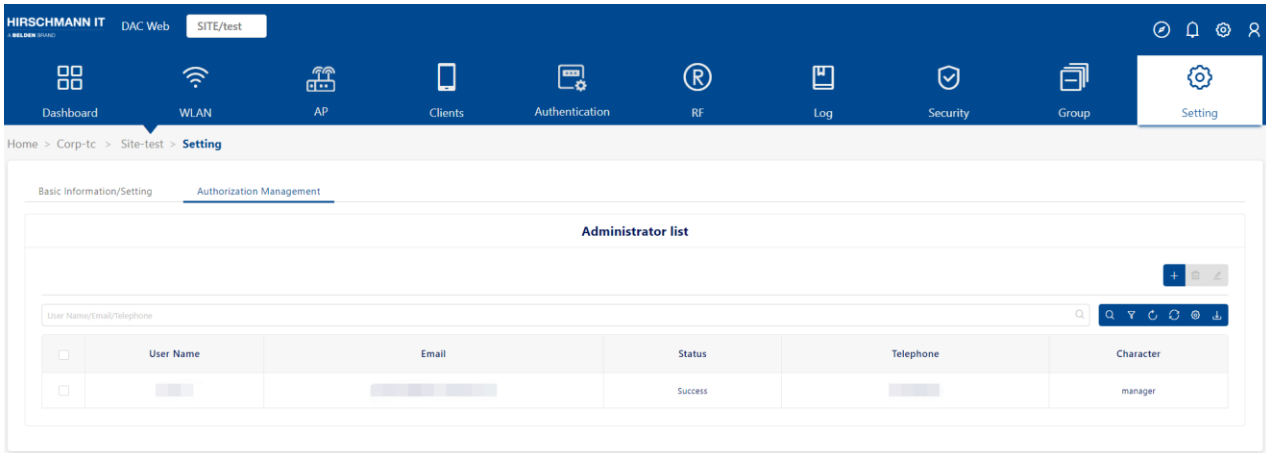
Figure 69: Site Setting window

■ Authorization management

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

▶ Administrator list

- **User Name:** User Name
- **Email:** Email
- **Status:** success/fail
- **Telephone:** The telephone of the user.
- **Character:** Character can be Manager, Viewer, or Guest Operator.



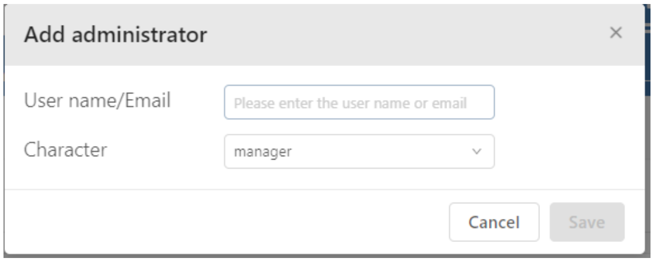
Administrator list

☐	User Name	Email	Status	Telephone	Character
☐	[redacted]	[redacted]	Success	[redacted]	manager

Figure 70: Authorization Management window

■ Add Administrator

□ Click the **“+”** icon. The **“Add administrator”** dialog opens.
□ Enter the **“User name”** or **“Email”** that you want to add.
□ Select **“Character”** from the drop-down list (Manager, Viewer, or Guest Operator).
□ Click the **“Save”** button to apply the settings.



User name/Email: Please enter the user name or email

Character: manager

Figure 71: Add Administrator window

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 has the corresponding permissions for the current Site. See “Create account” on page 33.

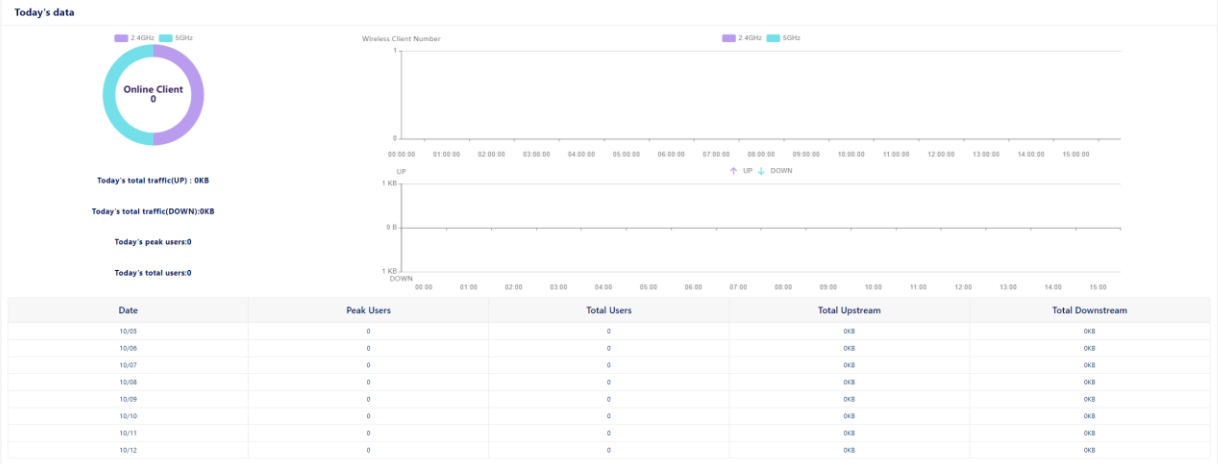
■ Delete Administrator

□ Select the administrator you want to delete.
□ Click the **“Delete”** icon.
□ Click the **“Yes”** button on the confirmation prompt.

3.6 Group view

3.6.1 Dashboard

- **Today's data:** Display the current number of real-time terminals, the number of historical terminals for the day and traffic, the peak number of users counted by day within the past 8 days, cumulative users, uplink traffic statistics, and downlink traffic statistics.



Today's data

Today's total traffic(UP) : 0KB

Today's total traffic(DOWN):0KB

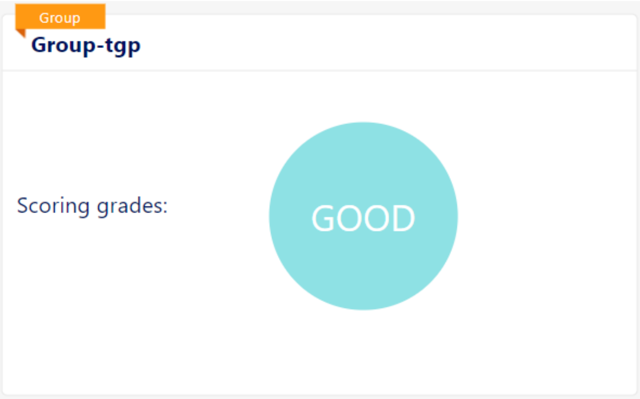
Today's peak users:0

Today's total users:0

Date	Peak Users	Total Users	Total Upstream	Total Downstream
10/05	0	0	0KB	0KB
10/06	0	0	0KB	0KB
10/07	0	0	0KB	0KB
10/08	0	0	0KB	0KB
10/09	0	0	0KB	0KB
10/10	0	0	0KB	0KB
10/11	0	0	0KB	0KB
10/12	0	0	0KB	0KB

Figure 72: Group Dashboard - Today’s data

- **Scoring grades:** Show the current Group health level (best, good, fair, or N/A).



Group-tgp

Scoring grades: GOOD

Figure 73: Group Dashboard – Scoring grades

- **Group Health Indication:** Display the specific health level details of all AP, terminal, or bandwidth dimensions of the current field. The health level can be divided into three grades: best, good, and fair.
  - **AP online rate:** Determined by the percentage of online APs to all APs in the group.

Best: percentage>80%; Good: 60%<percentage<80%;

Fair: percentage<60%

- **AP firmware health:**

  Best: when all the APs in the group are the latest version.

  Good: when the AP versions in the group are the same but not the latest.

  Fair: when the AP versions in the group are different.

- **Available bandwidth:** Determined by the ratio of the average available bandwidth to the total bandwidth of each AP in the group.

  Best: ratio>80%; Good: 60%<ratio<80%; Fair: ratio<60%

- **5G available num:** Determined by the average number of clients in the 5G band of online APs in the group.

  Best: average<8; Good: 8<average<16; Fair: average>16

- **2.4G available num:** Determined by the average number of clients in the 2.4G band of online APs in the group.

  Best: average<8; Good: 8<average<16; Fair: average>16

- **Client health degree:** Determined by the percentage of health clients to all clients in the group.

  Best: percentage>80%; Good: 60%<percentage<80%;

  Fair: percentage<60%

  Note: Whether a client is a healthy client is determined by its RSSI.

- **AP health degree:** Determined by the average CPU usage of the online AP in the group.

  Best: average<20%; Good: 20%<average<40%;

  Fair: average>40%

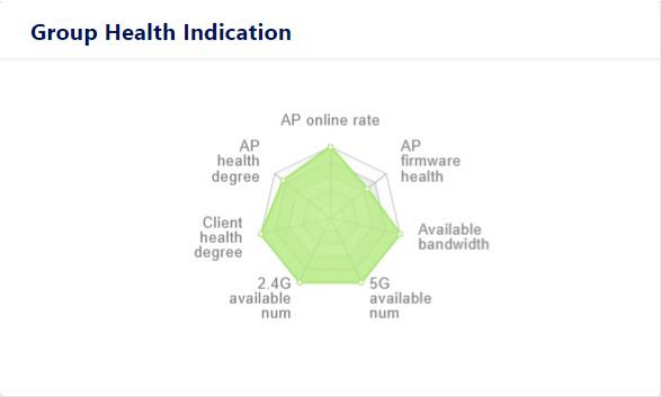


Figure 74: Group Dashboard – Group Health Indication

- **AP Type:** The specific model of AP and the corresponding histogram of the number of this model in the **"Site"**. The horizontal axis is the AP model, and the vertical axis represents the number of corresponding models.

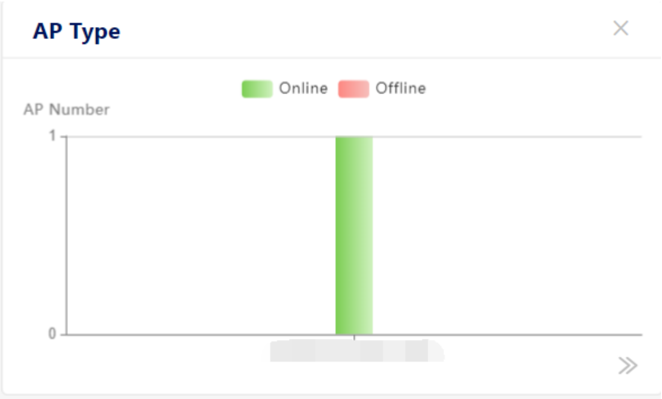


Figure 75: Group Dashboard - AP Type

- **AP Online Status:** Pie chart percentage of AP online and offline.

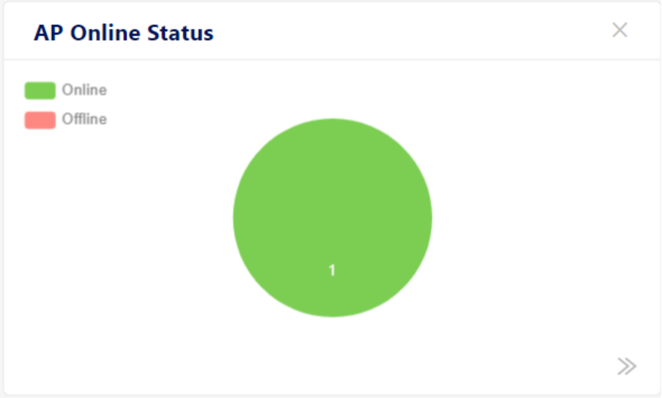


Figure 76: Group Dashboard - AP Online

- **AP Load Distribution:** Load balance in AP

  On the horizontal axis, we provide 7 reference values for the number of attached terminals of AP, which are: 0-9、10-19、 20-29、30-39、40-49、50-59、60+. The vertical axis represents the number of APs.

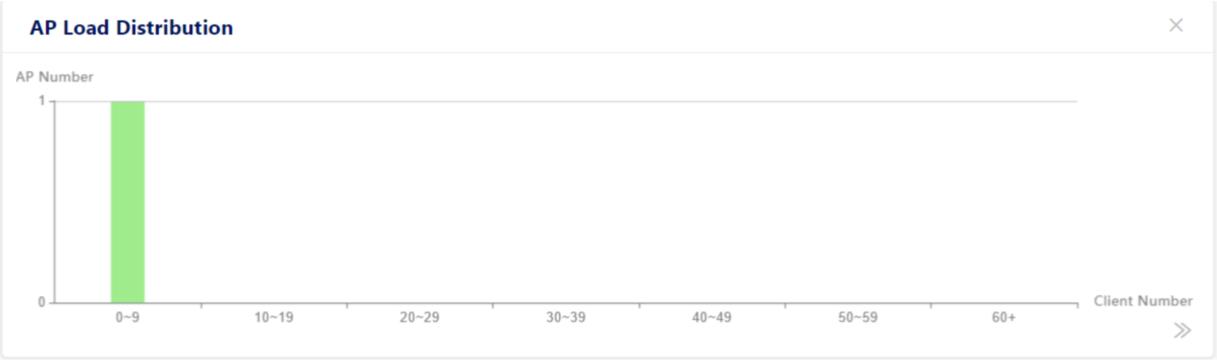
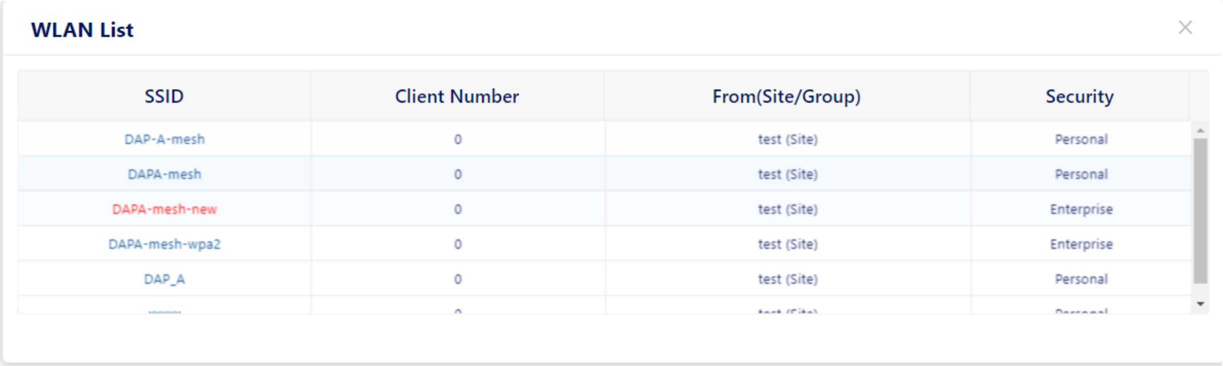


Figure 77: Group Dashboard - AP Load Distribution

- **Low Score AP:** Provide a list of APs whose scores are lower than the threshold standard. Remind customers to focus on the specific operation status and version information of APs.

  The AP list in the low-split AP tab is dynamic. If the AP indicators do not meet the threshold requirements, then the AP is displayed in the tab. Customers can click directly to 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 automatically disappears from the tab.
  AP threshold indicators are judged in the following 5 aspects:
  - AP CPU utilization
  - AP memory utilization
  - AP flash memory utilization
  - Number of terminal accesses
  - AP used bandwidth

- **WLAN List:** Show the SSID list on the Site.
  - **SSID:** SSID name of a wireless network
  - **Client Number:** Client Count associated with the SSID
  - **From(Site/Group):** Site or Group, which means the SSID is created from the Site or Group.
  - **Security:** Wireless security level, can be Open, Personal, or Enterprise.



WLAN List

SSID	Client Number	From(Site/Group)	Security
DAP-A-mesh	0	test (Site)	Personal
DAPA-mesh	0	test (Site)	Personal
DAPA-mesh-new	0	test (Site)	Enterprise
DAPA-mesh-wpa2	0	test (Site)	Enterprise
DAP_A	0	test (Site)	Personal
[illegible]	0	test (Site)	Personal

Figure 78: Group Dashboard - WLAN List

- **Wireless Client Health:**

  In the tab of terminal health, according to the signal strength (RSSI stands for Received Signals Strength Indicators) of the terminal signal uplink to the AP, we provide 3 levels of access health:

  - The terminal meeting the best RSSI threshold is classified as **"best"** level.
  - The terminal meeting the good RSSI threshold is classified as **"good"** level.
  - 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.

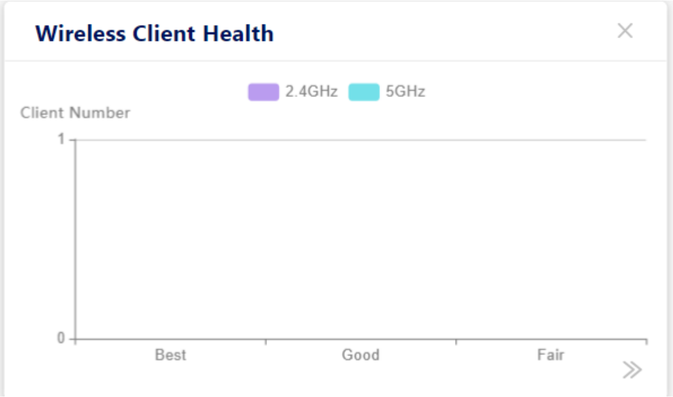


Figure 79: Group Dashboard - Wireless Client Health

- **Client Type:** The current hardware types of access terminals include computers, mobile devices, and others.

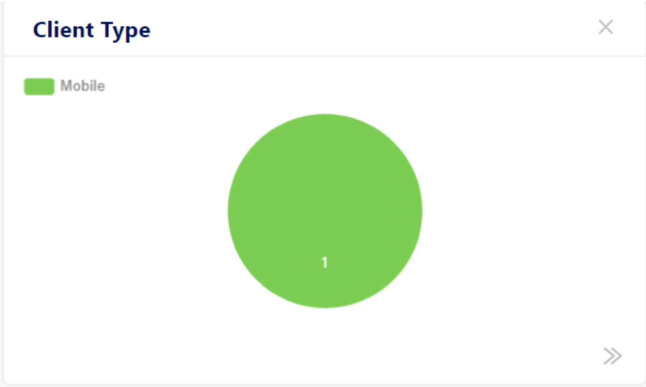


Figure 80: Group Dashboard - Client Type

- **Operating System:** The operating system type of the access terminal is intuitively given in the form of a pie chart.

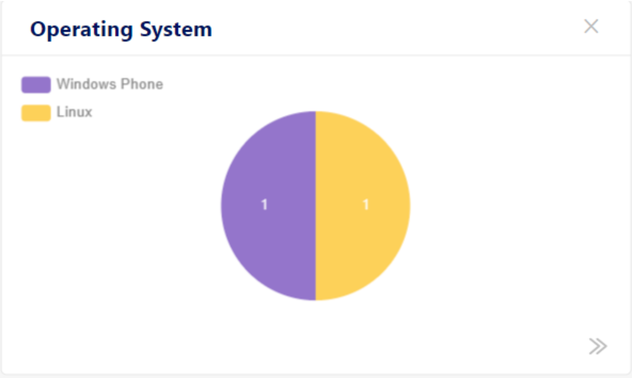


Figure 81: Group Dashboard - Operating System

- **Current Intrusive AP:** Show the proportion of interference AP and Rogue AP in the form of a pie chart.

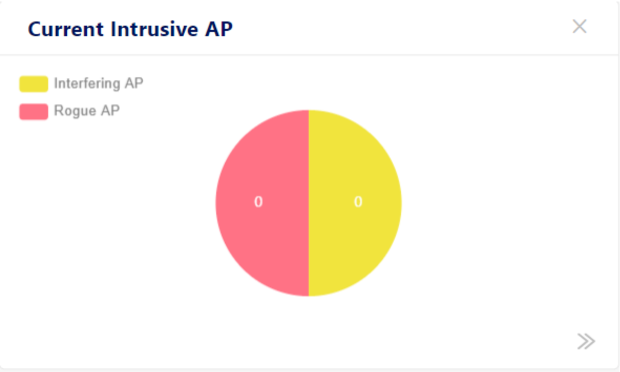


Figure 82: Group Dashboard - Current Intrusive AP

- **Current Intrusive Client:** Show the proportion of interference client and Rogue client in the form of a pie chart.

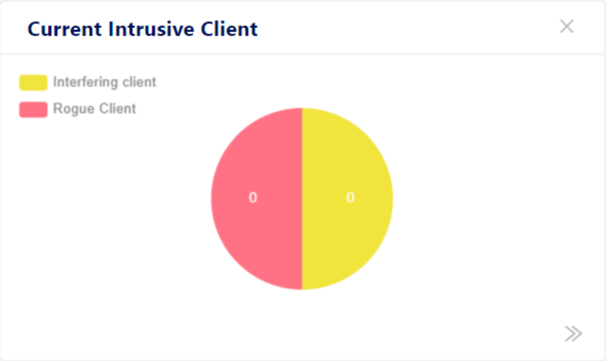


Figure 83: Group Dashboard - Current Intrusive Client

- **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 for the Site
  - **Traffic:** Histogram of Traffic

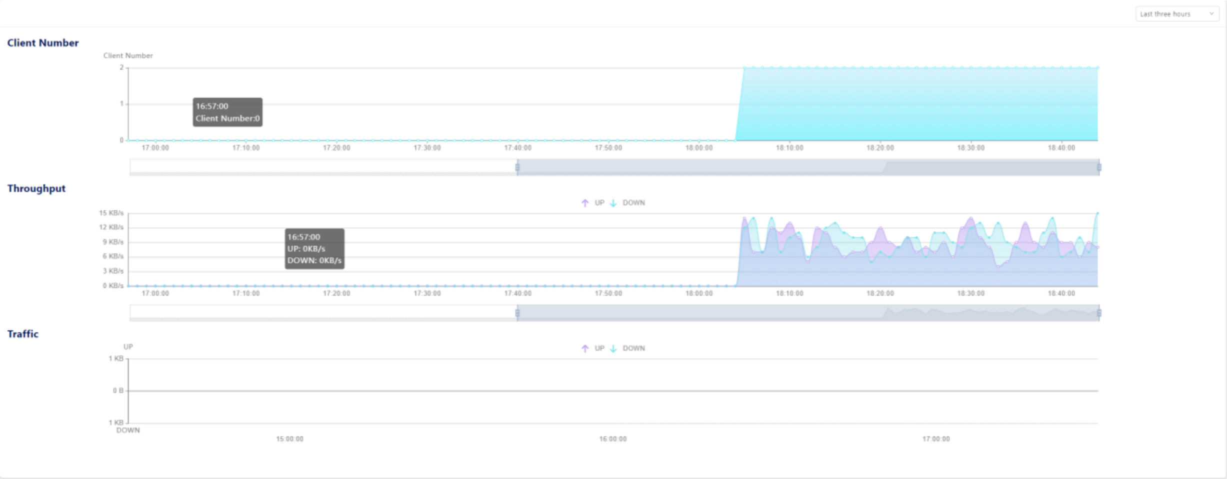


Figure 84: Group Dashboard - Historical Statistics

3.6.2 WLAN

Create, modify, and delete wireless networks for the Group. See “WLAN” on page 87.

3.6.3 AP

Provide monitoring of an AP device in the Group. Monitoring includes the records of syslog, the system log service for AP, and the key indicators in AP units. See “AP” on page 106.

3.6.4 Clients

Provide terminal management and monitoring. Management includes Blocklist processing for terminals with abnormal behavior. Monitoring includes type statistics of terminals, OS type statistics, and statistics and queries of various parameters of terminals attached to the network. See "Clients" on page 131.

3.6.5 Authentication

Create, modify, and delete authentication and other related policy configurations. See "Authentication" on page 131.

3.6.6 RF

Show the AP RF configuration. On the RF page of the Group, you can only view the configuration of RF and cannot modify it. See "RF" on page 211.

3.6.7 Log

Log of the system or log of the device. See "Log" on page 224.

3.6.8 Security

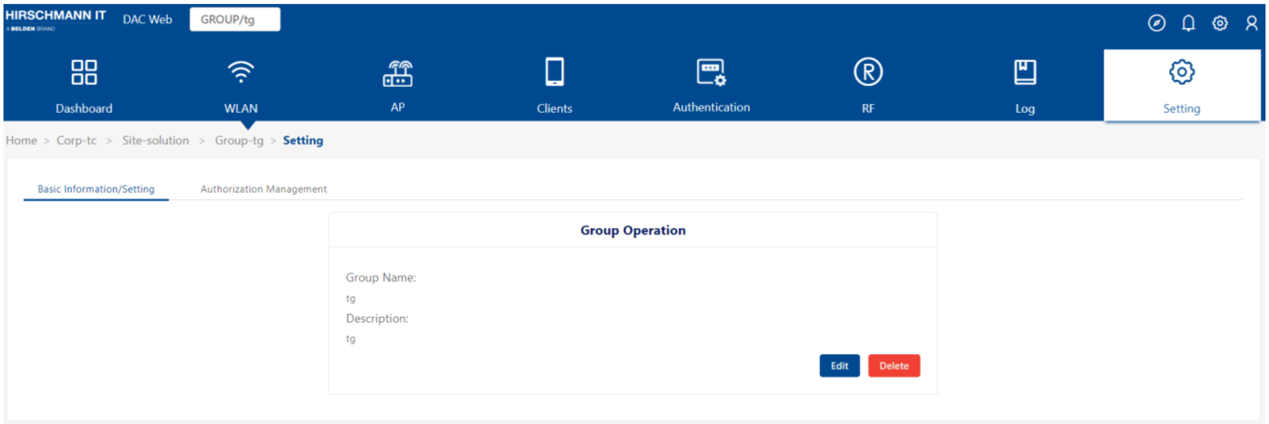
You can see the AP Record, Client Record, and Blocklist on this page. If you want to Configure Rogue AP strategy and a wireless attack detection strategy, then go to the "**Security**" View of the "**Site**".

See "Security" on page 231.

3.6.9 Setting

Settings of the Group.

- ■ **Basic Information/Setting**
  - ▶ **Group Operation**
    - **Edit:** Change the Group name or description.
    - **Delete:** Delete the Group.



Group Operation

Group Name:
tg
Description:
tg

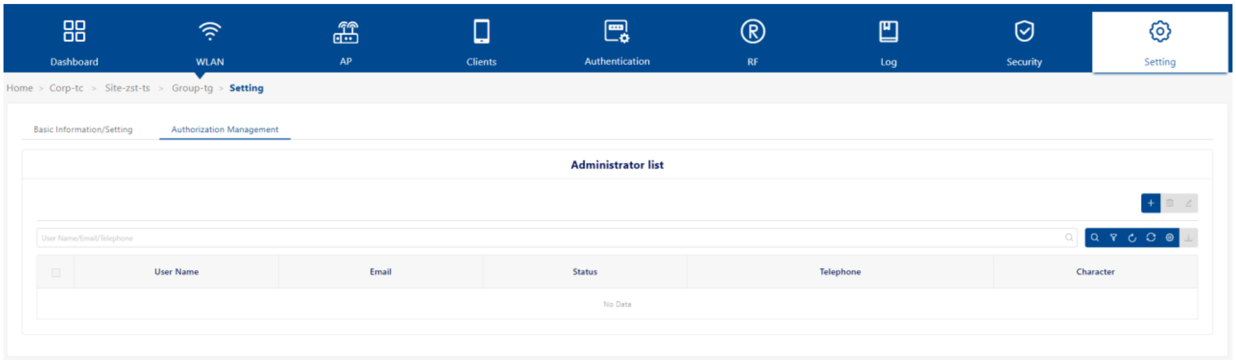
Figure 85: Basic Information/Setting

■ Authorization management

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

▶ Administrator list

- **User name:** User Name
- **Email:** Email
- **Status:** success/fail
- **Telephone:** The telephone of the user
- **Character:** Character can be admin or viewer


Dashboard
WLAN
AP
Clients
Authentication
RF
Log
Security
Setting
Home > Corp-tc > Site-zst-ts > Group-tg > Setting
Basic Information/Setting
Authorization Management
User Name/Email/Telephone

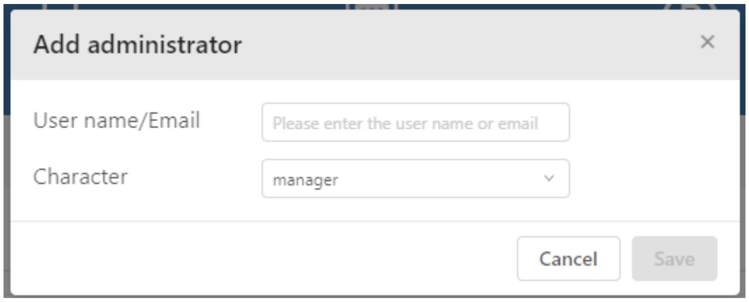
Administrator list

☐	User Name	Email	Status	Telephone	Character
No Data					

Figure 86: Authorization Management

■ Add Administrator

☐ Click the **"+"** icon. The **"Add Administrator"** dialog appears.
☐ Enter the **"User name"** or **"Email"** of the user you want to add.
☐ Select **"Character"** from the drop-down list (Manager or Viewer).
☐ Click the **"Save"** button to apply the settings.



Add administrator

User name/Email: Please enter the user name or email

Character: manager

Figure 87: Add Administrator window

■ **Delete Administrator**

□ Select the administrator you want to delete.
□ Click the **Delete** icon.
□ Click **“Yes”** on the confirmation prompt.

4 License

Currently, DAC has 2 kinds of license:

- **Basic License**

  Including Basic Function (create WLAN, terminal display, statistics, etc.) and Client Access Function. The Basic Function is authorized based on the total number of APs. The Client Access function is authorized based on the total number of authentication terminals.

- **Security License**

  Wireless security includes WIDS and WIPS. The security license is authorized based on the number of APs.

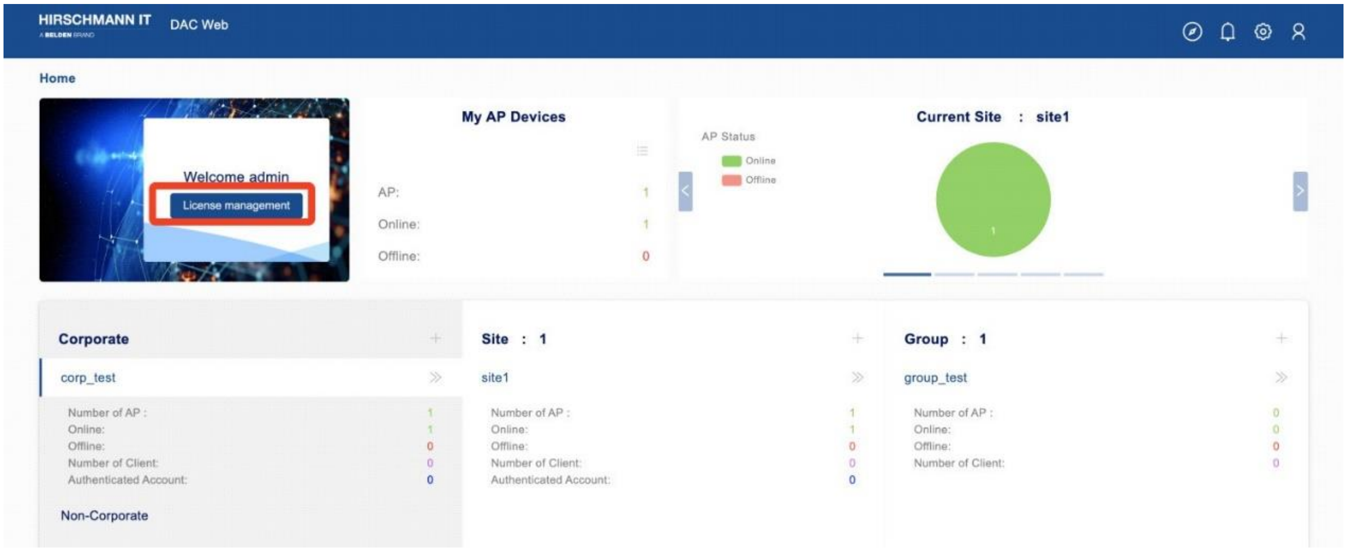
The licenses you can purchase are as follows:

Types	Part number	Part name	Description
Basic License	942999321	DAC-50	Software DAC platform with a license for 50 AP and 1000 clients
	942999322	DAC-256	Software DAC platform with a license for 256 AP and 5000 clients
	942999323	DAC-500	Software DAC platform with a license for 500 AP and 10000 clients
	942999324	DAC-1000	Software DAC platform with a 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: License types

The carrier of the license is in the form of a 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.

Click the **“License management”** button on the user **“Home”** page and the **“License”** screen appears.



AP: 1
Online: 1
Offline: 0

corp_test
Number of AP : 1
Online: 1
Offline: 0
Number of Client: 0
Authenticated Account: 0

site1
Number of AP : 1
Online: 1
Offline: 0
Number of Client: 0
Authenticated Account: 0

group_test
Number of AP : 0
Online: 0
Offline: 0
Number of Client: 0

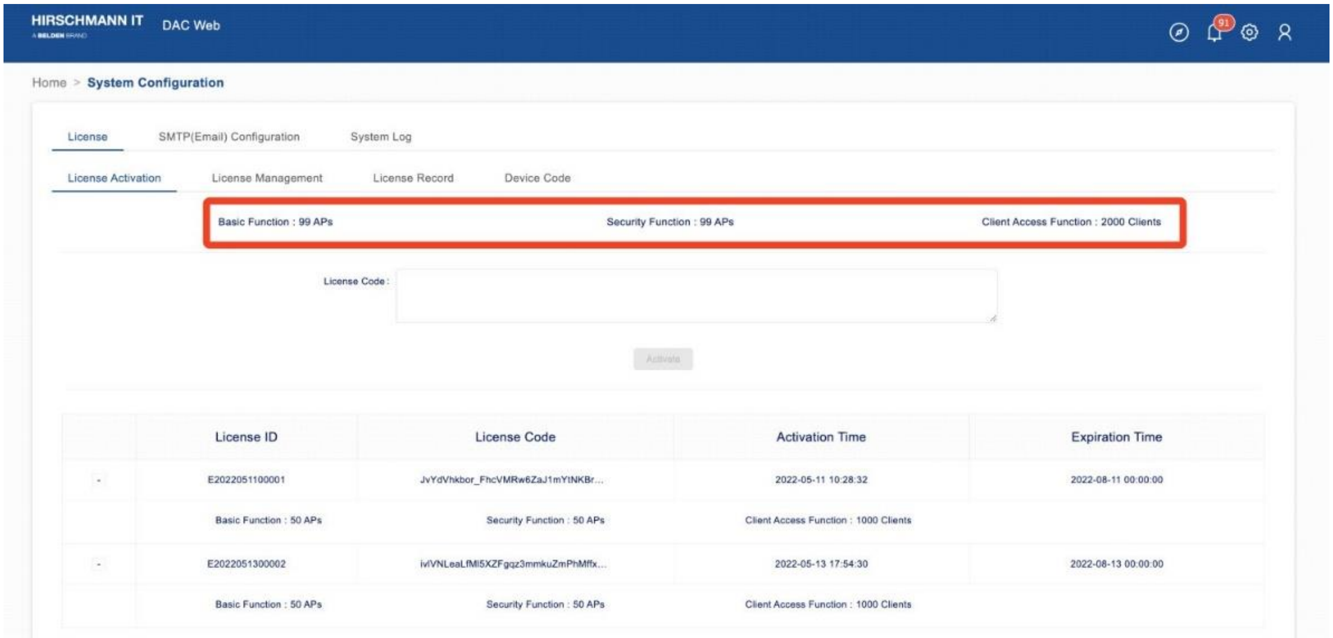
Figure 88: Home page

This chapter contains the following topics:

- License activation
- License management
- License record
- Device code

4.1 License activation

Use the **“License Activation”** page to activate the license code.



Basic Function : 99 APs   Security Function : 99 APs   Client Access Function : 2000 Clients

License Code :

	License ID	License Code	Activation Time	Expiration Time
-	E2022051100001	JvYdVhkbor_FhcVMRw6ZaJ1mYtNKBr...	2022-05-11 10:28:32	2022-08-11 00:00:00
	Basic Function : 50 APs	Security Function : 50 APs	Client Access Function : 1000 Clients	
-	E2022051300002	ivlVNLeaLfMl5XZFgqz3mmkuZmPhMffx...	2022-05-13 17:54:30	2022-08-13 00:00:00
	Basic Function : 50 APs	Security Function : 50 APs	Client Access Function : 1000 Clients	

Figure 89: License activation page

- □ Enter the **“License code”** obtained from the supplier into the input box.
- □ Click the **“Activate”** button. The **“License Code”** details appear.
  The details include the counts for each function.
  - ▶ Basic Function: Provide basic AP functions, including WLAN, RF, Data report and so on. As shown in Figure 89, the maximum number of APs available for the basic function is 99.
  - ▶ Security Function: Provide security functions, including Blacklist, wIDS/wIPS. As shown in Figure 89, the maximum number of APs available for the security function is 99.
  - ▶ Client Access Function: As shown in Figure 89, the maximum number of clients that are allowed to access is 2000.
- □ Click the **“Activation”** button on the detail window to enable the license.
  Then the newly activated licenses appear in the list of activated licenses.

If you have activated multiple licenses, then you can view the actual activated functions and the number of functions of each license. At the same time, you can see the remaining AP count of basic functions, the remaining count of terminals that can be authenticated, and the remaining AP count of security functions.

List of activated licenses:

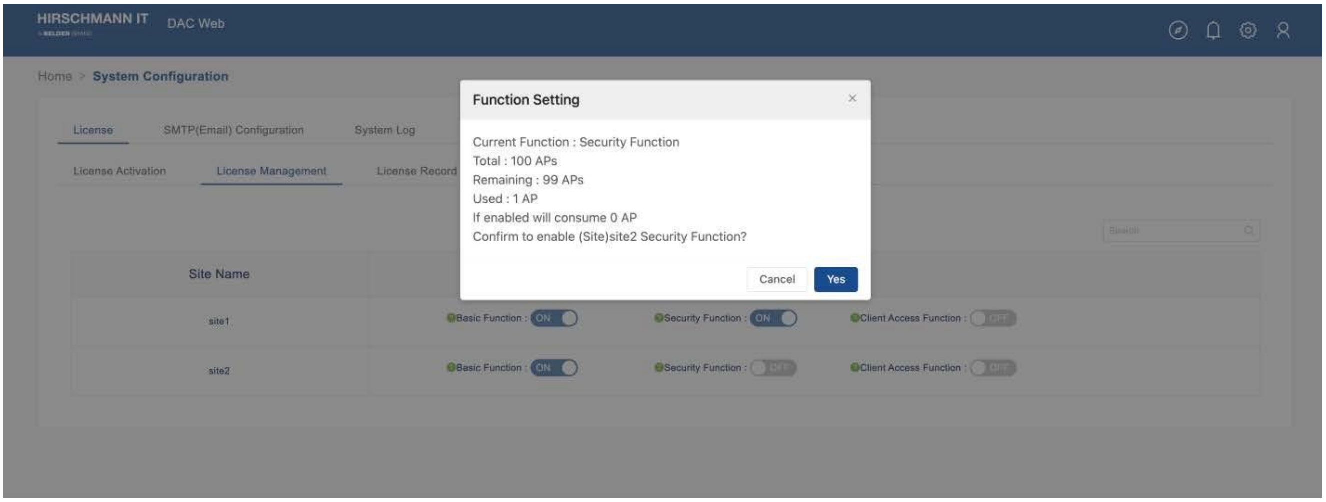
- **License ID:** License ID.
- **License Code:** License Code.
- **Activation Time:** The Time that you active this License.
- **Expiration Time:** When the expiration time comes, the count of devices in the license will not be available.

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.

4.2 License management

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

- □ Select the corresponding Site and click the function switch.
- □ Click the **“Yes”** button to confirm and enable the function.



Function Setting

Current Function : Security Function
Total : 100 APs
Remaining : 99 APs
Used : 1 AP
If enabled will consume 0 AP
Confirm to enable (Site)site2 Security Function?

Cancel Yes

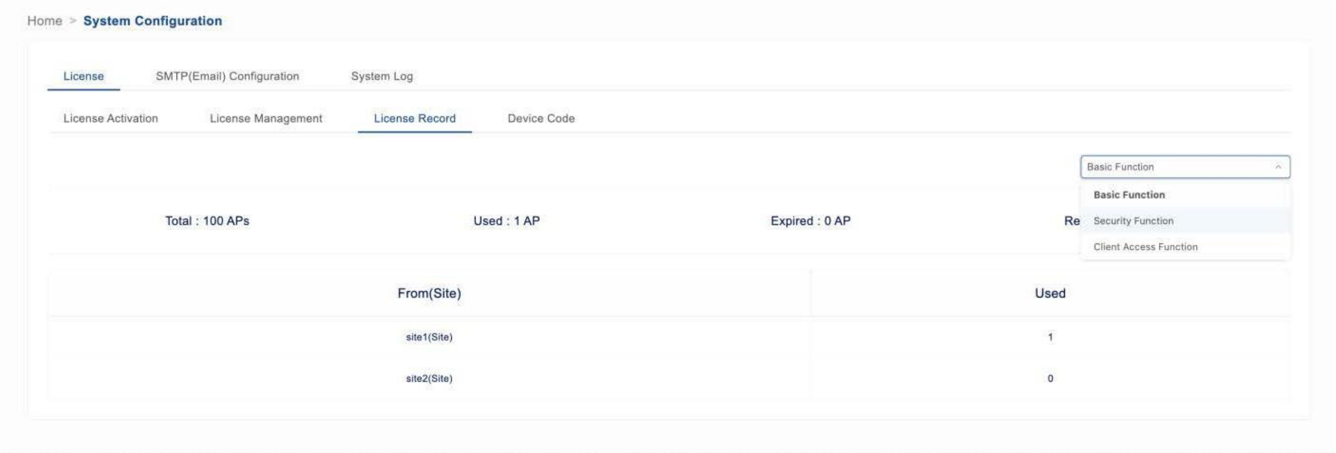
Site Name			
site1	Basic Function : ON	Security Function : ON	Client Access Function : OFF
site2	Basic Function : ON	Security Function : OFF	Client Access Function : OFF

Figure 90: DAC license management

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.

4.3 License record

Display the usage of each function in each Site and the remaining or expired points of the current account based on the function. You can select the Function to display from the drop-down list.



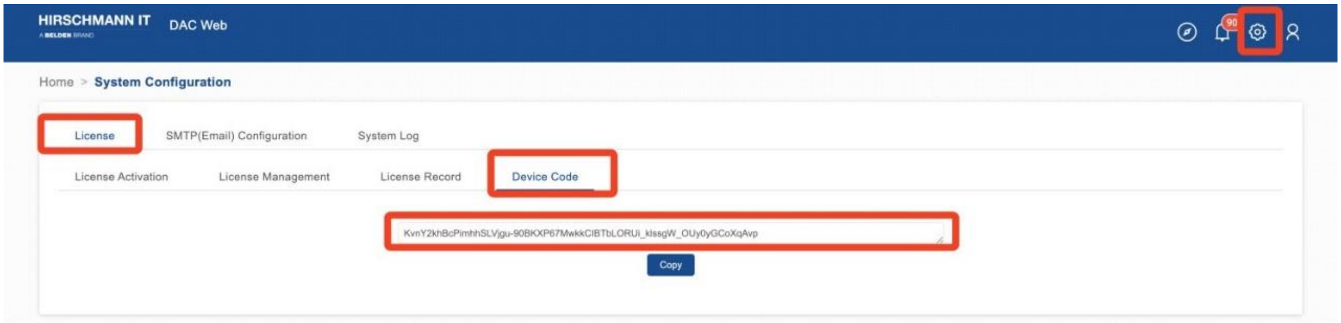
Total : 100 APs   Used : 1 AP   Expired : 0 AP   Re

From(Site)	Used
site1(Site)	1
site2(Site)	0

Figure 91: DAC license record

4.4 Device code

The 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 generates a license code, which can only be applied to the current device based on the device code.

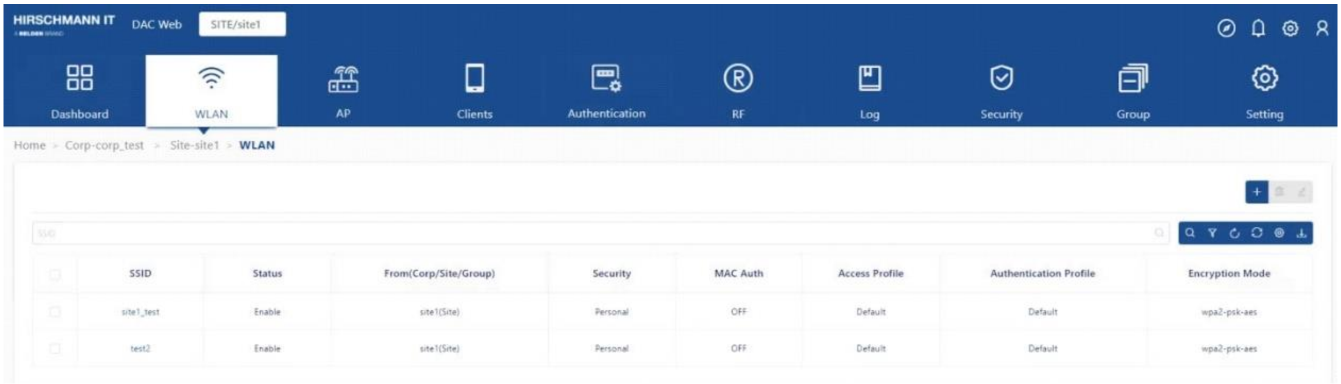


KvnY2khBcPimhhSLVjgu-90BKXP67MwkkCIBTbLORUi_klssgW_OUy0yGCoXqAvp

Figure 92: DAC device code

5 WLAN

This section describes the basic principles of wireless access. Also describes how to create or modify WLAN. You can configure WLAN in the **“Site”** or **“Group”** view.



□	SSID	Status	From(Corp/Site/Group)	Security	MAC Auth	Access Profile	Authentication Profile	Encryption Mode
□	site1_test	Enable	site1(Site)	Personal	OFF	Default	Default	wpa2-psk-aes
□	test2	Enable	site1(Site)	Personal	OFF	Default	Default	wpa2-psk-aes

Figure 93: WLAN page

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 the MAC Authentication status.
- **WLAN Connection:** After successful WLAN Access Authentication, the client establishes a connection with the DAP.
- **Network Access (Captive Portal) Authentication:** After the client connects 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
- Edit WLAN
- Delete WLAN

5.1 Security level

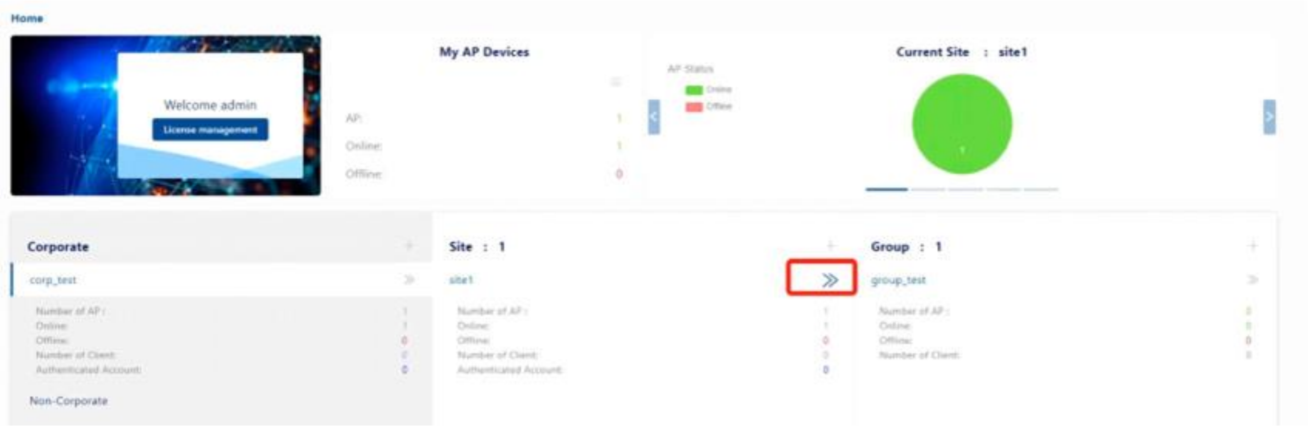
- **Open:** The Wi-Fi without any security configuration.
- **Personal:** A key protects the Wi-Fi. DAP authenticates the client by verifying the passphrase.
- **Enterprise:** An authentication server is used to authenticate the connecting client via 802.1x Authentication.

5.2 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 additional layer of security for authentication devices. MAC-based authentication is often used to authenticate and allow network access through certain devices while denying access to the rest.

5.3 Create WLAN

□ Click the **“>>”** icon to enter the **“Site”** view.



AP: 1
Online: 1
Offline: 0

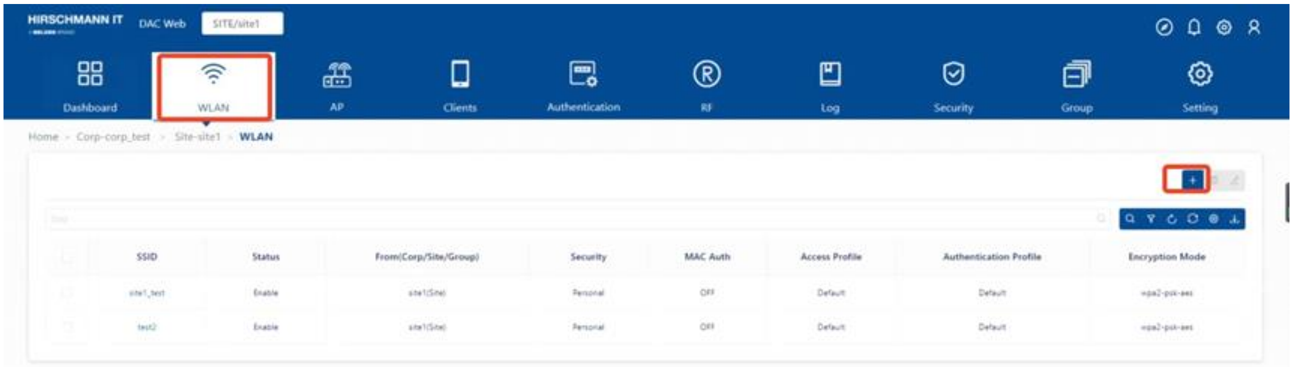
corp_test
Number of AP : 1
Online: 1
Offline: 0
Number of Client: 0
Authenticated Account: 0

site1
Number of AP : 1
Online: 1
Offline: 0
Number of Client: 0
Authenticated Account: 0

group_test
Number of AP : 0
Online: 0
Offline: 0
Number of Client: 0

Figure 94: Home page

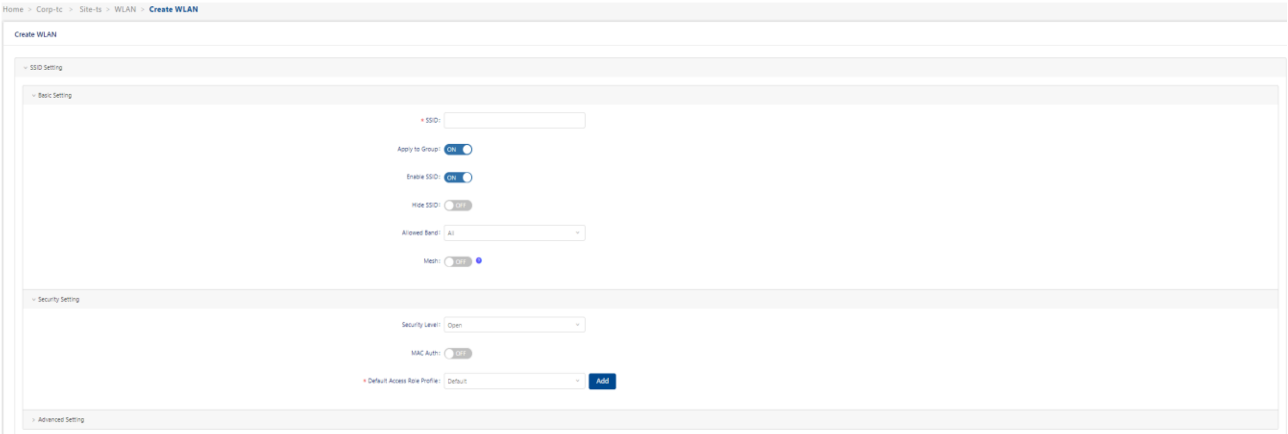
□ Click the **“WLAN”** tab to enter the **“WLAN”** list page.



SSID	Status	From(Corp/Site/Group)	Security	MAC Auth	Access Profile	Authentication Profile	Encryption Mode
site1_test	Enable	site1(Site)	Personal	OFF	Default	Default	wpa2-psk-aes
test2	Enable	site1(Site)	Personal	OFF	Default	Default	wpa2-psk-aes

Figure 95: WLAN list

□ On the WLAN tab of the **“Site”** or **“Group”** view, click the **“+”** icon on the head of WLAN list table. Then the **“Create WLAN”** window appears.



* SSID:
Apply to Group: ON
Enable SSID: ON
Hide SSID: OFF
Allowed Band: All
Mesh: OFF

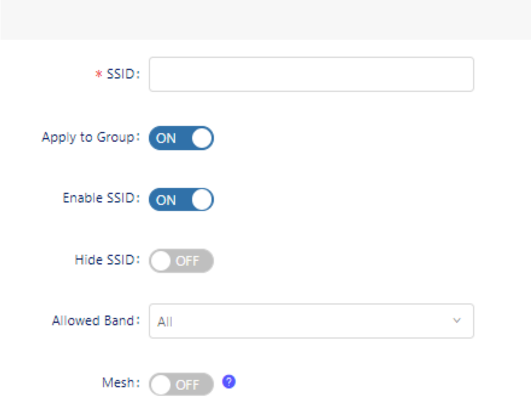
Security Level: Open
MAC Auth: OFF
* Default Access Role Profile: Default

Figure 96: WLAN window

5.3.1 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:** Enable or disable the WLANs that are assigned to the Group.
  - **Enable SSID:** Enable or disable the SSID.
  - **Hide SSID:** Enable or disable SSID in beacon frames. In the default setting, it is disabled.

    Note: Hiding the SSID does very little to increase security.
  - **Allowed Band:** The band(s) available on the service:
    - 2.4 GHz
    - 5 GHz
    - All - 5 GHz and 2.4 GHz (default)
  - **Mesh:** Enables or Disables SSID for mesh-based vehicle-ground fast link handover. After enabling mesh, it is limited to select the encryption mode of WPA2_PSK_AES, WPA3_SAE_AES, WPA2_ AES or WPA3_ AES. (Only take effect on DAP847-A)



* SSID:

Apply to Group: ON

Enable SSID: ON

Hide SSID: OFF

Allowed Band: All

Mesh: OFF

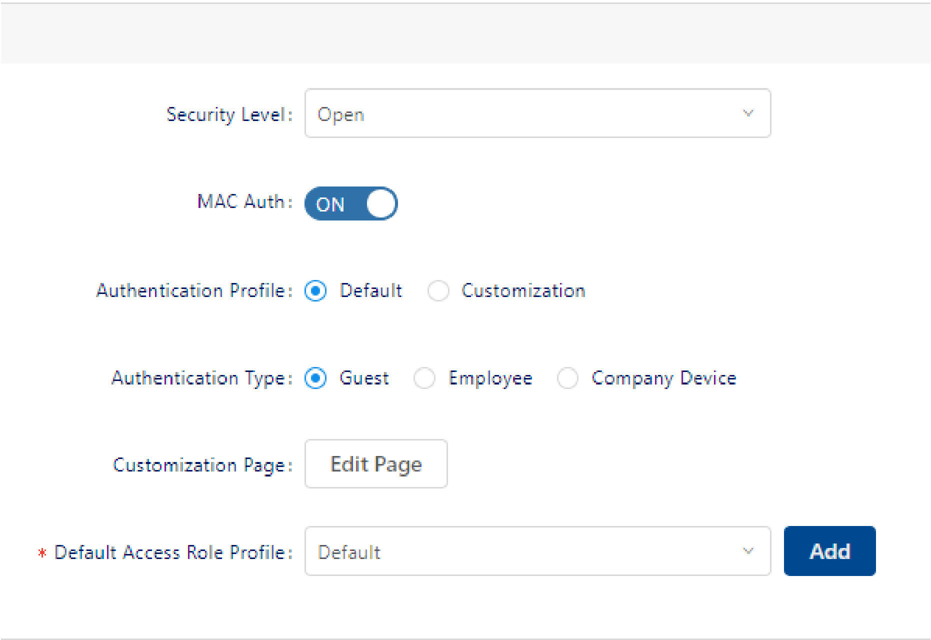
Figure 97*: WLAN Basic Setting*

- **Security setting**
  - **Security Level:** Select the security level for the WLAN Service.
  - **Open:** Unsecured Wi-Fi.

    To assign a role to clients, you can configure a default role or enable

MAC authentication.

- **MAC Auth:** Enable or disable the MAC authentication.
- **Authentication Profile:**
  - **Default:** an easy and fast configuration.
    Selecting **Default** means that you can select the web portal **Authentication Type** of **Guest** or **Employee** for the current SSID or set the access SSID for the **Company Device**.
  - **Customization:** need manual creation of the Access Policy, the Authentication Strategy, the Guest Access Strategy or the Employee Access Strategy. See “Authentication” on page 163.
- **Customization Page:** Select the template page for the web portal authentication, and customize the page as needed. Can only be set when the Authentication Type is set to **“Guest”** or **“Employee”**.



Security Level: Open

MAC Auth: ON

Authentication Profile: ● Default ○ Customization

Authentication Type: ● Guest ○ Employee ○ Company Device

Customization Page: Edit Page

* Default Access Role Profile: Default

Figure 98: Security Setting – “Open” Security Level

- **Personal:** A key protects the Wi-Fi.
- **Encryption Mode:** Select an encryption type from the drop-down list, 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.

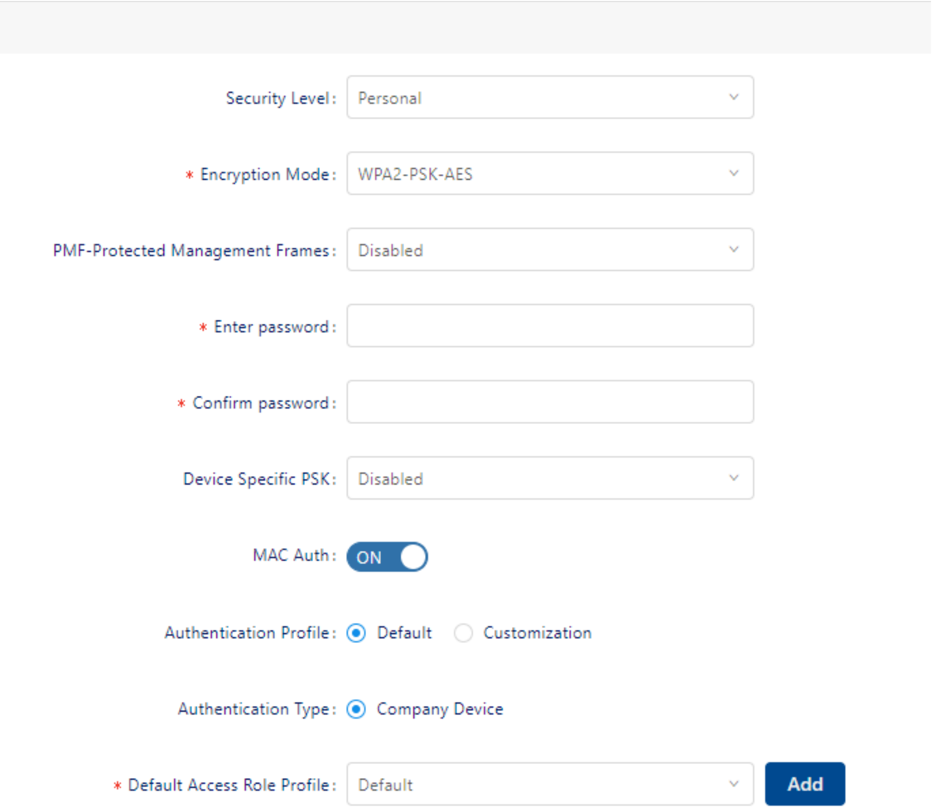
  - **WPA2_PSK_AES:** WPA2 with AES encryption using a pre-shared key.
  - **WPA3_SAE_AES:** WPA3 with AES encryption using a pre-shared key allows only WPA3 capable clients to access.
  - **WPA3_PSK_SAE_AES:** WPA3 and WPA2 mixed mode allow access to both WPA3 and WPA2 capable clients.

- **PMF-Protected Management Frames:** Configure whether connections are accepted from clients supporting Protected Management Frame for certain Security Levels or Encryption Types (**Enterprise:** WPA2_AES / WPA3_AES256 / WPA3AES, **Personal:** WPA2_PSK_AES / WPA3_SAE_AES / WPA3_PSK_SAE_AES).
  - **Disabled:** Disable Protected Management Frame requirements. A Protected Management Frame is required for WPA3 encryptions and cannot be disabled. The field is not configurable for WPA3 encryption.
  - **Optional:** Allow connections from clients supporting the Protected Management Frame and clients that do not.
  - **Required:** Only allow connections from clients supporting the Protected Management Frame.

- **Enter Password:** Password for the terminal to connect to the ESSID.
- **Confirm Password:** Enter the password again. **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, the AAA Server sends the RADIUS Access Accept for MAC Authentication for the device and also sends 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.
  - **Disabled:** Disable Device Specific PSK.
  - **Prefer Device Specific PSK:** AAA Server always uses 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, whether it exists or not. The Device Specific PSK cannot work with an External RADIUS Server. Devices are configured for Device Specific PSK on the Company device.

- **Authentication Profile:**
  - **Default:** an easy and fast configuration method.
    Selecting **Default** means that you can only set the access SSID for the **Company Device**.
  - **Customization:** need manual creation of the Access Policy, the Authentication Strategy, the Guest Access Strategy or the Employee Access Strategy. See "Authentication" on page 163.



Security Level: Personal

* Encryption Mode: WPA2-PSK-AES

PMF-Protected Management Frames: Disabled

* Enter password:

* Confirm password:

Device Specific PSK: Disabled

MAC Auth: ON

Authentication Profile: ● Default ○ Customization

Authentication Type: ● Company Device

* Default Access Role Profile: Default

Figure 99: Security Setting – "Personal" Security Level

- **Enterprise:** An authentication server is used to authenticate the connecting client via 802.1x Authentication.
- **Encryption Mode:** Select an Encryption Type from the drop-down list:
  - **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: 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.

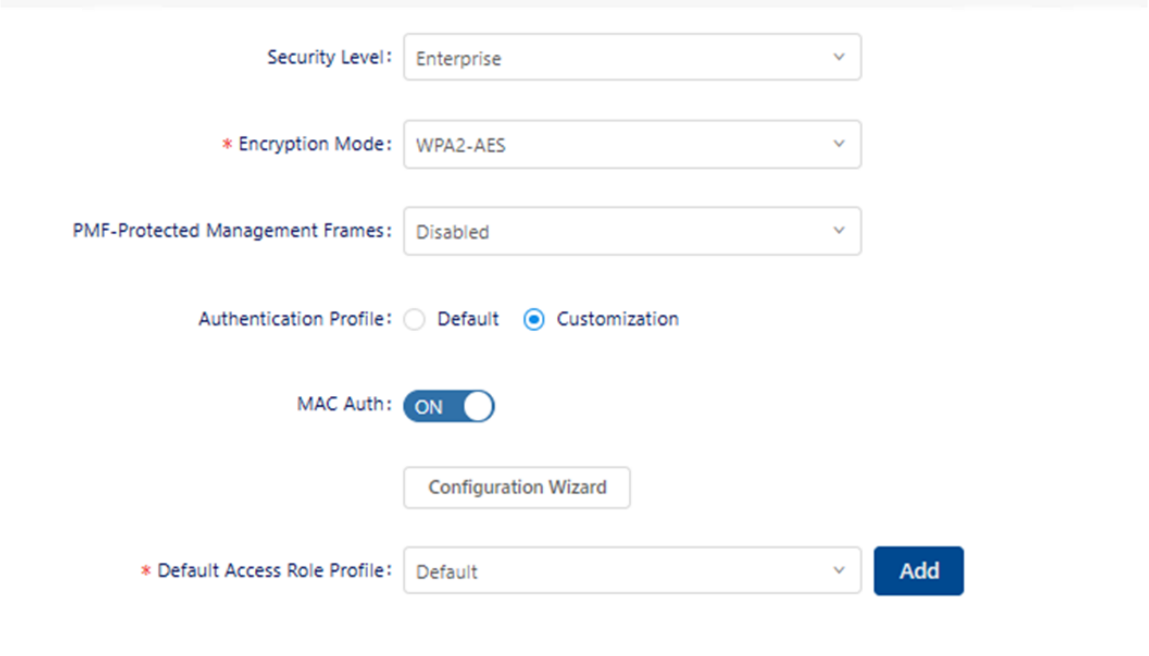
▶ **Default Access Role Profile:** Select the default Access Role Profile that will be applied to clients if a role cannot be assigned by other role assignment methods. See “Access role profile” on page 147.

▶ **Authentication Profile:**

- **Default: Default** provides an easy and fast configuration method. 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, Guest Access Strategy or Employee Access Strategy. See “Authentication” on page 139.
- **MAC Auth:** Enable or disable the MAC Authentication. This field is only applicable when **Customization** of the **Authentication Profile** is selected.

▶ **Authentication Source:** Can only be set when Authentication Profile is set to Default.

- **Local Database:** This SSID is used for Guest access.
- **External LDAP/AD:** This SSID is used for Employee access.
- **External Radius:** 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 based on MAC authentication. You can add Company Device MAC at Authentication → Setting → Company Device. See “Company device” on page 189.


Security Level: Enterprise

* Encryption Mode: WPA2-AES

PMF-Protected Management Frames: Disabled

Authentication Profile: ○ Default ● Customization

MAC Auth: ON

* Default Access Role Profile: Default

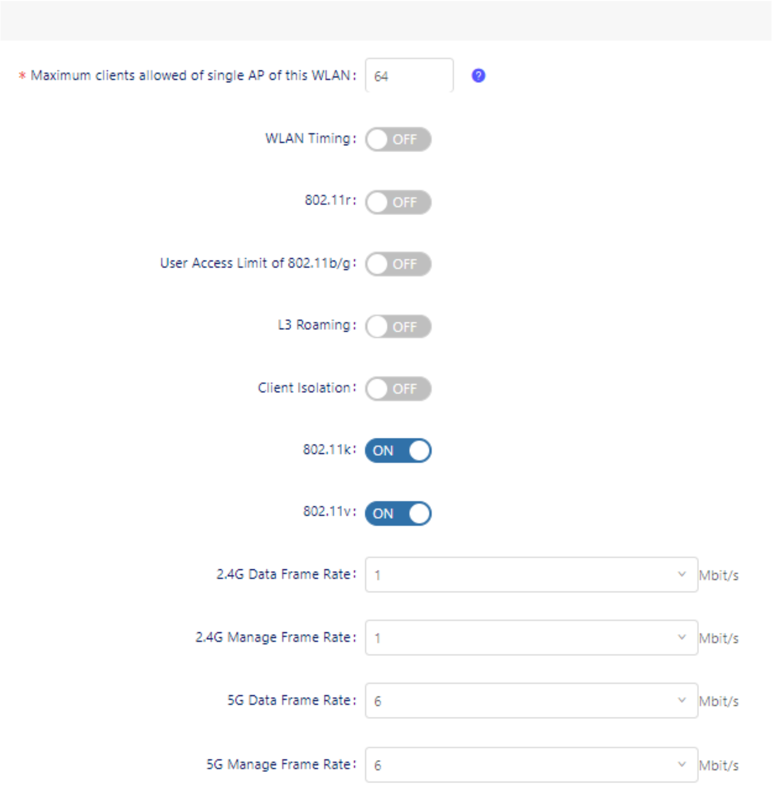
Figure 100: Security Setting – “Enterprise” Security level

- **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 (Possible values: 1..256, Default setting: 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 broadcasts the SSID every day.
      - **Weekday:** WLAN broadcasts the SSID every weekday.
      - **Weekend:** WLAN broadcasts the SSID every weekend.
    - **Custom WLAN work schedule:** Enable or disable a special time range configured on the work cycle.
    - **WLAN work schedule:** Select the time range.
  - **802.11r:** Enable or disable 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:** Enable or disable Layer 3 roaming.
    - Layer 3 roaming allows clients to move between Access Points and

connect to a new IP subnet and VLAN.

- **Client Isolation:** Enable or disable 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:** Enable or disable 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:** Enable or disable 802.11v.
  - The 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 to identify the best AP to transition to as they roam.
- **2.4G Data Frame Rate:** 2.4G band clients with lower data speeds will not be given access. The recommended value is 12.
- **2.4G Manage Frame Rate:** 2.4G band wireless management frame transmit rate. A higher value means less coverage and a lower value means larger coverage.
- **5G Data Frame Rate:** 5G band clients with lower data speeds will not be given access. The recommended value is 24.
- **5G Manage Frame Rate:** 5G band wireless management frame transmit rate. A higher value means less coverage and a lower value means larger coverage.



* Maximum clients allowed of single AP of this WLAN: 64

WLAN Timing: OFF

802.11r: OFF

User Access Limit of 802.11b/g: OFF

L3 Roaming: OFF

Client Isolation: OFF

802.11k: ON

802.11v: ON

2.4G Data Frame Rate: 1 Mbit/s

2.4G Manage Frame Rate: 1 Mbit/s

5G Data Frame Rate: 6 Mbit/s

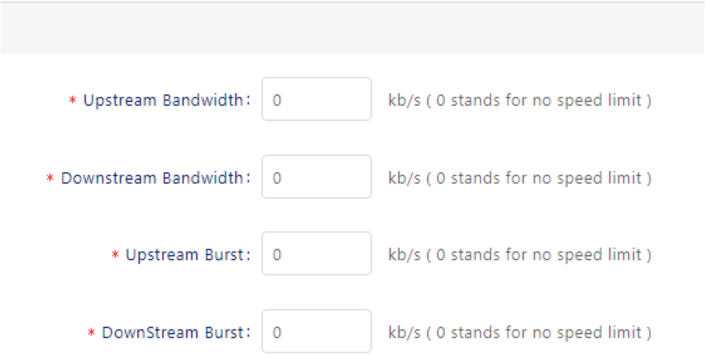
5G Manage Frame Rate: 6 Mbit/s

Figure 101: Advanced Setting

5.3.2 QoS setting

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

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



* Upstream Bandwidth: 0 kb/s (0 stands for no speed limit)

* Downstream Bandwidth: 0 kb/s (0 stands for no speed limit)

* Upstream Burst: 0 kb/s (0 stands for no speed limit)

* DownStream Burst: 0 kb/s (0 stands for no speed limit)

Figure 102: Bandwidth Contract

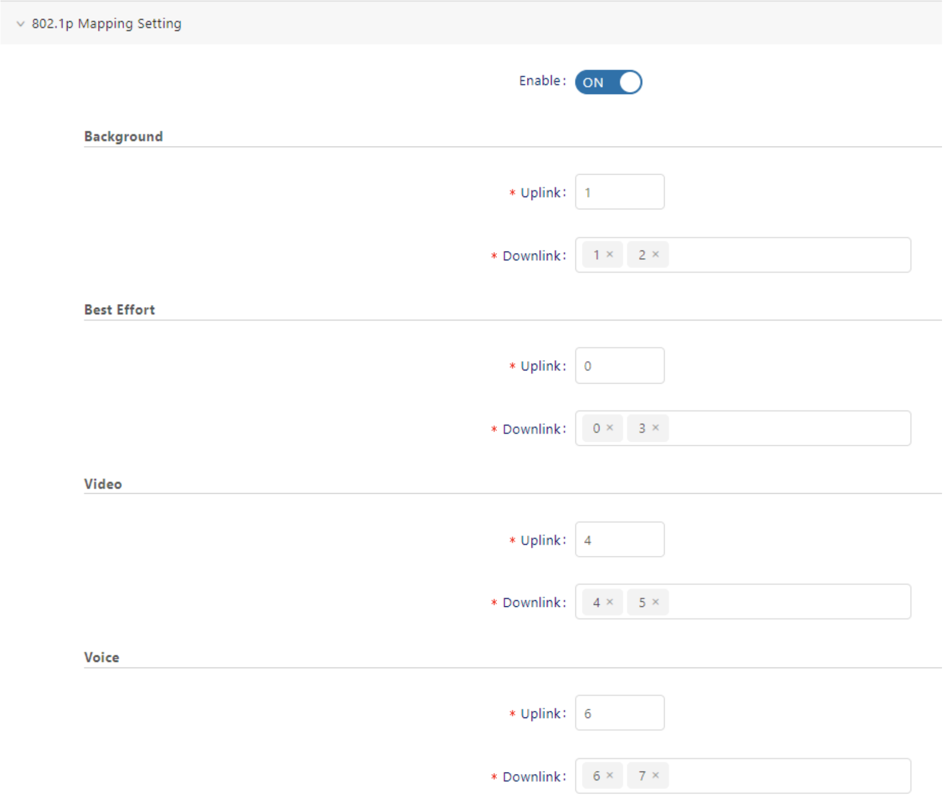
802.1p mapping settings

802.1p mapping setting is used to configure the uplink and downlink mapping mechanisms 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 in the field.
- To remove a value, click the **“x”** next to the value.

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

- ▶ **Voice:** WMM Voice is mapped to the 802.1p value.
  - **Uplink:** Maps uplink traffic (from AP to WAN network). (Possible values: 0..7, Default Setting: 6)
  - **Downlink:** Maps downlink traffic (from WAN network to AP). (Possible values: 0..7, Default Setting: 6, 7)



802.1p Mapping Setting

Enable: ON

Background

* Uplink: 1

* Downlink: 1 × 2 ×

Best Effort

* Uplink: 0

* Downlink: 0 × 3 ×

Video

* Uplink: 4

* Downlink: 4 × 5 ×

Voice

* Uplink: 6

* Downlink: 6 × 7 ×

Figure 103: 802.1p Mapping Setting

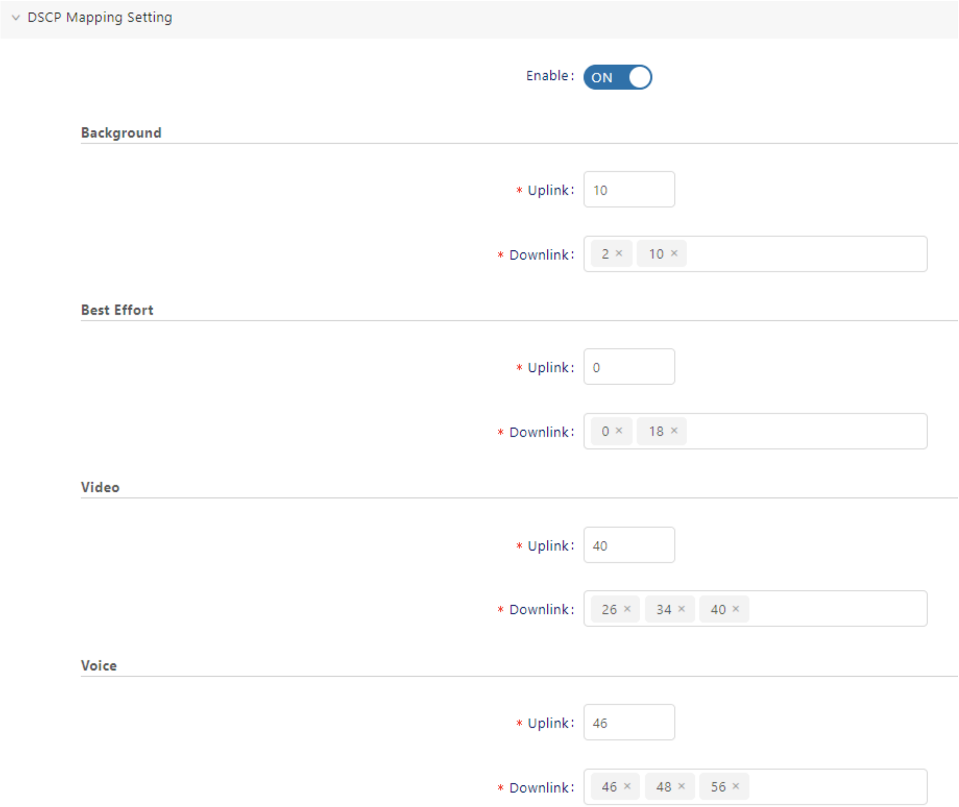
■ DSCP mapping settings

DSCP mapping settings are used to configure the uplink and downlink mapping mechanisms 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 in the field.
☐ To remove a value, click the **“x”** next to the value.

- ▶ **Enable:** If enabled, the original DSCP mapping for traffic is trusted (Default Setting: Disabled).
- ▶ **Background:** WMM Background will be mapped to the DSCP value.

  - **Uplink:** Maps uplink traffic (from AP to WAN network). (Possible values: 0..63, Default Setting: 10)
  - **Downlink:** Maps downlink traffic (from WAN network to AP). (Possible values: 0..63, Default Setting: 2, 10)
- **Best Effort:** WMM Best Effort will be mapped to the DSCP value.
  - **Uplink:** Maps uplink traffic (from AP to WAN network). (Possible values: 0..63, Default Setting: 0)
  - **Downlink:** Maps downlink traffic (from WAN network to AP). (Possible values: 0..63, Default Setting: 0, 18)
- **Video:** WMM Video will be mapped to the DSCP value.
  - **Uplink:** Maps uplink traffic (from AP to WAN network). (Possible values: 0..63, Default Setting: 40)
  - **Downlink:** Maps downlink traffic (from WAN network to AP). (Possible values: 0..63, Default Setting: 24, 36, 40)
- **Voice:** WMM Voice will be mapped to the DSCP value.
  - **Uplink:** Maps uplink traffic (from AP to WAN network). (Possible values: 0..63, Default Setting: 46)
  - **Downlink:** Maps downlink traffic (from WAN network to AP). (Possible values: 0..63, Default Setting: 46, 48, 56)



DSCP Mapping Setting

Enable: ON

Background

* Uplink: 10

* Downlink: 2 × 10 ×

Best Effort

* Uplink: 0

* Downlink: 0 × 18 ×

Video

* Uplink: 40

* Downlink: 26 × 34 × 40 ×

Voice

* Uplink: 46

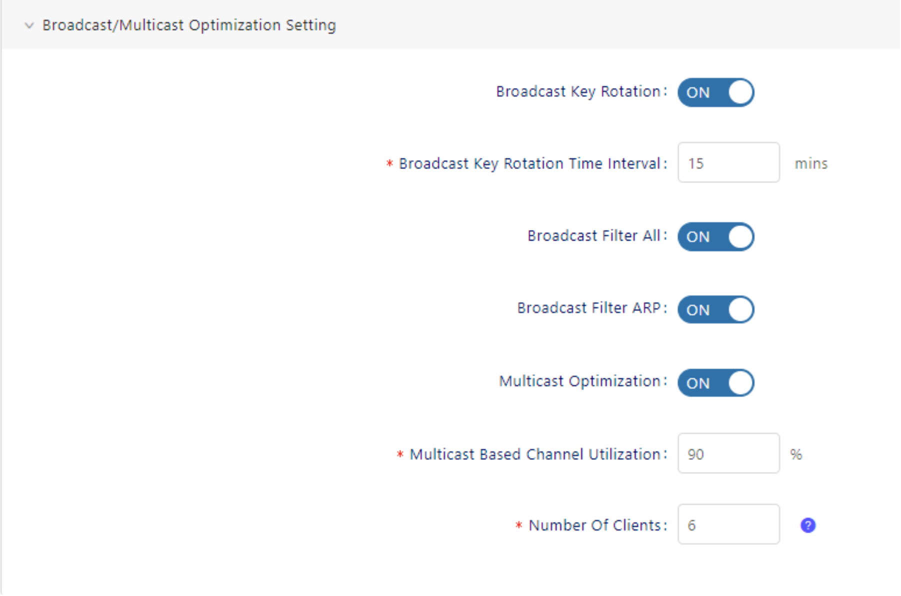
* Downlink: 46 × 48 × 56 ×

Figure 104: DSCP Mapping Setting

5.3.3 Broadcast/Multicast optimization settings

- **Broadcast Key Rotation:** Enable or disable the broadcast key rotation function. If enabled, the broadcast key rotates after every interval.
- **Broadcast Key Rotation Time Interval:** The interval, in minutes, to rotate the broadcast key (Possible values: 1..1440, Default Setting: 15).
- **Broadcast Filter All:** Enable or disable broadcast filtering. If enabled, all broadcast frames are dropped, except DHCP and Address Resolution Protocol (ARP) frames.
- **Broadcast Filter ARP:** Enable or disable broadcast filtering for ARP. If enabled, the AP acts 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 responds to the ARP request but does not forward the ARP request (broadcast) to all broadcast domains. This reduces ARP broadcast packet forwarding and significantly improves network performance.

  Note: APs do not act as ARP proxy for Gratuitous ARP packets. When the station gets an IP from DHCP or an IP release or renew, it will send Gratuitous ARP packets. AP does not respond to such special ARP packets and broadcasts them normally.
- **Multicast Optimization:** Enable or disable multicast traffic rate optimization.
- **Multicast Based Channel Utilization:** Configure multicast-based channel utilization optimization percentage. (Possible values: 0..100, Default Setting: 90)
- **Number of Clients:** Configure the threshold for multicast optimization. This is the maximum number of high throughputs.



Broadcast/Multicast Optimization Setting

Broadcast Key Rotation: ON

* Broadcast Key Rotation Time Interval: 15 mins

Broadcast Filter All: ON

Broadcast Filter ARP: ON

Multicast Optimization: ON

* Multicast Based Channel Utilization: 90 %

* Number Of Clients: 6

Figure 105: Broadcast/Multicast optimization settings

5.4 Edit WLAN

- □ Select the WLAN from the WLAN list.
- □ Click the **Edit** icon to open the **“Edit WLAN”** screen.
- □ Edit the fields that you need to change.
- □ Click the **“Effect Now”** button to save the changes to the server.

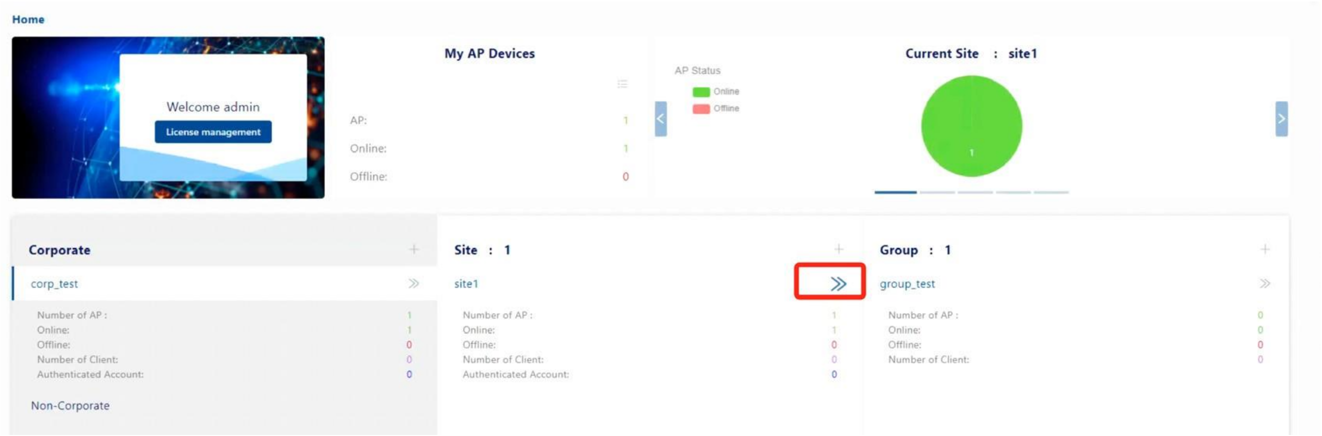
5.5 Delete WLAN

- □ Select the WLAN from the WLAN list.
- □ Click the **“Delete”** icon.
- □ Click **“Yes”** on the confirmation prompt. This removes the profile from the server.

6 AP

The AP screen displays information about all DAPs assigned to the Site. You can configure APs NTP, update the firmware of an AP, reboot an AP, set an APs LED Mode, and perform certain actions on APs (e.g., open the Web UI of the device to manage an individual AP, do some actions like ping or trace).

☐ Click **“>>”** at the Site, which enters the **“Site”** view.



My AP Devices

AP: 1
Online: 1
Offline: 0

Current Site : site1

Corporate

corp_test

Number of AP : 1
Online: 1
Offline: 0
Number of Client: 0
Authenticated Account: 0

Non-Corporate

Site : 1

site1

Number of AP : 1
Online: 1
Offline: 0
Number of Client: 0
Authenticated Account: 0

Group : 1

group_test

Number of AP : 0
Online: 0
Offline: 0
Number of Client: 0

Figure 106: Home Page

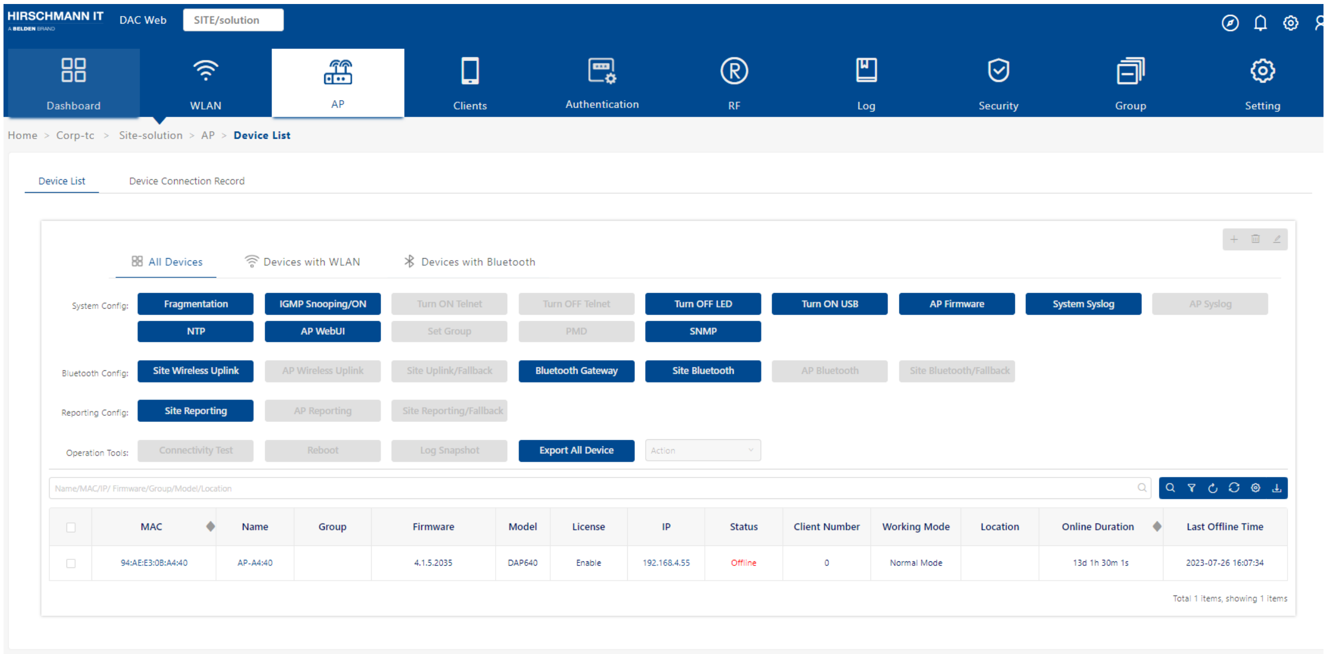
☐ Click the **“AP”** icon, and the **“AP”** screen displays.
This chapter contains the following topics:

- Device list
- Configurations for AP
- Configure Bluetooth
- Reporting config
- Operation tools
- Do actions from AP
- Device connections record

6.1 Device list

This list shows all AP devices on the Site. You can filter the device according to the basic functions of the AP, which include Wireless and Bluetooth.

- **All Devices:** The table shows all the devices on the Site.
- **Devices with WLAN:** The table shows devices with WLAN functionality. Only displayed when there are devices with WLAN functionality in the current Site.
- **Devices with Bluetooth:** The table shows devices with Bluetooth functionality. Only displayed when there are devices with Bluetooth functionality in the current Site.
- **MAC:** MAC address of the device.
- **Name:** Device Name.
- **Group:** Group of the device.
- **Firmware:** Firmware version of the device.
- **Model:** The model type of the Device (e.g., DAP640).
- **License:** License status of the device. If it is disabled, the DAC does not send the configuration to the DAP. So, the DAP does not broadcast an SSID.
- **IP:** The IP address of the device.
- **Status:** The AP status can be online or offline.
- **Client Number:** Clients are currently counted per device. 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:** In this mode, all radios under the AP will not broadcast an SSID.
- **Location:** Location of device.
- **Online Duration:** The online duration of the AP.
- **Last Offline Time:** The last time the device was disconnected.



□	MAC	Name	Group	Firmware	Model	License	IP	Status	Client Number	Working Mode	Location	Online Duration	Last Offline Time
□	94:AE:E3:0B:A4:40	AP-A4:40		4.1.5.2035	DAP640	Enable	192.168.4.55	Offline	0	Normal Mode		13d 1h 30m 1s	2023-07-26 16:07:34

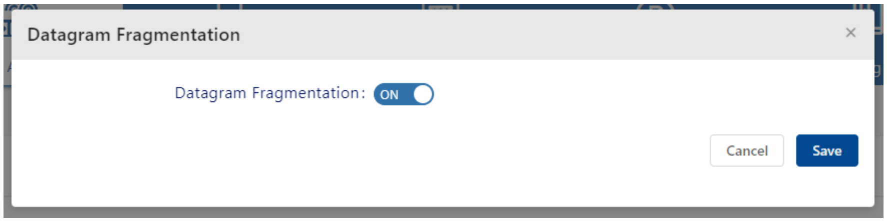
Total 1 items, showing 1 items

Figure 107: Device list window

6.2 Configurations for AP

6.2.1 Datagram fragmentation

UDP packet forwarding optimization is enabled to avoid excessive device load. The default is off.



Datagram Fragmentation

Datagram Fragmentation: ON

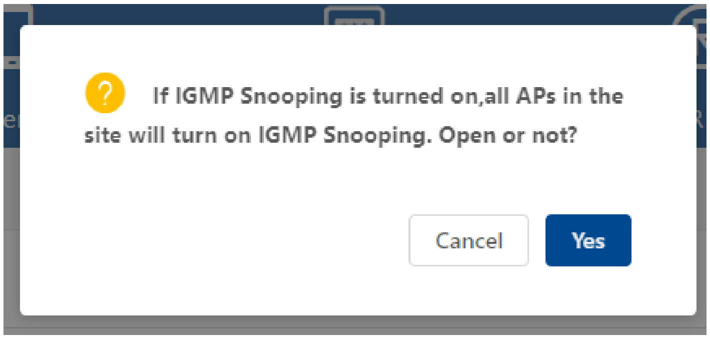
Figure 108: Datagram fragmentation

6.2.2 Turning on/off IGMP snooping

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

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic to control the 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 that do not need them, conserving bandwidth on those links.

- □ Click the **“IGMP Snooping/ON”** button to enable the **“IGMP Snooping”** function.
- □ Again, click the **“IGMP Snooping/ON”** button to disable the “**IGMP Snooping”** function.

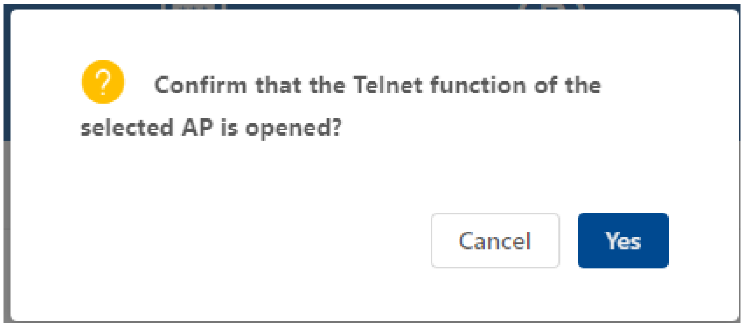


? If IGMP Snooping is turned on,all APs in the site will turn on IGMP Snooping. Open or not?

Figure 109: Turn On IGMP Snooping

6.2.3 Turning on/off telnet

- ☐ Select the APs that you want to enable telnet.
- ☐ Click the **"Turn On Telnet"** button.
- ☐ Click **"Yes"** on the confirmation prompt. The telnet function of selected APs will be turned on.
- ☐ No matter which AP's telnet in the current site gets enabled, then the **"Turn Off Telnet"** button becomes available. After clicking the **"Turn Off telnet"** button, the telnet of all APs in the current site is disabled.

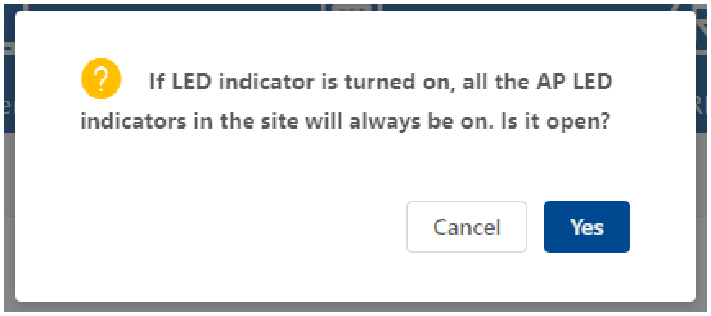


? Confirm that the Telnet function of the selected AP is opened?

Figure 110: Turning on/off Telnet

6.2.4 Turning on/off LED

- ☐ Click the **"Turn On LED"** button to turn the LED on. This setting is effective for all APs on the current Site.
- ☐ The button changes to **"Turn Off LED"**, and you can click it to turn off LEDs for all APs in the current Site.



If LED indicator is turned on, all the AP LED indicators in the site will always be on. Is it open?

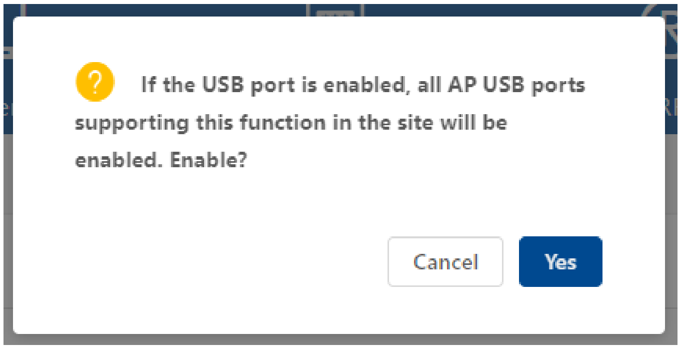
Figure 111: Turn On LED

6.2.5 Turning on/off USB

- □ Click the **"Turn On/Off USB"** button to enable or disable the USB port on your device.

This setting is effective for the devices on the current Site. This function is only effective for devices with a USB interface.

Note: When the power supply is insufficient, the USB interface on the device may also be unsuccessful to open.

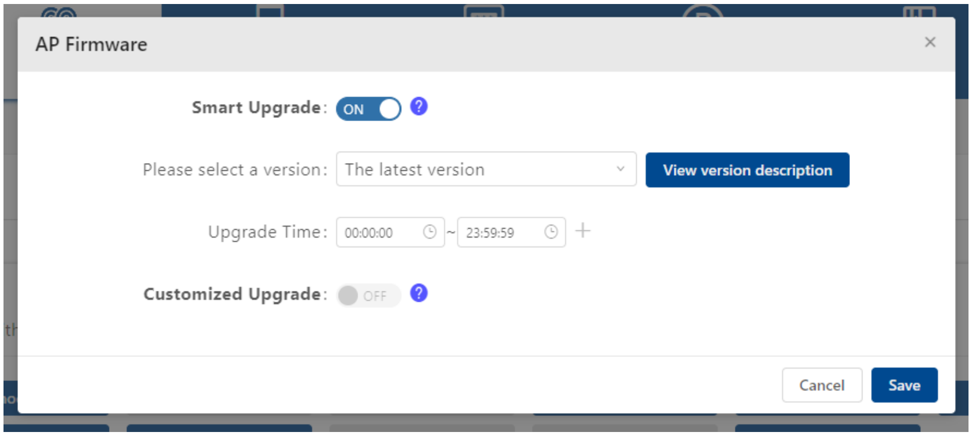


If the USB port is enabled, all AP USB ports supporting this function in the site will be enabled. Enable?

Figure 112: Turn On USB

6.2.6 Firmware upgrade

- □ Click the **"AP Firmware"** button, and the "AP **Firmware"** window opens.
- □ You can configure the firmware upgrade strategy. It includes **"Smart Upgrade"** and **"Customization Upgrade"**. You can only select one of them for a firmware upgrade.



AP Firmware

Smart Upgrade: ON

Please select a version: The latest version

View version description

Upgrade Time: 00:00:00 ~ 23:59:59 +

Customized Upgrade: OFF

Cancel Save

Figure 113: Firmware window

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 the cloud, you get DAP firmware from the supplier and upload firmware to DAC manually. See “AP local firmware management” on page 54. Then choose **“Smart Upgrade”** or **“Customization Upgrade”**, and the DAP downloads the firmware required for the upgrade from the DAC.

- **Smart Upgrade:** You should select a firmware version and set the upgrade time periods that you want the devices to upgrade. Usually, you should choose the latest version, which means that the DAC will try to synchronize the latest version from the cloud every day. It will automatically complete the firmware upgrade of the AP according to the rules of the smart upgrade.

  If you are not sure which version to choose, you can contact the supplier. Once the upgrade time period that you set is reached, all devices in the 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 the current Site are not upgraded 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 the 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 of the devices.

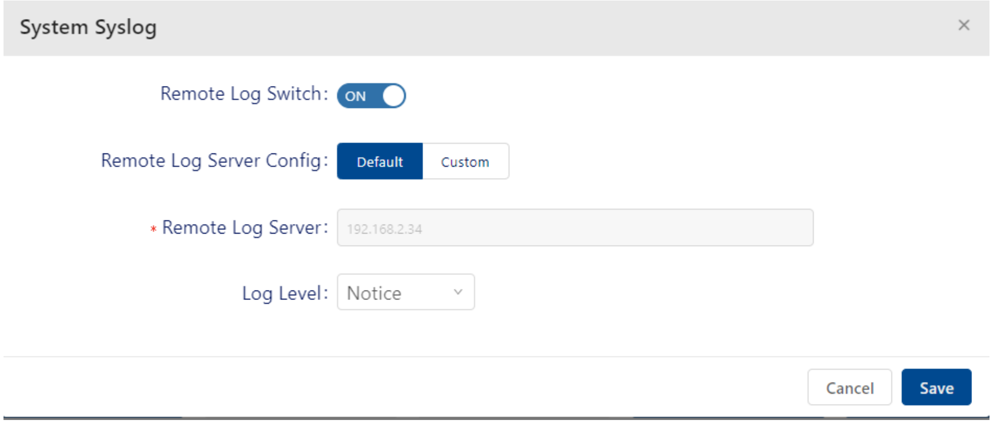
- **Customization Upgrade:** The customization upgrade task will only be updated at the set time. The task is automatically cleared after the device upgrade (only once). If the device upgrade is unsuccessful, you need to manually perform the next upgrade. This is the main difference from Smart upgrade.

6.2.7 Device syslog config

To locate the problem with 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 AP reporting logs under the current Site or select an AP and click the **“AP Syslog”** button to set the address of the selected AP reporting log.

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



System Syslog

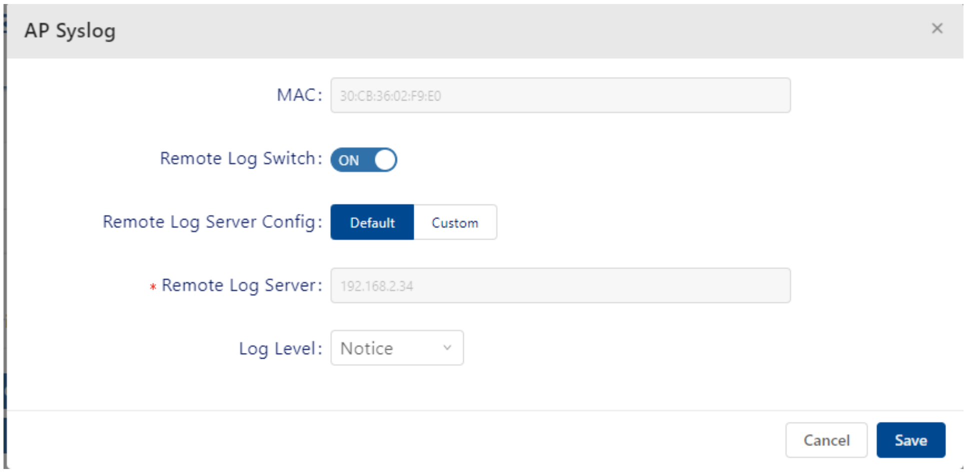
Remote Log Switch: ON

Remote Log Server Config: Default | Custom

* Remote Log Server: 192.168.2.34

Log Level: Notice

Figure 114: System Syslog



AP Syslog

MAC: 30:CB:36:02:F9:E0

Remote Log Switch: ON

Remote Log Server Config: Default | Custom

* Remote Log Server: 192.168.2.34

Log Level: Notice

Figure 115: AP Syslog

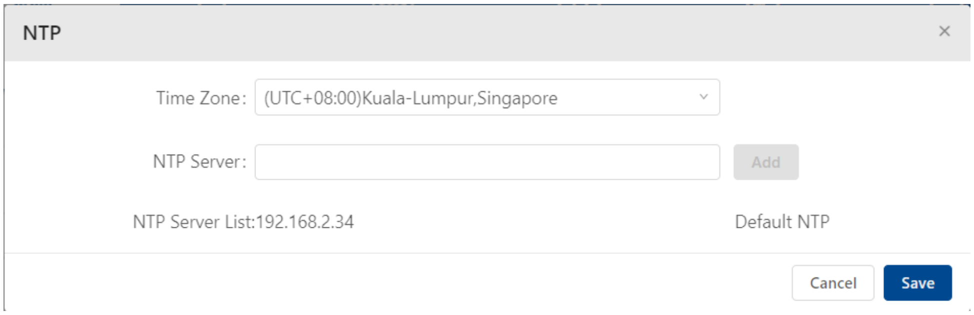
6.2.8 Configuring NTP of device

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

□ Click the **"NTP"** button. Then the **"NTP Config"** window opens.

- ▶ **Time Zone:** Select a time zone from the drop-down list.
- ▶ **NTP Server:** Enter the **"NTP Server address"**. Click the **"Add"** button to add a device to the NTP Server List. DAC has a built-in NTP Server. By default, it will send this NTP Server to devices in the current Site. By this way, the time synchronization between DAP and DAC is maintained.
- ▶ **NTP Server List:** NTP Server List currently added.

□ Click the **"Save"** button to save the configurations and apply these configurations to devices on this Site. The currently supported NTP protocol is version 4.



NTP

Time Zone: (UTC+08:00)Kuala-Lumpur,Singapore

NTP Server:

NTP Server List:192.168.2.34

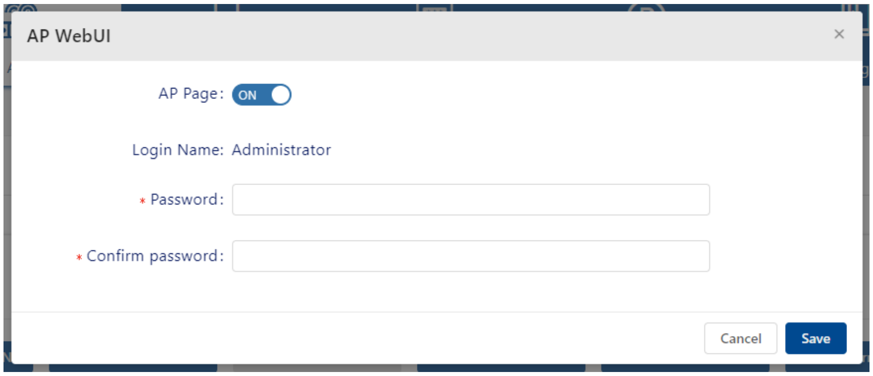
Default NTP

Figure 116: NTP

6.2.9 Access to AP Web UI

It is necessary to directly access the WebUI of an AP device for some maintenance operations.

- ☐ Click the **“AP WebUI”** button to open the **“AP WebUI”** module window.
  - ▶ **AP Page:** Turn On or Off AP WebUI.
  - ▶ **Login Name:** The login name must be **“administrator”**.
  - ▶ **Password:** The password of the administrator. You can log in to AP WebUI with this password.
  - ▶ **Confirm password:** Confirm the password.
- ☐ Click the **Save** button to save the configurations.
- ☐ Click **“IP Address”** in the Device List to access the AP's WebUI.
- ☐ Enter the **“Password”** to log in to the AP WebUI Page.



AP WebUI

AP Page: ON

Login Name: Administrator

* Password:

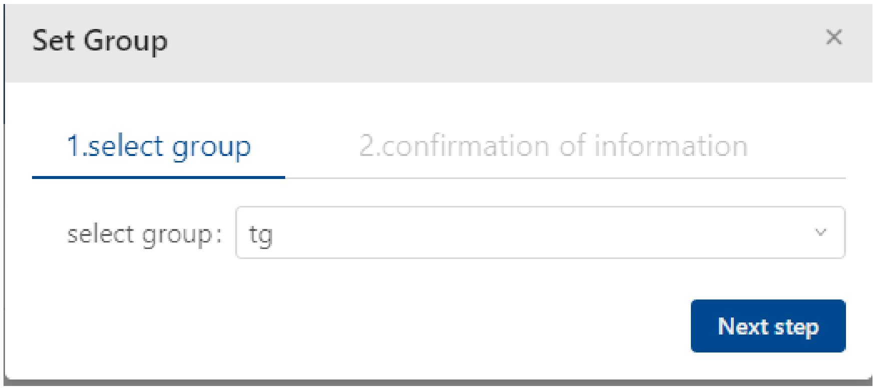
* Confirm password:

Figure 117: AP Web UI

6.2.10 Assign APs to Group

□ Select APs from the Device List.
□ Click the **“Set Group”** button, and the **“Set Group”** module window opens.
□ Select a Group from the drop-down list.
□ Click the **“Next step”** button, and the confirmation of information view opens.
□ Click the **“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 a new Group. See “Create a new Group” on page 28.



select group: tg

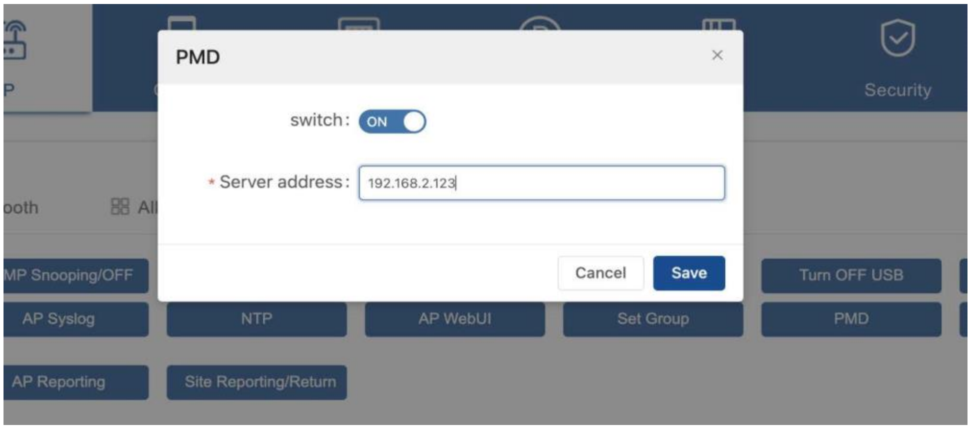
Figure 118: Assign APs to Group

6.2.11 PMD

PMD is a troubleshooting method that helps identify the 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 a key process crashes on the DAP. By default, sending PMD files to an external TFTP server is disabled.

□ Select the APs that you want to collect PMD files from the AP list.
□ Click the **“PMD”** button. Then the **“PMD”** window appears.
□ Turn on the **“Switch”**.
□ Enter the **“Server address”** with TFTP server address.
□ Click the **“Save”** button to save the config.



PMD

switch: ON

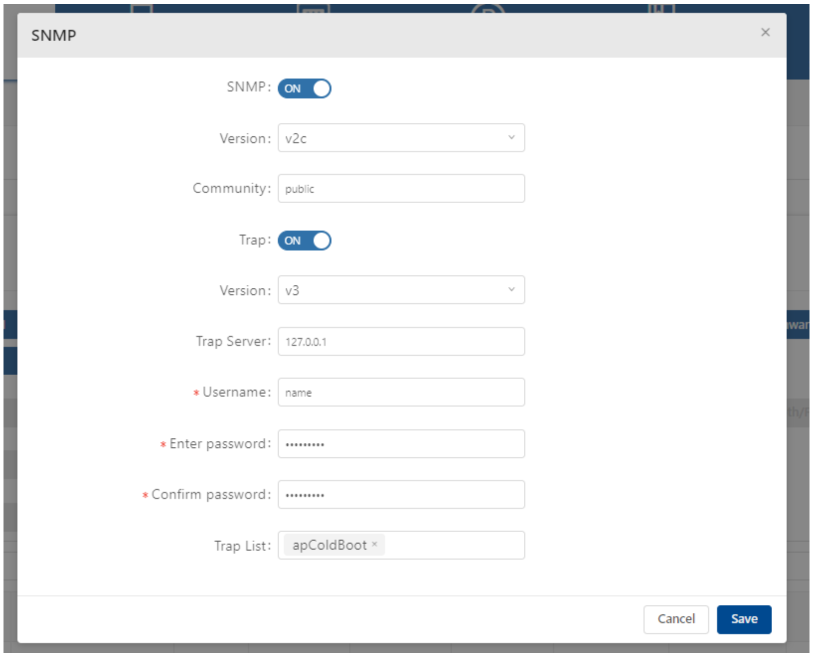
* Server address: 192.168.2.123

Figure 119: PMD window

6.2.12 SNMP

SNMP is an application layer protocol which helps to record, store, and share information about the SNMP-enabled devices in the network, in order to give you deeper insights into the workings of the devices. The SNMP trap is the message sent by the agent to the manager. It is sent when a preset event occurred.

- □ The SNMP configuration takes effect on all APs in the site.
- □ Click the “**SNMP”** button. Then the **“Edit SNMP”** window appears.
  - ▶ **SNMP:** Turn on/off the SNMP configuration.
  - ▶ **Version:** The version of SNMP. v2c and v3 are supported.
  - ▶ **Community:** A community string used to access to the AP’s statistics.
  - ▶ **Trap:** Turn on/off the SNMP Trap configuration.
  - ▶ **Trap Server:** The IP address of the SNMP trap host.
  - ▶ **Username:** The name of the user used for the host to connect to agents. Need to be filled in when v3 version is chosen.
  - ▶ **Enter Password:** The password of the user used for the host to connect to agents. Need to be filled in when v3 version is chosen.
  - ▶ **Confirm Password:** Enter the password again to check consistency. Need to be filled in when v3 version is chosen.
  - ▶ **Trap List:** The kind of events sent by the SNMP agent.



SNMP

SNMP: ON

Version: v2c

Community: public

Trap: ON

Version: v3

Trap Server: 127.0.0.1

* Username: name

* Enter password: •••••••••

* Confirm password: •••••••••

Trap List: apColdBoot ×

Figure 120: SNMP window

6.3 Configure Bluetooth

6.3.1 Bluetooth configurations

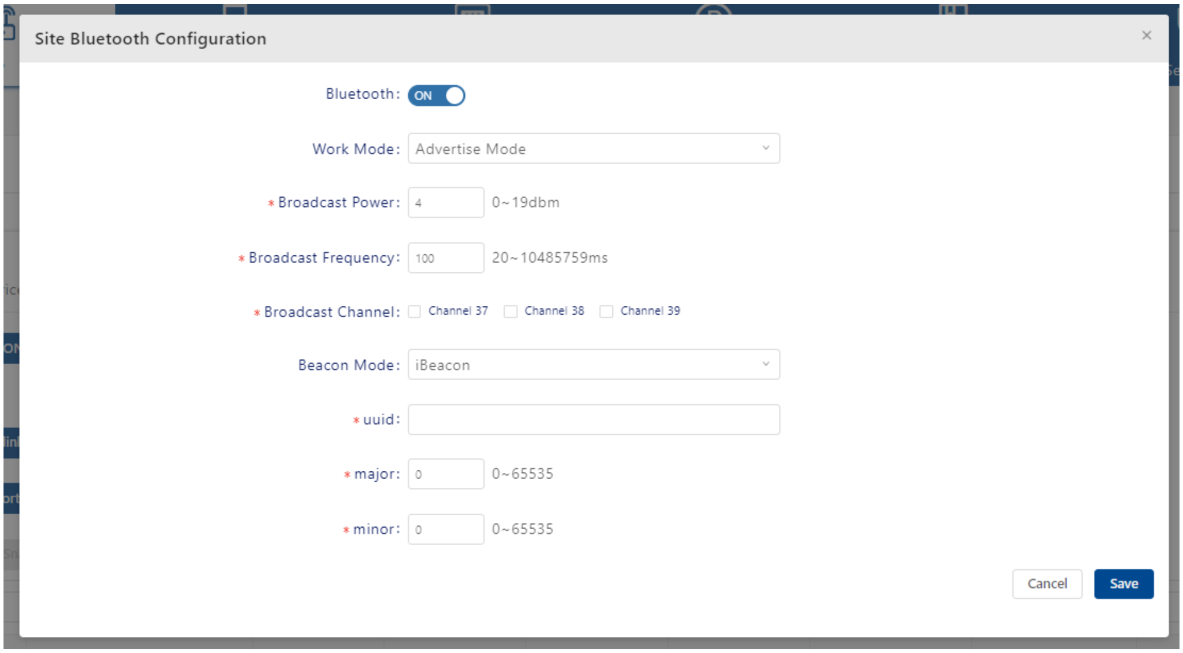
You can set the Bluetooth configuration of the whole Site or select a specific AP for private Bluetooth configuration. The AP's private Bluetooth configuration takes precedence over the Site's overall configuration.

- □ Select the AP.
- □ Click the **“Site Bluetooth/Fallback”** button to clear the independent Bluetooth configuration of the AP. These APs reuse the Bluetooth configuration of the Site.
- □ Click the **“Site Bluetooth”** button to open the **“Site Bluetooth Configuration”** module window or select AP.
- □ Click the **“AP Bluetooth”** button to open the **“AP Bluetooth Configuration”** module window.
  - ▶ **Bluetooth:** Switch off Bluetooth. If On, all Bluetooth devices in the Site or the selected devices turn on 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 broadcasts BLE packets.
    - **Advertise & Scanner Mode:** Enable **“Bluetooth beacon scanning”** and **“BLE advertising”** functions.

- ■ **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. (Possible values: 4..10240, Default Setting: 100)
  - ▶ **Scan Window:** Duration of each scan, in milliseconds. (Possible values: 4..10240)
  - ▶ **Scan Filter:** Enable or disable scan filter.

- **Details of Advertise Mode**
  - **Broadcast Power:** The transmit power used to broadcast BLE packets. (Possible values: - 20..- 10, Default Setting: 4)
  - **Broadcast Frequency:** The time circle during which the BLE packets will be broadcast, in milliseconds. (Possible values: 20..9,000,000, Default Setting: 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 Eddystone format.

    A unique static ID with a 10-byte Namespace component and a 6-byte Instance component.
      - **Namespace:** 20 characters containing 0-9, a-f.
      - **Instance ID:** 12 characters containing 0-9, a-f.
  - **Edyurl:** Google Eddystone format. A compressed URL that, once parsed and decompressed, is directly usable by the client.
  - **Plain_URL:** Plain URL which will be compressed.



Site Bluetooth Configuration

Bluetooth: ON

Work Mode: Advertise Mode

* Broadcast Power: 4 0~19dbm

* Broadcast Frequency: 100 20~10485759ms

* Broadcast Channel: □ Channel 37 □ Channel 38 □ Channel 39

Beacon Mode: iBeacon

* uuid:

* major: 0 0~65535

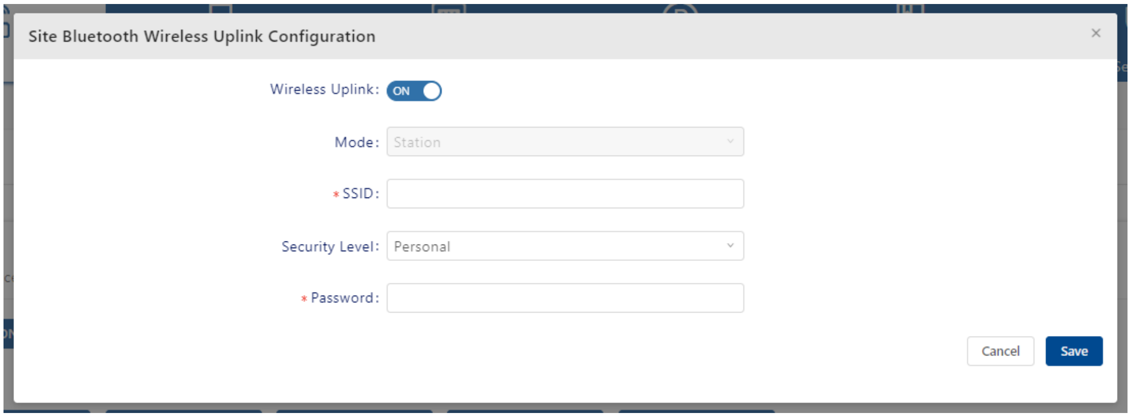
* minor: 0 0~65535

Figure 121: Site Bluetooth Configuration

6.3.2 Config Bluetooth and the 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 or data link to complete the device registration, Bluetooth information reporting, etc.

- Click the **“Site Wireless Uplink”** button and open the **“Site Bluetooth Wireless Uplink Configuration”** window. Or click the **“AP Wireless Uplink”** button and the **“Bluetooth Wireless Uplink Configuration”** window.
- Click the **“Save”** button to apply configurations to Bluetooth Devices on the Site.
  - **Wireless Uplink:** WLAN uplink status on/off.
  - **Mode:** Station (Cannot change).
  - **SSID:** SSID of the Bluetooth device that will connect.
  - **Security Level:** The security level of the SSID to which this Bluetooth device will connect. It can be Open or Personal.
  - **Password:** When the security level is Personal, you should set a password.



Site Bluetooth Wireless Uplink Configuration

Wireless Uplink: ON

Mode: Station

* SSID:

Security Level: Personal

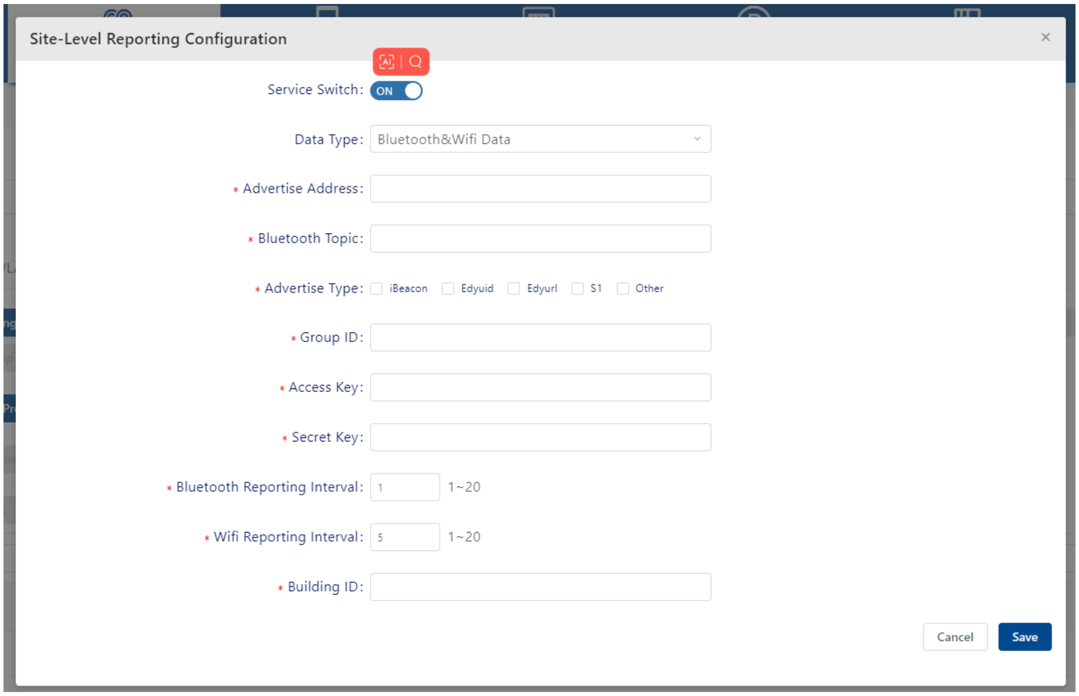
* Password:

Figure 122: Site Bluetooth Uplink Configuration

6.4 Reporting config

The Reporting Config function is used to set the AP device to report information, such as the terminal list, RSSI, etc., to the third-party system through an MQTT broker. The third-party system can make some new applications based on this information, such as indoor location, etc.

- □ Click the **“Site Reporting”** button to set all devices to report information.
- □ Select devices and click the **“AP Reporting”** button to set the selected devices to report information.
  - ▶ **Service Switch:** Enable or disable the switch service.
  - ▶ **Data Type:** Select Bluetooth Data, Wi-Fi Data, or Both of them.
  - ▶ **Advertise Address:** Advertise Address.
  - ▶ **Bluetooth Topic:** Send messages to the MQTT broker with Bluetooth Topic.
  - ▶ **Advertise Type:**
    - **iBeacon:** Apple developed the iBeacon protocol. This protocol determines the device's physical location, tracks customers, or triggers a location-based action on the device.
    - **Edyuid:** Google Eddystone format.
      - A unique static ID with a 10-byte Namespace component and a 6-byte Instance component.
    - **Edyurl:** Google Eddystone format. A compressed URL that, once parsed and decompressed, is directly usable by the client.
    - **Other:** Other advertise type.
  - ▶ **Group ID:** Group ID of the device.
  - ▶ **Access Key:** Access key to connect to an MQTT broker.
  - ▶ **Secret Key:** The Secret key to connect to an MQTT broker.
  - ▶ **Bluetooth Reporting Interval:** Reporting interval of Bluetooth messages (Possible values: 1..20).
  - ▶ **Wifi Reporting Interval:** Reporting interval of Wi-Fi messages (Possible values: 1..20).
  - ▶ **Building ID:** Building ID.



Site-Level Reporting Configuration

Service Switch: ON

Data Type: Bluetooth&Wifi Data

* Advertise Address:

* Bluetooth Topic:

* Advertise Type: □ iBeacon □ Edyuid □ Edyurl □ S1 □ Other

* Group ID:

* Access Key:

* Secret Key:

* Bluetooth Reporting Interval: 1 1~20

* Wifi Reporting Interval: 5 1~20

* Building ID:

Figure 123: Site Report Configuration

6.5 Operation tools

Operation tools provide a set of small tools that facilitate users carrying out simple operations and maintenance operations.

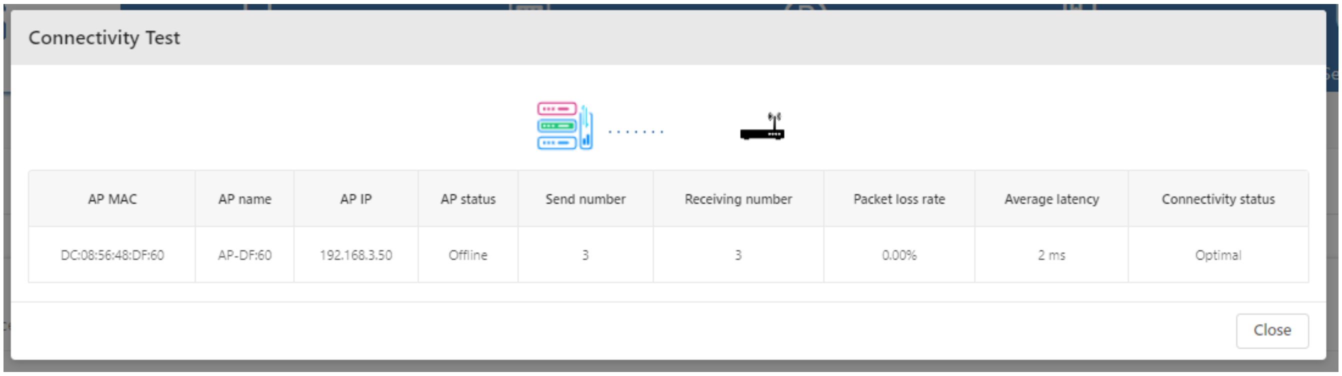
6.5.1 Connectivity test

The connectivity test is used to test whether the selected device can be reached from the DAC through the ping command.

□ Select one or more APs (no more than 10).

□ Click the **“Connectivity Testing”** button. The **“Connectivity Testing”** dialog appears in a few seconds. You will see a table containing the Ping results.

- **AP MAC:** AP MAC.
- **AP name:** Name of the AP.
- **AP IP:** IP Address of the AP.
- **AP status:** AP status is online or offline.
- **Send number**: The number of ping packages sent.
- **Receiving number:** The number of packages received.
- **Package loss rate:** Package loss rate.
- **Average latency:** Average latency.
- **Connectivity status:** The network connectivity status, “Optimal” or “Abnormal”.



AP MAC	AP name	AP IP	AP status	Send number	Receiving number	Packet loss rate	Average latency	Connectivity status
DC:08:56:48:DF:60	AP-DF:60	192.168.3.50	Offline	3	3	0.00%	2 ms	Optimal

Figure 124: Connectivity Test

6.5.2 Reboot a device

□ Select the device to reboot manually.
□ Click the **“Reboot”** button.

When the device is rebooted, it reconnects to the DAC. Then, the latest configuration available on the DAC is downloaded to the AP. If the AP is unable to connect to the DAC, the AP reboots with the latest saved local configuration.

6.5.3 Log snapshot

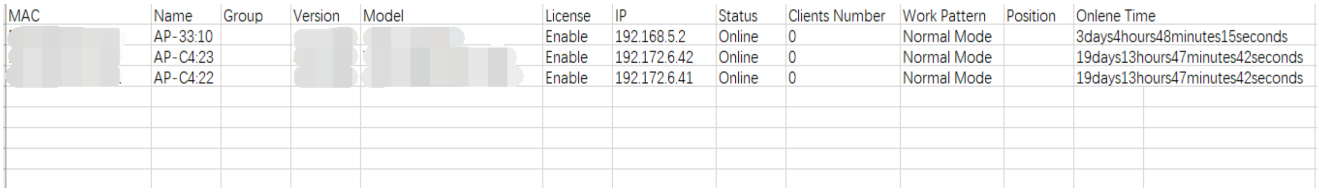
Sometimes it is necessary to collect some information from the device to facilitate R&D and find problems.

□ Select a device.
□ Click the **“Log Snapshot”** button.

It is needed to wait a moment for the device to upload its snapshot log file to DAC. You need to stay on the current page during file uploading. When the file transfer is complete, the browser automatically starts downloading the file.

6.5.4 Export all device information

Click the **“Export All Device”** button. You can export the information of all devices from the Site. In the download file window, you can change the export file name. The file type is xlsx, which can be opened with Microsoft Office Excel.

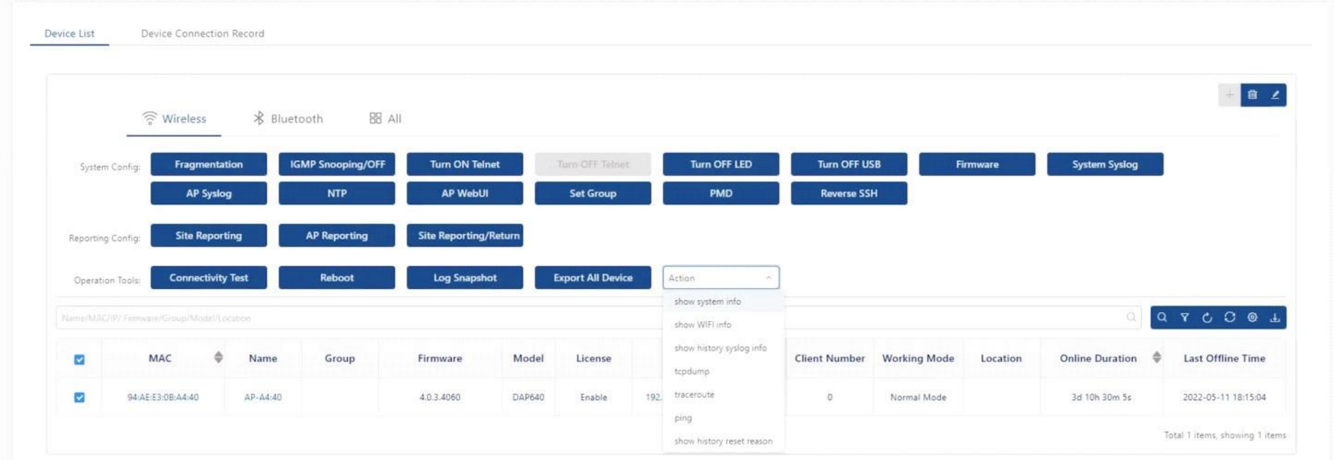


MAC	Name	Group	Version	Model	License	IP	Status	Clients Number	Work Pattern	Position	Onlene Time
[redacted]	AP-33:10		[redacted]	[redacted]	Enable	192.168.5.2	Online	0	Normal Mode		3days4hours48minutes15seconds
[redacted]	AP-C4:23		[redacted]	[redacted]	Enable	192.172.6.42	Online	0	Normal Mode		19days13hours47minutes42seconds
[redacted]	AP-C4:22		[redacted]	[redacted]	Enable	192.172.6.41	Online	0	Normal Mode		19days13hours47minutes42seconds

Figure 125: Exported All Devices List

6.6 Do actions from AP

Executes a specific command on the device and returns the output of the command. You can perform actions from the drop-down list.



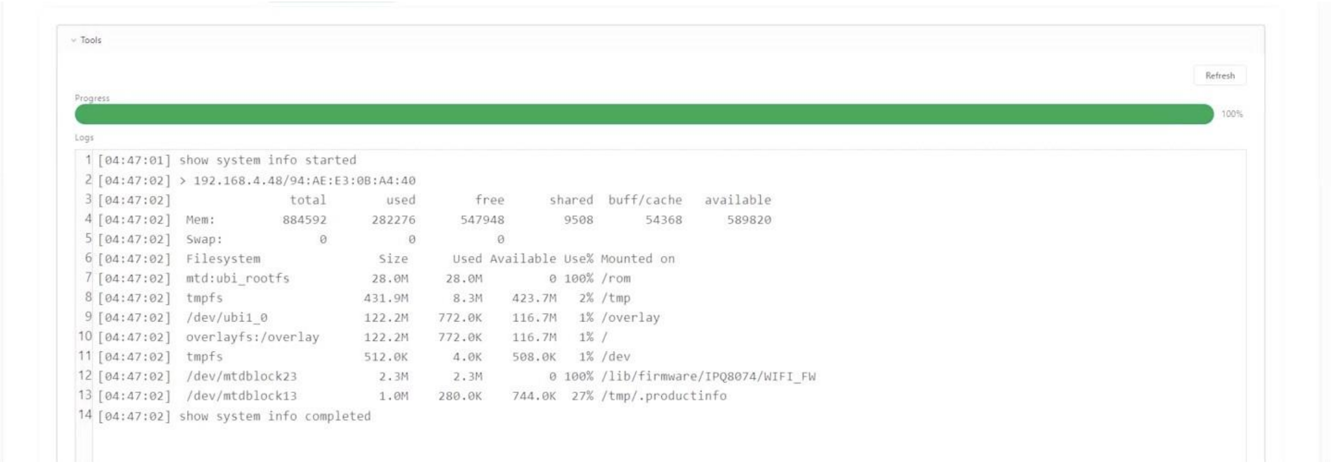
☑	MAC	Name	Group	Firmware	Model	License		Client Number	Working Mode	Location	Online Duration	Last Offline Time
☑	94:AE:E3:0B:A4:40	AP-A4:40		4.0.3.4060	DAP640	Enable	192.	0	Normal Mode		3d 10h 30m 5s	2022-05-11 18:15:04

Total 1 items, showing 1 items

Figure 126: Actions drop-down menu

6.6.1 Show system info

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



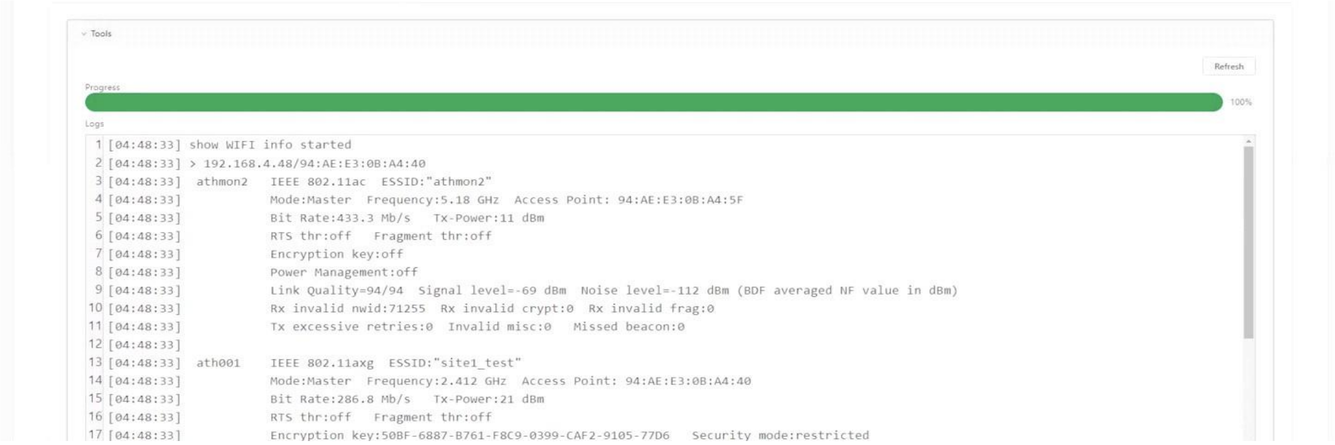
```
[04:47:01] show system info started
[04:47:02] > 192.168.4.48/94:AE:E3:0B:A4:40
[04:47:02]               total        used        free      shared  buff/cache   available
[04:47:02]  Mem:         884592      282276      547948        9508       54368      589820
[04:47:02]  Swap:             0           0           0
[04:47:02]  Filesystem                Size      Used Available Use% Mounted on
[04:47:02]  mtd:ubi_rootfs           28.0M     28.0M         0 100% /rom
[04:47:02]  tmpfs                   431.9M      8.3M    423.7M   2% /tmp
[04:47:02]  /dev/ubi1_0             122.2M    772.0K    116.7M   1% /overlay
[04:47:02]  overlayfs:/overlay      122.2M    772.0K    116.7M   1% /
[04:47:02]  tmpfs                   512.0K      4.0K    508.0K   1% /dev
[04:47:02]  /dev/mtdblock23           2.3M      2.3M         0 100% /lib/firmware/IPQ8074/WIFI_FW
[04:47:02]  /dev/mtdblock13           1.0M    280.0K    744.0K  27% /tmp/.productinfo
[04:47:02] show system info completed
```

Figure 127: Show system info

6.6.2 Show WIFI info

It shows the wireless interface information of the specified DAP, which includes:

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

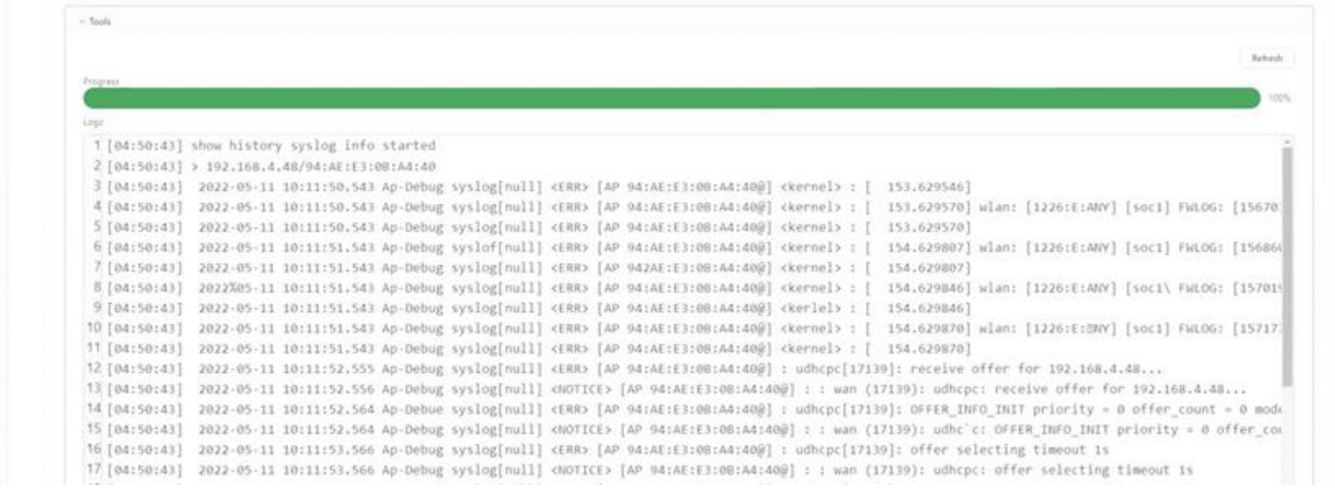


```
[04:48:33] show WIFI info started
[04:48:33] > 192.168.4.48/94:AE:E3:0B:A4:40
[04:48:33]  athmon2   IEEE 802.11ac  ESSID:"athmon2"
[04:48:33]            Mode:Master  Frequency:5.18 GHz  Access Point: 94:AE:E3:0B:A4:5F
[04:48:33]            Bit Rate:433.3 Mb/s   Tx-Power:11 dBm
[04:48:33]            RTS thr:off   Fragment thr:off
[04:48:33]            Encryption key:off
[04:48:33]            Power Management:off
[04:48:33]            Link Quality=94/94  Signal level=-69 dBm  Noise level=-112 dBm (BDF averaged NF value in dBm)
[04:48:33]            Rx invalid nwid:71255  Rx invalid crypt:0  Rx invalid frag:0
[04:48:33]            Tx excessive retries:0  Invalid misc:0   Missed beacon:0
[04:48:33]
[04:48:33]  ath001    IEEE 802.11axg  ESSID:"site1_test"
[04:48:33]            Mode:Master  Frequency:2.412 GHz  Access Point: 94:AE:E3:0B:A4:40
[04:48:33]            Bit Rate:286.8 Mb/s   Tx-Power:21 dBm
[04:48:33]            RTS thr:off   Fragment thr:off
[04:48:33]            Encryption key:50BF-6887-B761-F8C9-0399-CAF2-9105-77D6   Security mode:restricted
```

Figure 128: Show WIFI info

6.6.3 Show history syslog info

It shows the historic Syslog messages generated since the last time the system was running (Before this time system up) of the specified DAP.

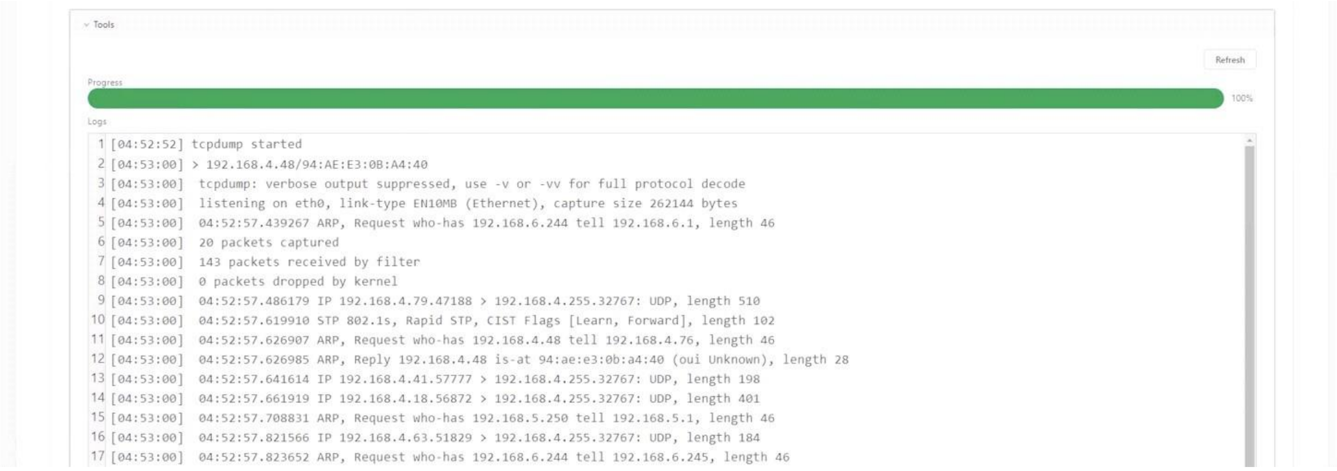


```
[04:50:43] show history syslog info started
[04:50:43] > 192.168.4.48/94:AE:E3:0B:A4:40
[04:50:43]  2022-05-11 10:11:50.543 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:0B:A4:40@] <kernel> : [  153.629546]
[04:50:43]  2022-05-11 10:11:50.543 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:0B:A4:40@] <kernel> : [  153.629570] wlan: [1226:E:ANY] [soc1] FWLOG: [15670
[04:50:43]  2022-05-11 10:11:50.543 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:0B:A4:40@] <kernel> : [  153.629570]
[04:50:43]  2022-05-11 10:11:51.543 Ap-Debug syslof[null] <ERR> [AP 94:AE:E3:0B:A4:40@] <kernel> : [  154.629807] wlan: [1226:E:ANY] [soc1] FWLOG: [15686
[04:50:43]  2022-05-11 10:11:51.543 Ap-Debug syslog[null] <ERR> [AP 942AE:E3:0B:A4:40@] <kernel> : [  154.629807]
[04:50:43]  2022%05-11 10:11:51.543 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:0B:A4:40@] <kernel> : [  154.629846] wlan: [1226:E:ANY] [soc1\ FWLOG: [15701
[04:50:43]  2022-05-11 10:11:51.543 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:0B:A4:40@] <kerlel> : [  154.629846]
[04:50:43]  2022-05-11 10:11:51.543 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:0B:A4:40@] <kernel> : [  154.629870] wlan: [1226:E:ANY] [soc1] FWLOG: [15717
[04:50:43]  2022-05-11 10:11:51.543 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:0B:A4:40@] <kernel> : [  154.629870]
[04:50:43]  2022-05-11 10:11:52.555 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:0B:A4:40@] : udhcpc[17139]: receive offer for 192.168.4.48...
[04:50:43]  2022-05-11 10:11:52.556 Ap-Debug syslog[null] <NOTICE> [AP 94:AE:E3:0B:A4:40@] : : wan (17139): udhcpc: receive offer for 192.168.4.48...
[04:50:43]  2022-05-11 10:11:52.564 Ap-Debue syslog[null] <ERR> [AP 94:AE:E3:0B:A4:40@] : udhcpc[17139]: OFFER_INFO_INIT priority = 0 offer_count = 0 mod
[04:50:43]  2022-05-11 10:11:52.564 Ap-Debug syslog[null] <NOTICE> [AP 94:AE:E3:0B:A4:40@] : : wan (17139): udhc`c: OFFER_INFO_INIT priority = 0 offer_co
[04:50:43]  2022-05-11 10:11:53.566 Ap-Debug syslog[null] <ERR> [AP 94:AE:E3:0B:A4:40@] : udhcpc[17139]: offer selecting timeout 1s
[04:50:43]  2022-05-11 10:11:53.566 Ap-Debug syslog[null] <NOTICE> [AP 94:AE:E3:0B:A4:40@] : : wan (17139): udhcpc: offer selecting timeout 1s
```

Figure 129: Show history syslog info

6.6.4 Tcpdump

The “tcpdump” action captures many packets on the device.

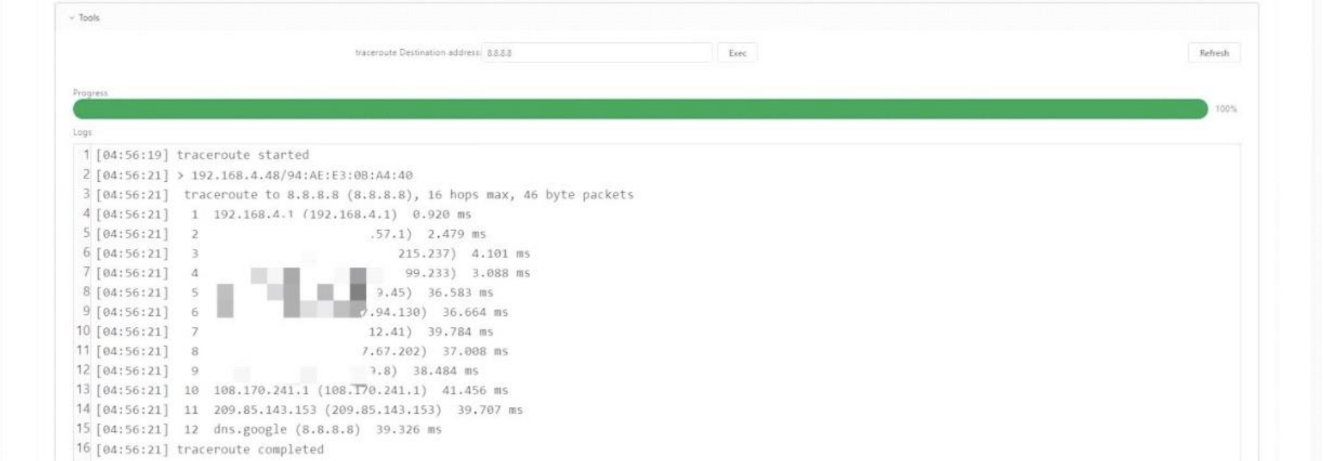


```
[04:52:52] tcpdump started
[04:53:00] > 192.168.4.48/94:AE:E3:0B:A4:40
[04:53:00]  tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
[04:53:00]  listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
[04:53:00]  04:52:57.439267 ARP, Request who-has 192.168.6.244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

Figure 130: Tcpdump command

6.6.5 Traceroute

Traceroute from the specified DAP to another host in the network.



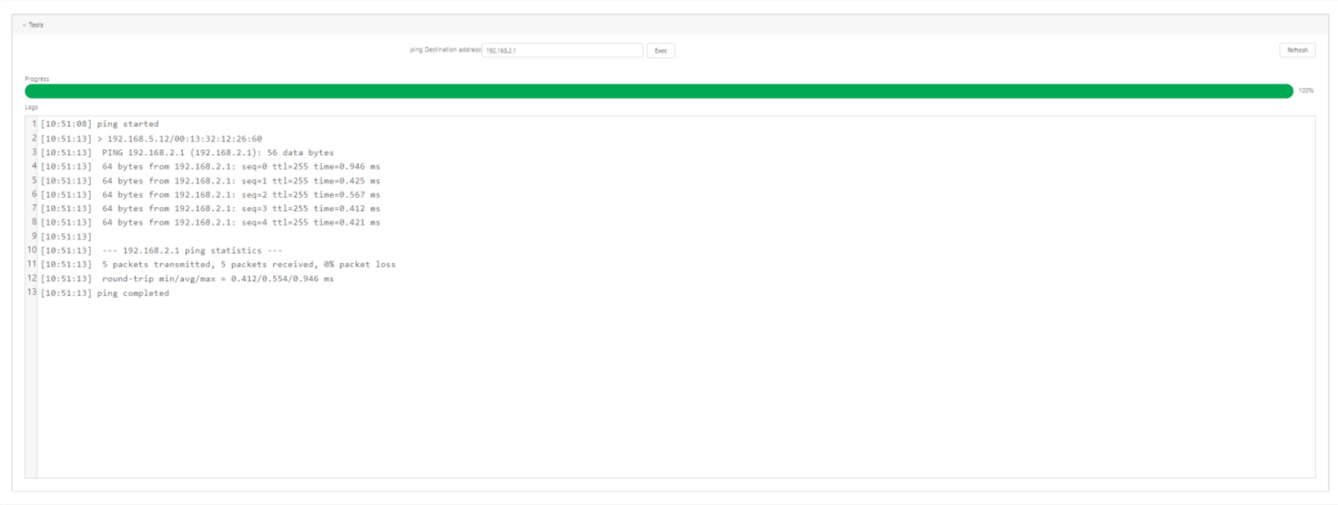
traceroute Destination address: 8.8.8.8

```
[04:56:19] traceroute started
[04:56:21] > 192.168.4.48/94:AE:E3:0B:A4:40
[04:56:21]  traceroute to 8.8.8.8 (8.8.8.8), 16 hops max, 46 byte packets
[04:56:21]   1  192.168.4.1 (192.168.4.1)  0.920 ms
[04:56:21]   2  [redacted]             .57.1)  2.479 ms
[04:56:21]   3                           215.237)  4.101 ms
[04:56:21]   4                            99.233)  3.088 ms
[04:56:21]   5                        9.45)  36.583 ms
[04:56:21]   6                        .94.130)  36.664 ms
[04:56:21]   7                        12.41)  39.784 ms
[04:56:21]   8                       7.67.202)  37.008 ms
[04:56:21]   9                        .8)  38.484 ms
[04:56:21]  10  108.170.241.1 (108.170.241.1)  41.456 ms
[04:56:21]  11  209.85.143.153 (209.85.143.153)  39.707 ms
[04:56:21]  12  dns.google (8.8.8.8)  39.326 ms
[04:56:21] traceroute completed
```

Figure 131: Traceroute command

6.6.6 Ping

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



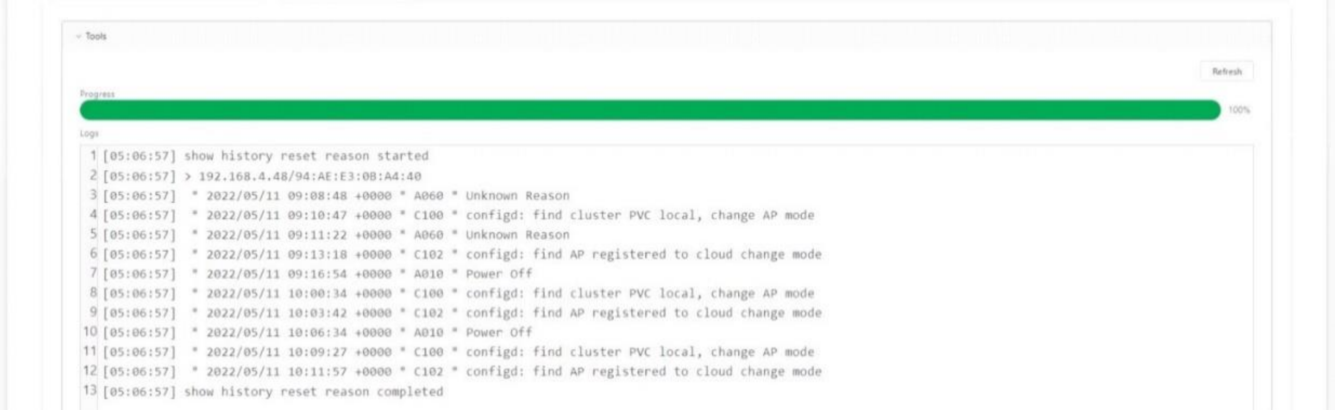
ping Destination address: 192.168.2.1

```
[10:51:08] ping started
[10:51:13] > 192.168.5.12/00:13:32:12:26:60
[10:51:13]  PING 192.168.2.1 (192.168.2.1): 56 data bytes
[10:51:13]  64 bytes from 192.168.2.1: seq=0 ttl=255 time=0.946 ms
[10:51:13]  64 bytes from 192.168.2.1: seq=1 ttl=255 time=0.425 ms
[10:51:13]  64 bytes from 192.168.2.1: seq=2 ttl=255 time=0.567 ms
[10:51:13]  64 bytes from 192.168.2.1: seq=3 ttl=255 time=0.412 ms
[10:51:13]  64 bytes from 192.168.2.1: seq=4 ttl=255 time=0.421 ms
[10:51:13]
[10:51:13]  --- 192.168.2.1 ping statistics ---
[10:51:13]  5 packets transmitted, 5 packets received, 0% packet loss
[10:51:13]  round-trip min/avg/max = 0.412/0.554/0.946 ms
[10:51:13] ping completed
```

Figure 132: Ping command

6.6.7 Show history reset reason

It shows the latest ten reboot records of the specified DAP, which include reboot time and reboot reason. It is the same output for the command reset_record under DAP CLI mod.



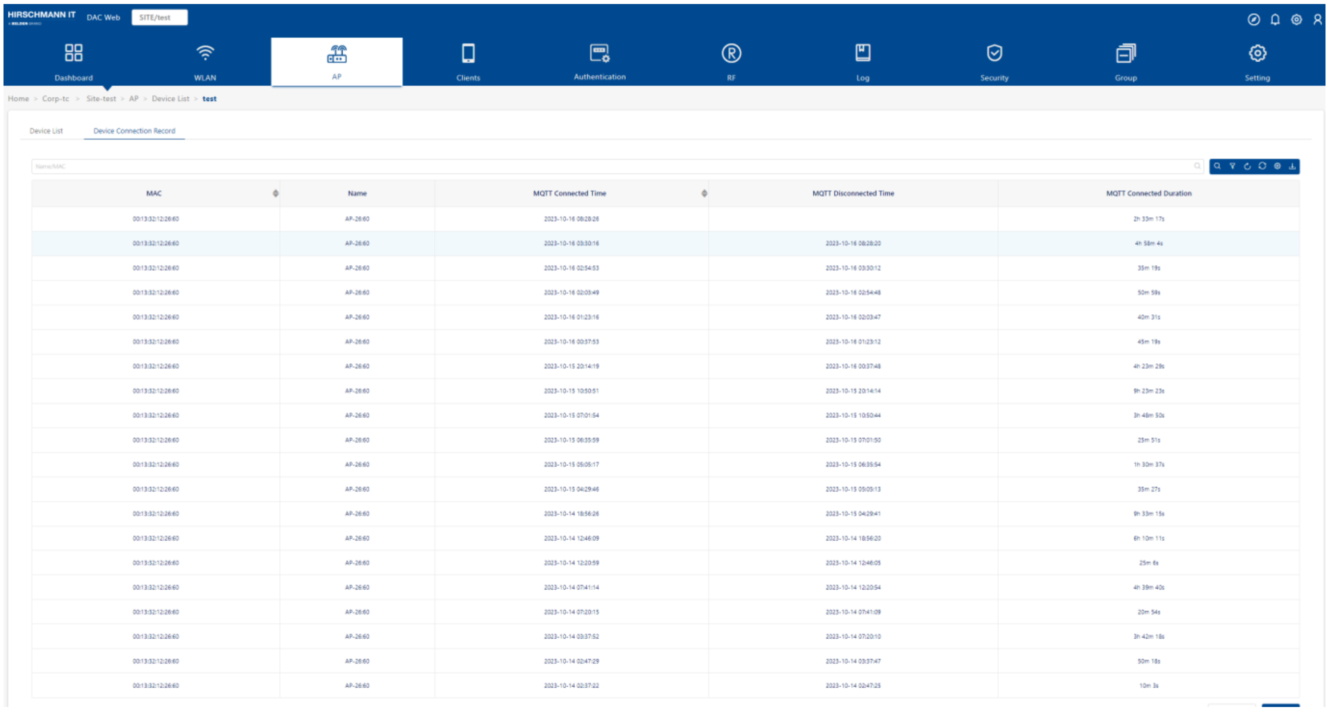
```
[05:06:57] show history reset reason started
[05:06:57] > 192.168.4.48/94:AE:E3:0B:A4:40
[05:06:57]  * 2022/05/11 09:08:48 +0000 * A060 * Unknown Reason
[05:06:57]  * 2022/05/11 09:10:47 +0000 * C100 * configd: find cluster PVC local, change AP mode
[05:06:57]  * 2022/05/11 09:11:22 +0000 * A060 * Unknown Reason
[05:06:57]  * 2022/05/11 09:13:18 +0000 * C102 * configd: find AP registered to cloud change mode
[05:06:57]  * 2022/05/11 09:16:54 +0000 * A010 * Power Off
[05:06:57]  * 2022/05/11 10:00:34 +0000 * C100 * configd: find cluster PVC local, change AP mode
[05:06:57]  * 2022/05/11 10:03:42 +0000 * C102 * configd: find AP registered to cloud change mode
[05:06:57]  * 2022/05/11 10:06:34 +0000 * A010 * Power Off
[05:06:57]  * 2022/05/11 10:09:27 +0000 * C100 * configd: find cluster PVC local, change AP mode
[05:06:57]  * 2022/05/11 10:11:57 +0000 * C102 * configd: find AP registered to cloud change mode
[05:06:57] show history reset reason completed
```

Figure 133: Show history reset reason command

6.7 Device connections record

This list contains the connection history of the device. The device generates a record when connected to the DAC. MQTT updates the disconnected time when disconnecting the device.

- **MAC:** MAC address of the device.
- **Name:** Name of the device.
- **MQTT Connected Time:** The last updated record at the connected time.
- **MQTT Disconnected Time:** MQTT disconnect time of the connection.
- **MQTT Connected Duration:** MQTT connect duration of the connection.

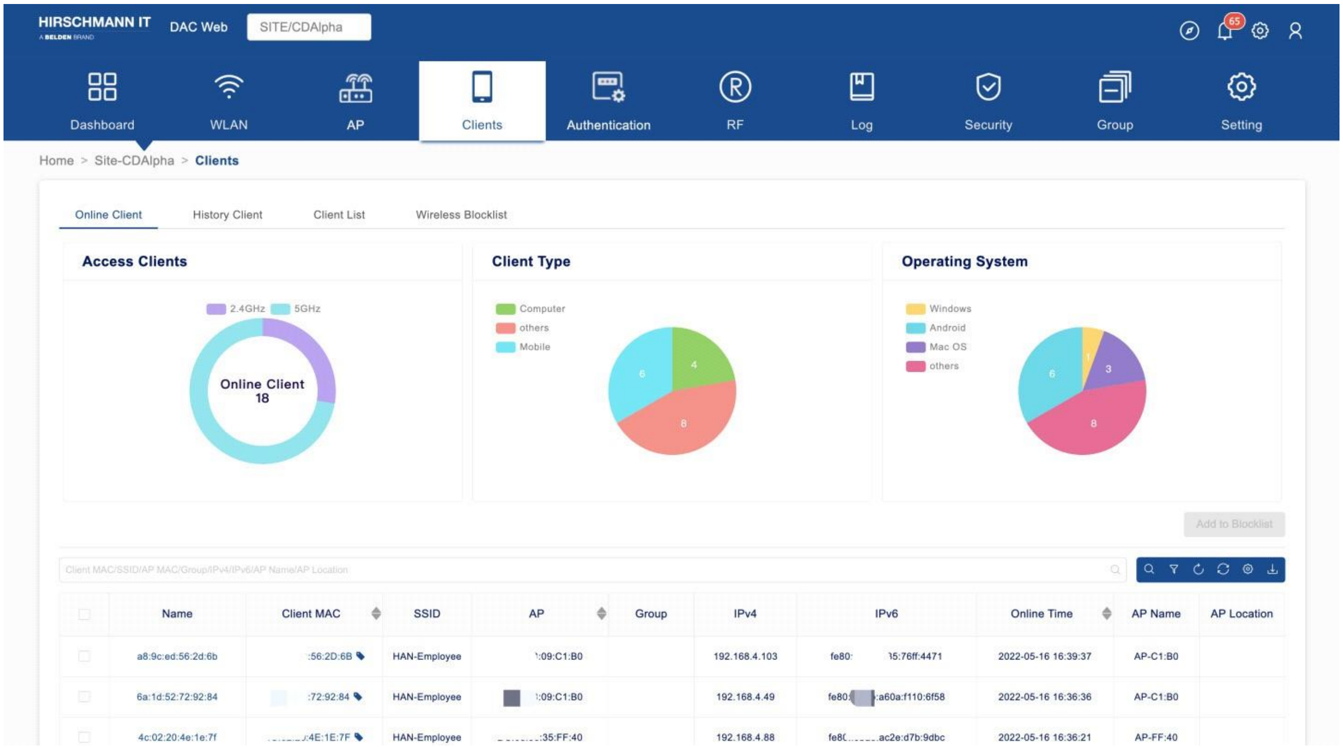


MAC	Name	MQTT Connected Time	MQTT Disconnected Time	MQTT Connected Duration
00:13:32:12:26:60	AP-26:60	2023-10-16 08:28:26		2h 33m 17s
00:13:32:12:26:60	AP-26:60	2023-10-16 03:30:16	2023-10-16 08:28:20	4h 58m 4s
00:13:32:12:26:60	AP-26:60	2023-10-16 02:54:53	2023-10-16 03:30:12	35m 19s
00:13:32:12:26:60	AP-26:60	2023-10-16 02:03:49	2023-10-16 02:54:48	50m 59s
00:13:32:12:26:60	AP-26:60	2023-10-16 01:23:16	2023-10-16 02:03:47	40m 31s
00:13:32:12:26:60	AP-26:60	2023-10-16 00:37:53	2023-10-16 01:23:12	45m 19s
00:13:32:12:26:60	AP-26:60	2023-10-15 20:14:19	2023-10-16 00:37:48	4h 23m 29s
00:13:32:12:26:60	AP-26:60	2023-10-15 10:50:51	2023-10-15 20:14:14	9h 23m 23s
00:13:32:12:26:60	AP-26:60	2023-10-15 07:01:54	2023-10-15 10:50:44	3h 48m 50s
00:13:32:12:26:60	AP-26:60	2023-10-15 06:35:59	2023-10-15 07:01:50	25m 51s
00:13:32:12:26:60	AP-26:60	2023-10-15 05:05:17	2023-10-15 06:35:54	1h 30m 37s
00:13:32:12:26:60	AP-26:60	2023-10-15 04:29:46	2023-10-15 05:05:13	35m 27s
00:13:32:12:26:60	AP-26:60	2023-10-14 18:56:26	2023-10-15 04:29:41	9h 33m 15s
00:13:32:12:26:60	AP-26:60	2023-10-14 12:46:09	2023-10-14 18:56:20	6h 10m 11s
00:13:32:12:26:60	AP-26:60	2023-10-14 12:20:59	2023-10-14 12:46:05	25m 6s
00:13:32:12:26:60	AP-26:60	2023-10-14 07:41:14	2023-10-14 12:20:54	4h 39m 40s
00:13:32:12:26:60	AP-26:60	2023-10-14 07:20:15	2023-10-14 07:41:09	20m 54s
00:13:32:12:26:60	AP-26:60	2023-10-14 03:37:52	2023-10-14 07:20:10	3h 42m 18s
00:13:32:12:26:60	AP-26:60	2023-10-14 02:47:29	2023-10-14 03:37:47	50m 18s
00:13:32:12:26:60	AP-26:60	2023-10-14 02:37:22	2023-10-14 02:47:25	10m 3s

Figure 134: Device Connection Record

7 Clients

The client page shows clients that connect to the current Site.



□	Name	Client MAC	SSID	AP	Group	IPv4	IPv6	Online Time	AP Name	AP Location
□	a8:9c:ed:56:2d:6b	:56:2D:6B	HAN-Employee	:09:C1:B0		192.168.4.103	fe80: 15:76ff:4471	2022-05-16 16:39:37	AP-C1:B0	
□	6a:1d:52:72:92:84	:72:92:84	HAN-Employee	[redacted] :09:C1:B0		192.168.4.49	fe80:[redacted]:a60a:f110:6f58	2022-05-16 16:36:36	AP-C1:B0	
□	4c:02:20:4e:1e:7f	:4E:1E:7F	HAN-Employee	:35:FF:40		192.168.4.88	fe80 ac2e:d7b:9dbc	2022-05-16 16:36:21	AP-FF:40	

Figure 135: Client page

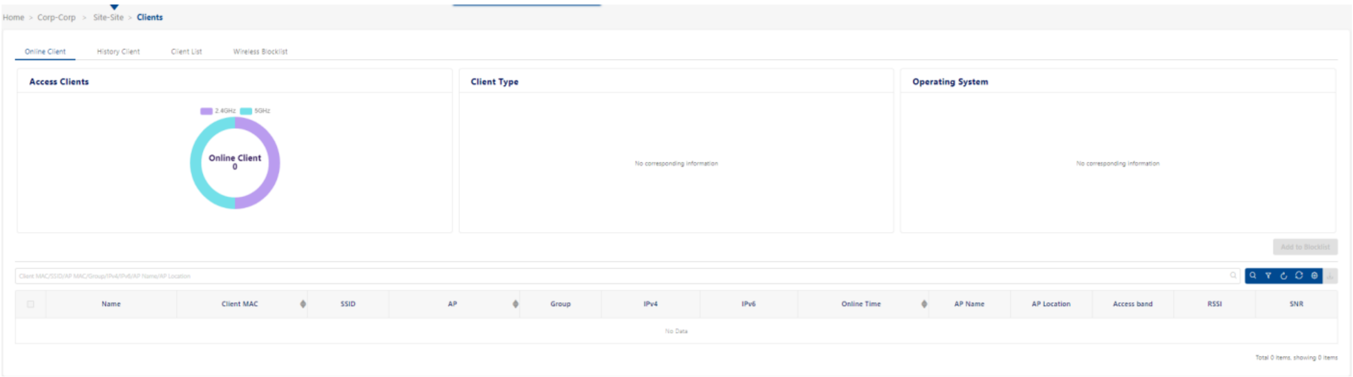
This chapter contains the following topics:

- Online clients
- History clients
- Client list
- Wireless blocklist

7.1 Online clients

This module shows the current list of online clients. There are three pie charts showing the distribution of clients in different dimensions.

- **Access Clients:** Pie chart of client band (2.4 G or 5 G).
- **Client Type:** Pie chart of client types, including Computer, Mobile, and others.
- **Operating System:** Pie chart of the client’s operating system.



Home > Corp-Corp > Site-Site > Clients

Online Client | History Client | Client List | Wireless Blocklist

Access Clients

Client Type

No corresponding information

Operating System

No corresponding information

Add to Blocklist

Client MAC/SSID/AP MAC/Group/IPv4/IPv6/AP Name/AP Location

□	Name	Client MAC	SSID	AP	Group	IPv4	IPv6	Online Time	AP Name	AP Location	Access band	RSSI	SNR
						No Data							

Total 0 items, showing 0 items

Figure 136: Online Client

■ List of clients

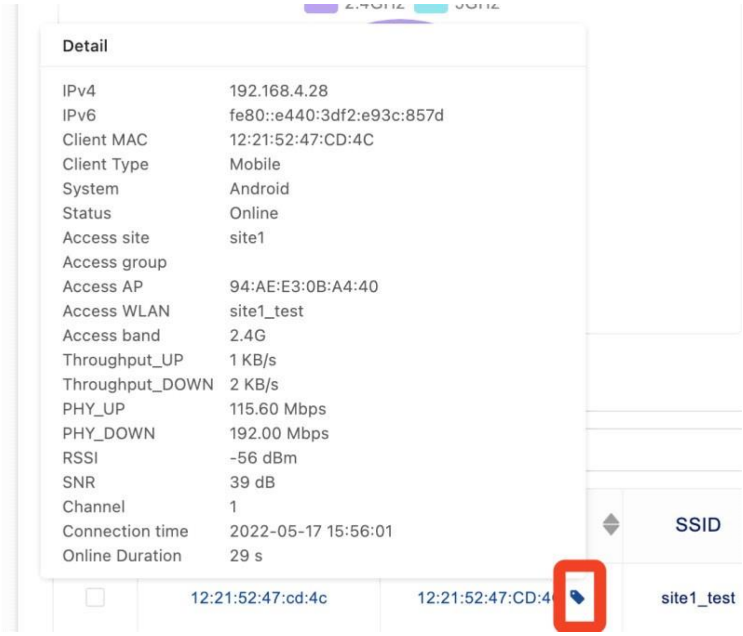
The list shows the clients currently connected to the AP at the Site. Because there is a certain interval for AP data reporting, there is a certain delay in the data update here.

- **Name:** Client name.
- **Client MAC:** MAC Address of the client.
- **SSID:** SSID to which the client is associated.
- **AP:** The MAC address of the AP to which the client is associated.
- **Group:** The Group of the AP to which the client is associated.
- **IPv4:** IPv4 address of the client.
- **IPv6:** IPv6 address of the client.
- **Online Time:** The time when the client is associated with the wireless network.
- **AP Location:** Location of the AP device.
- **Access Band:** The radio band through which the client is attached to

the AP (2.4 GHz or 5 GHz). The user needs to click the “⚙” button to manually add the data.

- **RSSI:** The Received Signal Strength Indicator of the client (Possible values: 0..99). The user needs to click the “⚙” button to manually add the data.
- **SNR:** Signal-to-noise ratio. The user needs to click the “⚙” button to manually add the data.

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



Detail

IPv4	192.168.4.28
IPv6	fe80::e440:3df2:e93c:857d
Client MAC	12:21:52:47:CD:4C
Client Type	Mobile
System	Android
Status	Online
Access site	site1
Access group	
Access AP	94:AE:E3:0B:A4:40
Access WLAN	site1_test
Access band	2.4G
Throughput_UP	1 KB/s
Throughput_DOWN	2 KB/s
PHY_UP	115.60 Mbps
PHY_DOWN	192.00 Mbps
RSSI	-56 dBm
SNR	39 dB
Channel	1
Connection time	2022-05-17 15:56:01
Online Duration	29 s

			SSID
□	12:21:52:47:cd:4c	12:21:52:47:CD:4	site1_test

Figure 137: Online client info

- **Client Type:** The client device type, including PC, Mobile, and others.
- **System:** The operating system of the client.
- **Throughput_UP:** The packet sending rate of the client. The traffic statistics are collected by the client that is the sender of the packet.
- **Throughput_DOWN:** The packet acceptance rate of the client. The traffic statistics are collected by the client that is the receiver of the packet.
- **PHY_UP:** The physical sending rate of the client. The traffic statistics are collected by the client that is the sender of the packet.
- **PHY_DOWN:** The physical acceptance rate of the client. The traffic statistics are collected by the client that is the receiver of the packet.

- ▶ **Channel:** The working channel of the client.

7.1.1 Add client to blocklist from online clients

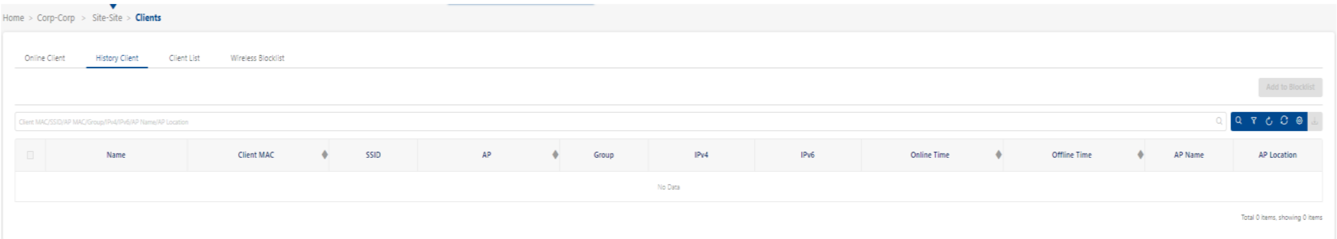
□ Select the client(s) in the List of Clients to block.
□ Click the **“Add to Blocklist”** button.
□ Set **“Expiry Time”** on the Confirmation Prompt.
□ Click **“Save”**.

The client will no longer be able to access the network. They will be displayed on the Wireless blocklist screen.

7.2 History clients

The History Clients table shows the connection records from the past.

- **Client MAC:** MAC Address of the client.
- **SSID:** SSID to which the client was associated.
- **AP:** The MAC address of the AP to which the client is associated.
- **Group:** The Group of the AP to which the client is associated.
- **IPv4:** IPv4 Address of the client.
- **IPv6:** IPv4 Address of the client.
- **Online Time:** The time when the client is associated with the wireless network.
- **Offline Time:** The time when the client disassociated from the wireless network.


Home > Corp-Corp > Site-Site > Clients
Online Client
History Client
Client List
Wireless Blocklist
Add to Blocklist
Client MAC/SSID/AP MAC/Group/IPv4/IPv6/AP Name/AP Location

□	Name	Client MAC	SSID	AP	Group	IPv4	IPv6	Online Time	Offline Time	AP Name	AP Location
No Data											

Total 0 items, showing 0 items

Figure 138: History Client

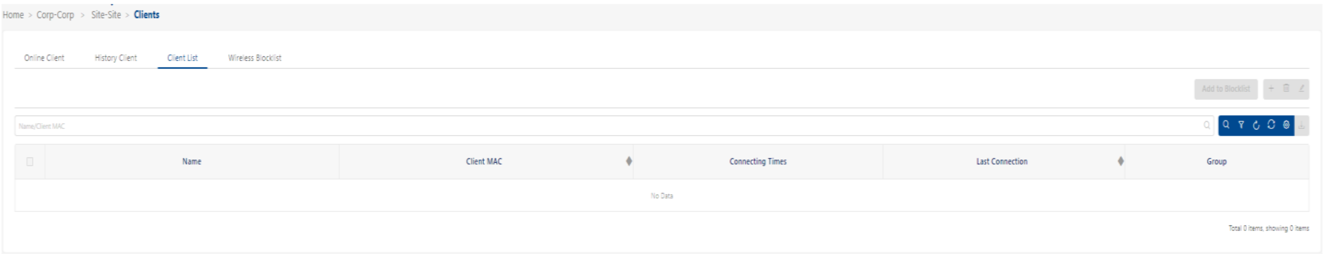
7.3 Client list

The total counts of connections for all clients connected to the Site and the last connection time are recorded.

- **Name:** Client Name. Default is MAC of client.

  To find the terminal conveniently, you can modify it.

  Select one client, click the **“Edit”** icon, enter the **“Name”** field, and click the **“Save”** button.
- **Client MAC:** MAC address of client.
- **Connecting Times:** Count of connections for the client.
- **Last Connection:** Time when the client last accessed the Site.
- **Group:** The Group from which the client last accessed the Site.



□	Name	Client MAC	Connecting Times	Last Connection	Group
No Data					

Total 0 items, showing 0 items

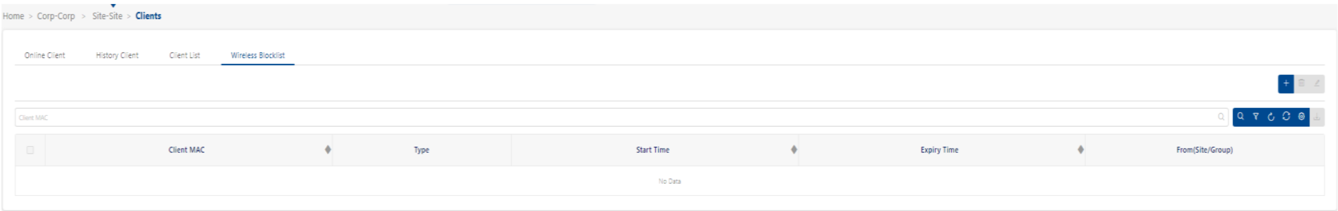
Figure 139: Client List

7.4 Wireless blocklist

Blocklist focuses on the basic access control mechanism for users connecting to SSID based on the client level. Those clients on the Blocklist are denied associating with the DAP. Once a client is on the Blocklist, it cannot connect to any WLAN of any security level (Enterprise, Personal, or Open). You can add or delete the Blocklist based on the client’s MAC address.

The **Wireless Blocklist** screen shows information about all clients that have been blocked on the Site. It is also used to manually add clients to the Blocklist.

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



□	Client MAC	Type	Start Time	Expiry Time	From(Site/Group)
			No Data		

Figure 140: Wireless Blocklist

7.4.1 Adding a client to the blocklist manually

- ☐ Click the “**+**” icon, and the **“Add to Blocklist”** window appears.
- ☐ Enter the client's MAC address.
- ☐ Click the **“Save”** button.

Repeat to add additional clients. You should set an Expire time for the client that means the client cannot connect to the SSID of the Site until the expiration time.

7.4.2 Deleting a client from the blocklist

- □ Select the client(s) from the blocklist.
- □ Click the **“Delete”** icon.
- □ Click **“Yes”** on the confirmation prompt.

8 Authentication

The DAC has a built-in AAA server. According to the WLAN configuration, the DAP sends an authentication request to the DAC, which may be 802.1x authentication, MAC authentication, or other authentication methods.

This chapter contains the following topics:

- Authentication concepts
- Network control
- Authentication
- Guess access
- Employee access
- Setting
- Default config and quick entrance
- Configuration instance for authentication

8.1 Authentication concepts

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 for 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 and are suitable for wireless networks include EAP Transport Layer Security (EAP-TLS), Protected EAP (PEAP), and EAP Tunneled 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 3 components:

- **Client**: The device attempting to gain access to the network.
- **Authenticator:** The gatekeeper to the network who permits or denies access to the clients. The wireless controller acts as the authenticator, relaying information between the authentication server and the client.

  Note: The EAP type must be consistent between the authentication server and the client and transparent to the controller.
- **Authentication Server:** Provides a database of information required for authentication and informs the Authenticator whether 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 user (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.

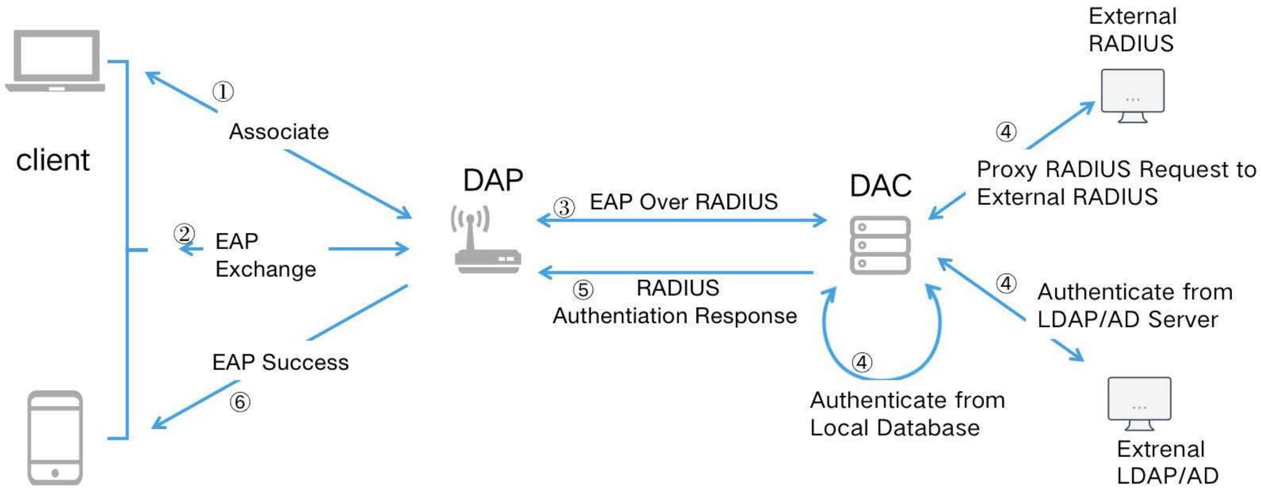


Figure 141: 802.1X Authentication process

Figure 141 shows the basic process of 802.1x authentication process in our system. For Step 4, DAC uses different Data Sources to verify the 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 the RADIUS protocol.

4 The DAC uses different Data Sources (based on different configurations) to verify the user.

5 The DAC returns the EAP authentication result to the DAP through the RADIUS protocol.

6 The DAP returns the EAP authentication result to the client.

■ MAC Authentication

MAC authentication authenticates devices based on their physical Media Access Control (MAC) address. The MAC of the devices will be used as Username 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 a **Guest / Employee Access Strategy**, the MAC has been authenticated by the portal before, 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, enter the **"User name"** and **"Password"** to complete the portal authentication process. If it is successful, the MAC authentication binding record will be saved according to the policy.

- **Web portal authentication**

Web Portal Authentication is a 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 the 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.

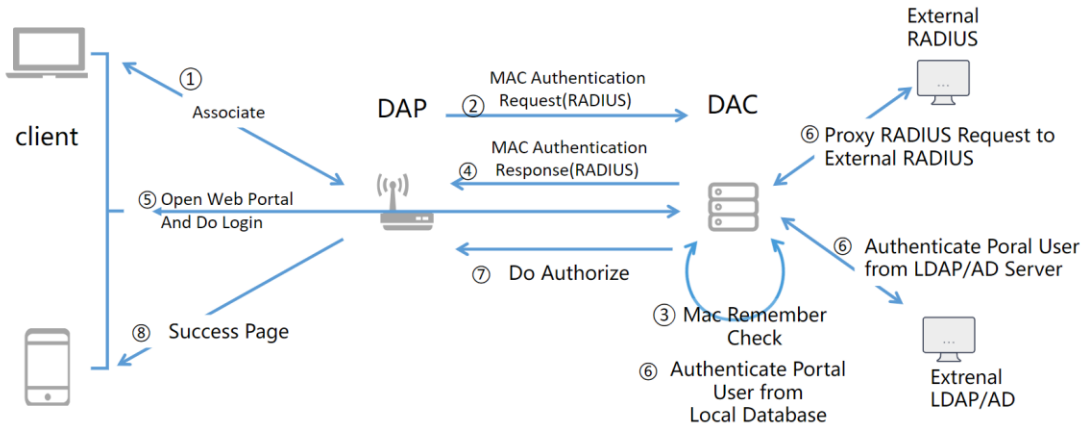

External RADIUS
client
① Associate
DAP
MAC Authentication ② Request(RADIUS)
DAC
⑥ Proxy RADIUS Request to External RADIUS
MAC Authentication ④ Response(RADIUS)
⑤ Open Web Portal And Do Login
⑥ Authenticate Poral User from LDAP/AD Server
⑦ Do Authorize
③ Mac Remember Check
⑧ Success Page
⑥ Authenticate Portal User from Local Database
Extrenal LDAP/AD

Figure 142: Web Portal Authentication process

Figure 142 shows the basic process of WEB Portal authentication in our system. For Step 6, DAC can use different Data Sources to verify the user.

1. The client initiates Wireless Association.
2. The DAP initiates MAC authentication through the RADIUS protocol.
3. The DAC performs a remember check (checks, if the MAC of the client bound to an account is valid).
4. The DAC replies to 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 be redirected 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 uses different Data Sources based on different configurations to verify users.
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 displays 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. See “Access role profile” on page 147 for details.

Access policy

RADIUS package carries several users or 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. See “Access policy” on page 127 for details.

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. See “Authentication strategy” on page 129.

Guest access strategy

Define the web Authentication Strategy for Guest. You can customize the web page by clicking the **“Edit Page”** button. See “Captive portal” on page 198 and “Guest access strategy” on page 136.

Employee access strategy

Define the web Authentication Strategy for Employee. See “Employee access strategy” on page 143.

Authentication source

The data source used in the 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 A**uthentication 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 the 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 the parameter setting in **Authentication** → **Setting** → **LDAP / AD Configuration**. See "LDAP/AD configuration" on page 150.
- **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**.

Remembered 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** is recorded. When the terminal accesses the wireless network again within the validity period, it does not need to do **Web Portal Authentication.**

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

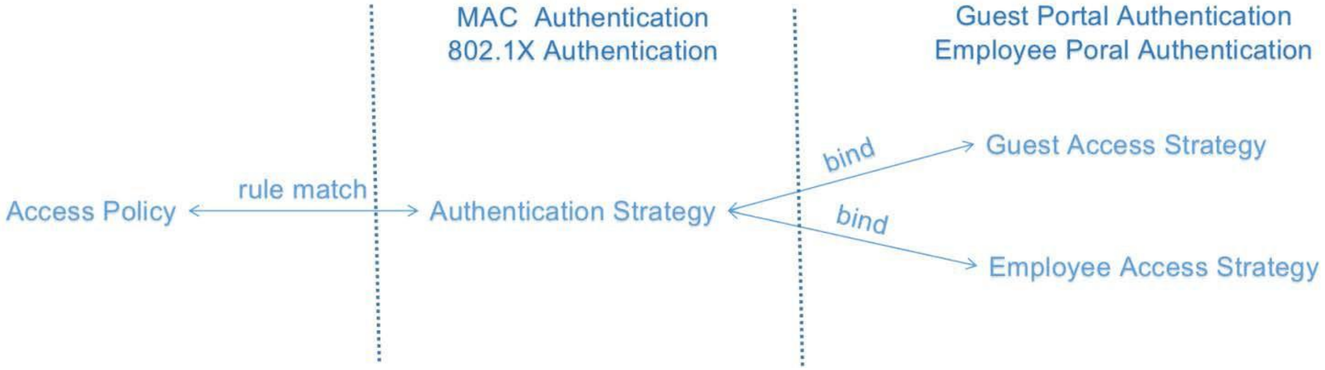


Figure 143: Relationship between access policy with strategies

In summary, terminal access may require 2 authentication steps, MAC Authentication or 802.1 X Authentication, and web authentication. **Authentication Strategy** is used to define MAC Authentication or 802.1 X Authentication. The authentication result determines whether subsequent web authentication is required. **Guest Access Strategy** or **Employee Access Strategy** is the configuration of web authentication.

8.2 Network control

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

8.2.1 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 a user role with which every client on the wireless network is associated.

■ **Creating an access role profile**

□ Click the **“+”** icon.
□ Specify the **“Profile Name”** and configure the profile as described below.
□ Click the **“Save”** button.

Policy and policy list

An Access Role Profile can be configured with an existing Policy List. The set of rules within the Policy List is 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 list.
□ Click the **“Add”** link to create a new policy list.

Location policy

□ Select a **“Location Access Policy”** from the drop-down list.

Period policy

□ Select a **“Period Policy”** from the drop-down list.

Bandwidth control settings

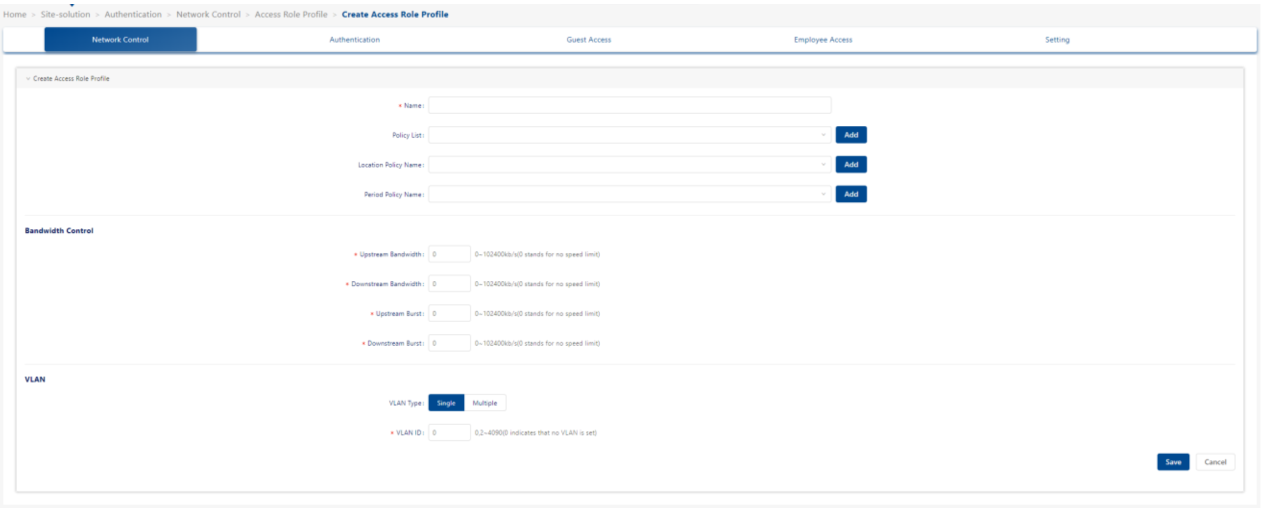
- **Upstream Bandwidth:** The maximum bandwidth limit allocated for ingress traffic on UNP (User Network Profile) ports assigned to the profile. If the maximum ingress bandwidth value is set to **“0”**, all ingress traffic is not limited.
- **Downstream Bandwidth:** The maximum bandwidth limit allocated for egress traffic on UNP ports assigned to the profile. If the maximum egress bandwidth value is set to **“0”**, 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 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 a profile. This value determines how much 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 single VLAN or multiple VLANs (as a VLAN pool) for an Access Role Profile. For a single VLAN type, you can set VLAN ID to **“0”**, which means mapping an Access Role Profile to untagged traffic.

Note: You can select a VLAN Pool, by entering multiple VLANs.

You can enter VLANs as a possible value (e.g., 10..20), as individual VLANs (21, 23, 25), or both (10..20, 21, 23, 25).


Home > Site-solution > Authentication > Network Control > Access Role Profile > Create Access Role Profile
Network Control
Authentication
Guest Access
Employee Access
Setting
Add
Add
Add
Save
Cancel

Create Access Role Profile

* Name:

Policy List:

Location Policy Name:

Period Policy Name:

Bandwidth Control

* Upstream Bandwidth: 0 0~102400kb/s(0 stands for no speed limit)

* Downstream Bandwidth: 0 0~102400kb/s(0 stands for no speed limit)

* Upstream Burst: 0 0~102400kb/s(0 stands for no speed limit)

* Downstream Burst: 0 0~102400kb/s(0 stands for no speed limit)

VLAN

VLAN Type: [✓ Single] Multiple

* VLAN ID: 0 0,2~4090(0 indicates that no VLAN is set)

Figure 144: Create Access Role Profile

- **Editing an access role profile**

□ Select the profile in the Access Role Profile List.
□ Click the **“Edit”** icon. Then the **“Edit Access Role Profile”** screen appears.
□ Edit the fields as described above.
□ Click the **“Save”** button to save the changes to the server.

Note: You cannot edit the Access Role Profile Name.

- **Deleting an access role profile**

□ Select the profile in the **“Access Role Profile”** screen.
□ Click the **“Delete”** icon.
□ Click **“Yes”** on the confirmation prompt. This removes the profile from the server.

8.2.2 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 the **“+”** icon. The wizard will then guide you through the following screens:

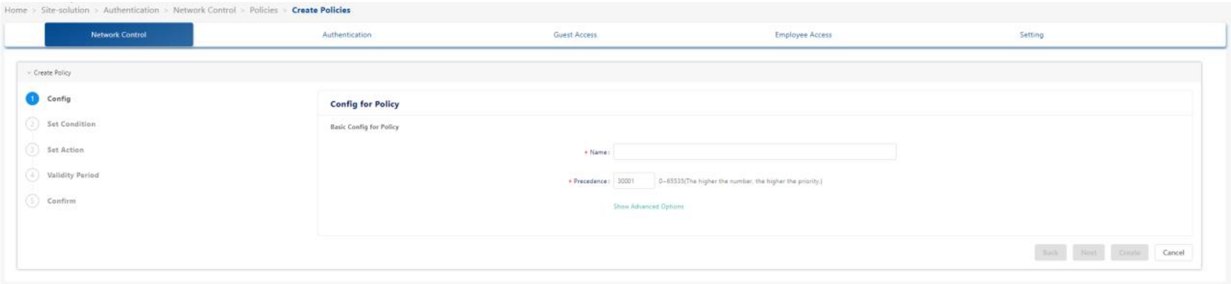
- **Config:** Basic policy configuration (e.g., Policy Name, Precedence).
- **Set Condition:** Specify the conditions that must be true before traffic will be allowed to flow.
- **Set Action:** Specify parameters for the traffic that will flow.
- **Validity Period:** Specify the time period for the policy 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 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. In the default setting, the precedence field is pre-filled with the lowest unused precedence value (Possible values: 0..65535).



* Name:

* Precedence: 30001 0~65535(The higher the number, the higher the priority.)

Figure 145: Basic Config for Policy

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 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 the parameters for the Condition(s), click the **"Next"** button at the bottom of the screen to move to the next step.
- ☐ 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 or 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 or network Group.

  Note: 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 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 2 TCP or UDP ports, 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 or service Group.

L2 MACs

A MAC Condition applies the Policy to traffic flowing from/to a MAC Address/Group.

Note: 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 1 router hop.

□ Select the parameter(s) you want to configure by selecting the applicable check bottom.

□ Click **Single** to configure a single MAC Address or **Group** to configure a MAC Group.

□ Enter a MAC address or select a MAC Group from the drop-down list. (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 this option is not selected, the traffic destined for the Source MAC Address/Group traffic is not going to be processed.

▶ **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 this option is not selected, the traffic destined for the Destination MAC Address/Group is not going to be processed.

L3 IPs

An IP Condition applies the Policy to traffic originating from, or flowing to, an IP Address/Group IP Address. 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 **“Single”** to configure a single IP Address, or click **“Group”** to configure a Group IP Address.

□ Enter an **“IP Address”** or select a Group IP Address from the drop-down list. (You can also click the **“+”** icon to go to the Groups application and create a new Group IP Address.)

▶ **Source IP Address/ Group IP Address:** Configuring a Source IP Address/ Group IP Address Condition restricts the policy to traffic that flows from this IP Address or Subnet Mask/Group IP Address only. If this option is not selected, the traffic destined for the Source IP Address or Subnet Mask/ Group IP Address traffic is not going to be processed.

- **Destination IP Address/ Group IP Address:** Configuring a Destination IP Address/Group IP Address Condition restricts the policy to traffic that flows to this IP Address/Group IP Address only. If this option is not selected, the traffic destined for the Destination IP Address or Subnet Mask/Group IP Address traffic is not going to be processed.

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 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 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.

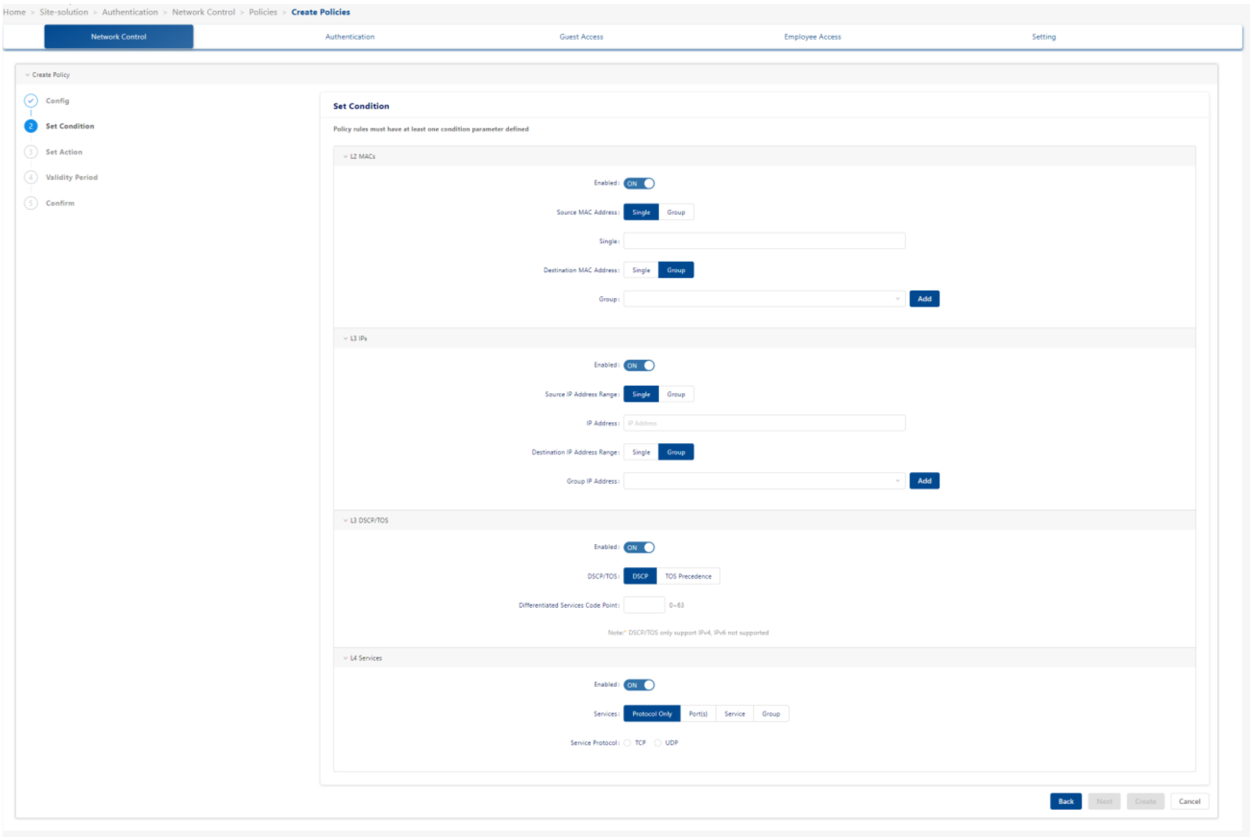
L4 Services

A Service Condition applies the policy to Service Protocol traffic (TCP or UDP) flowing from/to 2 TCP or UDP ports, or to traffic flowing from/to a TCP or UDP Service or Service Group. Select the 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 list to

specify a specific port for the service you selected. You can also click the **“Add”** icon to create new Service Ports.

- **Service:** Select a Service from the drop-down list. You can also click the **“Add”** icon to go to the Groups application and create a new Service.
- **Group:** Select a Service Group from the drop-down list. You can also click the **“Add”** icon to create a new Service Group.



Set Condition

Policy rules must have at least one condition parameter defined

L2 MACs

Enabled: ON

Source MAC Address: [✓ Single] Group

Single:

Destination MAC Address: Single [✓ Group]

Group: Add

L3 IPs

Enabled: ON

Source IP Address Range: [✓ Single] Group

IP Address: IP Address

Destination IP Address Range: Single [✓ Group]

Group IP Address: Add

L3 DSCP/TOS

Enabled: ON

DSCP/TOS: [✓ DSCP] TOS Precedence

Differentiated Services Code Point: 0~63

Note:* DSCP/TOS only support IPv4, IPv6 not supported

L4 Services

Enabled: ON

Services: [✓ Protocol Only] Port(s) Service Group

Service Protocol: ○ TCP ○ UDP

Figure 146: Set Condition

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 will 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.

- □ When you have completed all the parameters for the Action(s), click the **“Next”** button at the bottom of the screen or click **“Validity Period”** on the left side of the screen to move to the next step.
- □ 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, that is guaranteed to be transmitted from the port. 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: 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: 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 or disable DSCP/TOS Precedence. The TOS byte is defined in RFC 791. This byte contains 2 fields. The precedence field is the 3 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 of 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.

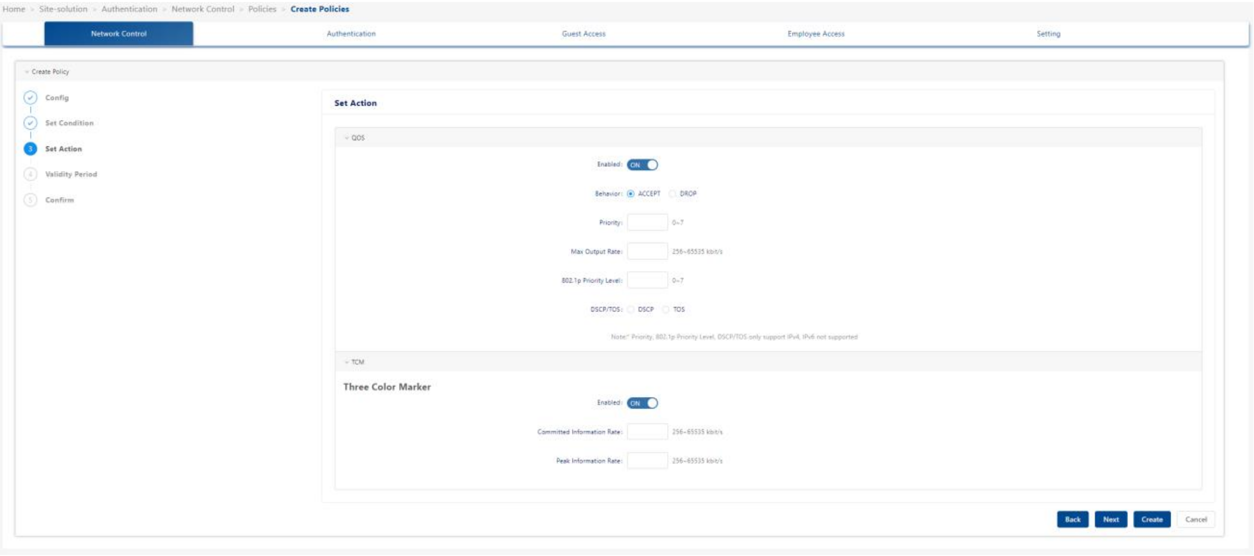
  Note: You can enable either the DSCP or the TOS Precedence radio to specify the mechanism you want to use (if any) to convey QoS information in the IP header of frames. DSCP and TOS are mutually exclusive. You can use either DSCP or TOS, but not both. This parameter is not supported on AOS Wireless Devices and is ignored when applied to those devices.

TCM

The TCM Policy Action option enables you to specify Three-Color Marking (TCM) actions 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)



Set Action

QOS

Enabled: ON

Behavior: ● ACCEPT ○ DROP

Priority: 0~7

Max Output Rate: 256~65535 kbit/s

802.1p Priority Level: 0~7

DSCP/TOS: ○ DSCP ○ TOS

Note:* Priority, 802.1p Priority Level, DSCP/TOS only support IPv4, IPv6 not supported

TCM

Three Color Marker

Enabled: ON

Committed Information Rate: 256~65535 kbit/s

Peak Information Rate: 256~65535 kbit/s

Figure 147: Set Action

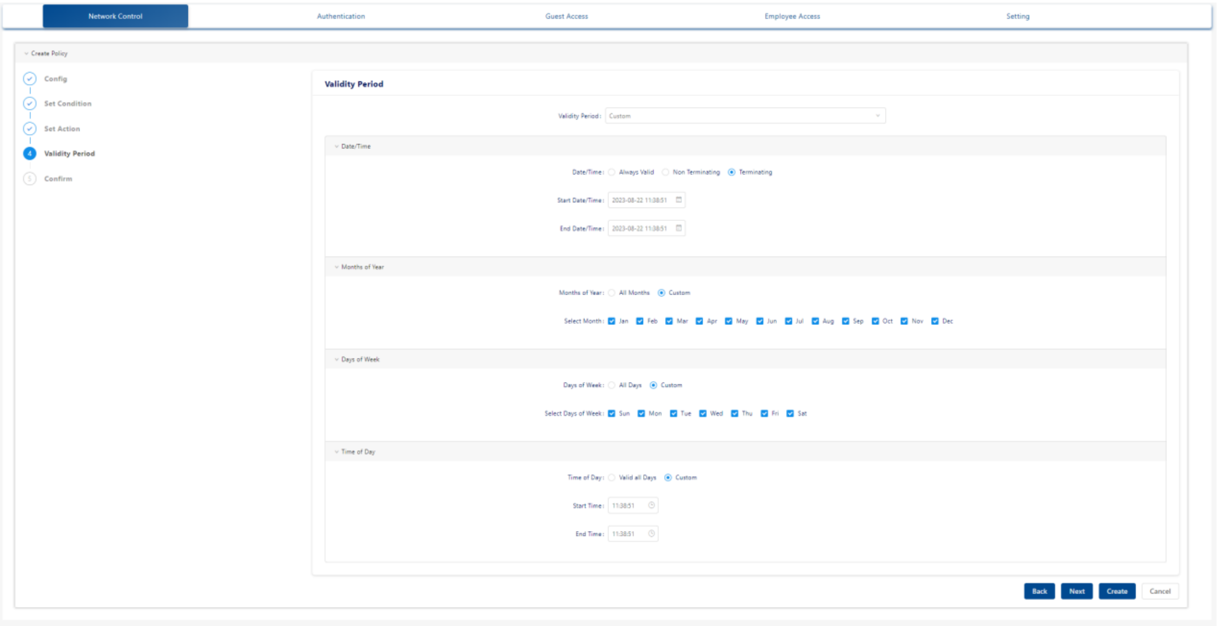
Validity period

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) in all months of the year. Each weekday are 24 hours (midnight to midnight).

- ▶ **Weekends:** The policy will be enforced on Saturday and Sunday in all months of the year. Each Saturday and Sunday are 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.



Validity Period

Validity Period : Custom

Date/Time

Date/Time : ○ Always Valid ○ Non Terminating ● Terminating

Start Date/Time : 2023-08-22 11:38:51

End Date/Time : 2023-08-22 11:38:51

Months of Year

Months of Year : ○ All Months ● Custom

Select Month : ☑ Jan ☑ Feb ☑ Mar ☑ Apr ☑ May ☑ Jun ☑ Jul ☑ Aug ☑ Sep ☑ Oct ☑ Nov ☑ Dec

Days of Week

Days of Week : ○ All Days ● Custom

Select Days of Week : ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time of Day

Time of Day : ○ Valid all Days ● Custom

Start Time : 11:38:51

End Time : 11:38:51

Figure 148: Validity Period for Policy

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

Note: The pre-configured validity period **AllTheTime** is the default. 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.

□ Click the **“Edit”** icon. Use the wizard to make any edits.

■ **Deleting policy**

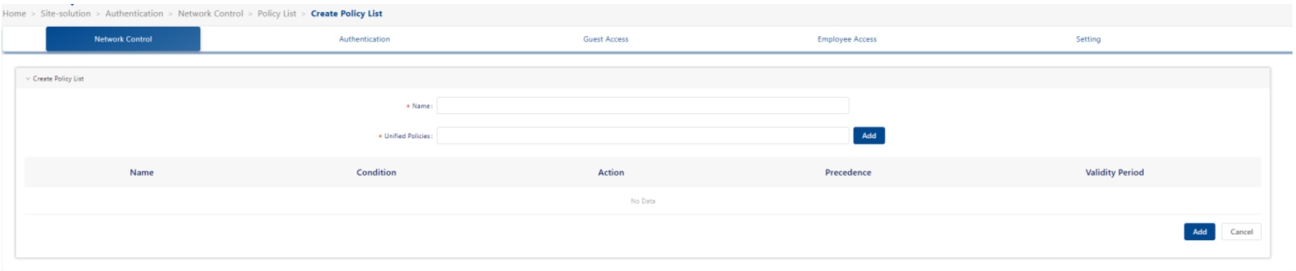
□ To delete a policy(ies), select the policy(ies) in the Existing Unified Policies Table.
□ Click the **“Delete”** icon.
□ Click **“Yes”** on the confirmation prompt.

8.2.3 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 the **“+”** icon. The Create Policy List Wizard appears.
□ Complete the screens as described below.
□ Click the **“Add”** button.


Home > Site-solution > Authentication > Network Control > Policy List > Create Policy List
Network Control
Authentication
Guest Access
Employee Access
Setting
Add
Add
Cancel

Create Policy List

* Name:

* Unified Policies:

Name	Condition	Action	Precedence	Validity Period
No Data				

Figure 149: Policy List

Config for policy list

□ Enter a Name for the Policy List.
□ Select the Policies you want to include in the list from the **Unified Policies** drop-down list. All the currently configured Unified Policies appear in the list.
□ Click the **“Add”** button, and the “**Create policy**” panel appears.
□ Create a new Policy to add to the list.
□ When you select a Policy from the drop-down list, the Policy will

appear in the table below. Review the Policy List configuration(s) in the table.

□ Click the **“Add”** button. The new Policy List appears 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.
□ Click the **Edit** icon. Then the **“Edit Policy List”** screen appears.
□ Click the **“Add Unified Policies”** drop-down list. All the currently configured Unified Policies appear in the list.
□ Click the **“Add”** icon, and the “**Create Policy**” screen appears. Create a new policy to add to the list.
□ Click the **“Edit”** button to edit the Unified policy. The updated Policy List appears on the Policy Lists screen.

■ Deleting a policy list

□ To delete a Policy List(s), select the list(s).
□ Click the **“Delete”** icon.
□ Click **“Yes”** on the confirmation prompt.

Note: You cannot delete a Policy List that is associated with an Access Role Profile. To delete the list, you must first remove it from the associated Access Role Profile.

8.2.4 Location policy

The Location Policy screen displays all configured Location Policies and 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 applies to devices classified in the Access Role Profile.

■ Creating a location policy

□ Click the **“+”** icon.
□ Complete the fields as described below.

- ☐ Click 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.

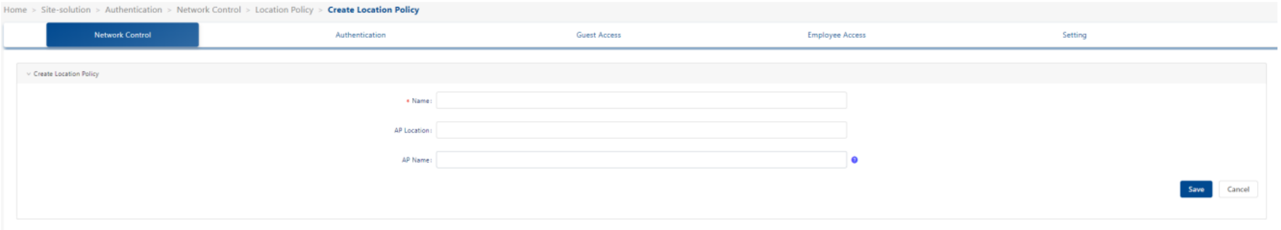


Figure 150: Location Policy

■ Editing a location policy

- ☐ Select the policy in the Location Policy List.
- ☐ Click the **“Edit”** icon, and the **“Edit Location Policy”** screen appears.
- ☐ Edit the fields as described above.
- ☐ Click the **“Save”** button to save the changes.

Note: You cannot edit the profile name.

■ Deleting a location policy

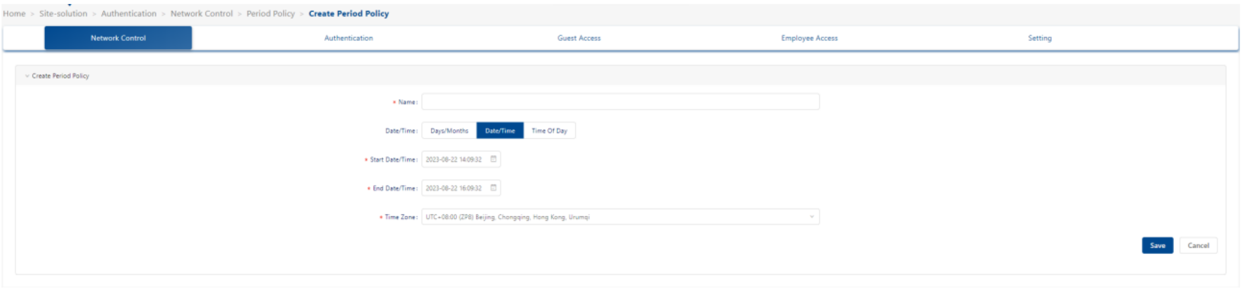
- ☐ Select the policy in the Location Policy List.
- ☐ Click the **“Delete”** icon.
- ☐ Click **“Yes”** on the confirmation prompt.

8.2.5 Period policy

The Period Policy screen displays all configured Period Policies 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 applies to devices classified in the Access Role Profile.

■ Creating a period policy

- □ Click the **“+”** icon.
- □ Complete the fields as described below.
- □ Click the **“Save”** button.
  - ▶ **Name:** User-configured Period Policy Name.
  - ▶ **Date/Time:** Click the Days/Months, Date/Time, and Time of Day sliders to configure the time when the devices can access the network.
  - ▶ **Start Time:** The time when the **Period Policy** of the **Access Role Profile** takes effect.
  - ▶ **End Time:** The time when the **Period Policy** of the **Access Role Profile** stops taking effect.
  - ▶ **Timezone:** Select the time zone in which the Period Policy is active.



* Name:
Date/Time: Date/Time
* Start Date/Time: 2023-08-22 14:09:32
* End Date/Time: 2023-08-22 16:09:32
* Time Zone: UTC+08:00 (ZP8) Beijing, Chongqing, Hong Kong, Urumqi

Figure 151: Period Policy

■ Editing a period policy

- □ Select the policy in the Period Policy List.
- □ Click the **“Edit”** icon, and the **“Edit Period Policy”** screen appears.
- □ Edit the fields as described above.
- □ Click the **“Save”** button to save the changes.

Note: You cannot edit the profile name.

■ Deleting a period policy

- □ Select the policy in the Period Policy List.
- □ Click the **“Delete”** icon.
- □ Click **“Yes”** on the confirmation prompt.

8.3 Authentication

The Authentication module is used for configuration of the user Access Strategy.

8.3.1 Dashboard

Dashboard consists of 4 diagrams.

Authentication Result Statistic: Figure 152 demonstrates the result of authentication (Success/Failure). Dimension of authentication method consists of MAC,802.1x, Captive Portal. Dimension of client type consists of Employee, Company Device, Unknown, and Guest. Dimension of a time zone consists of several time zone.

The remaining three diagrams show the contents described in the label. They are “Top 10 AP with Authentication Request”, “Top 10 AP with Authentication Failure”, and “Top 10 Reason of Authentication Failure”.

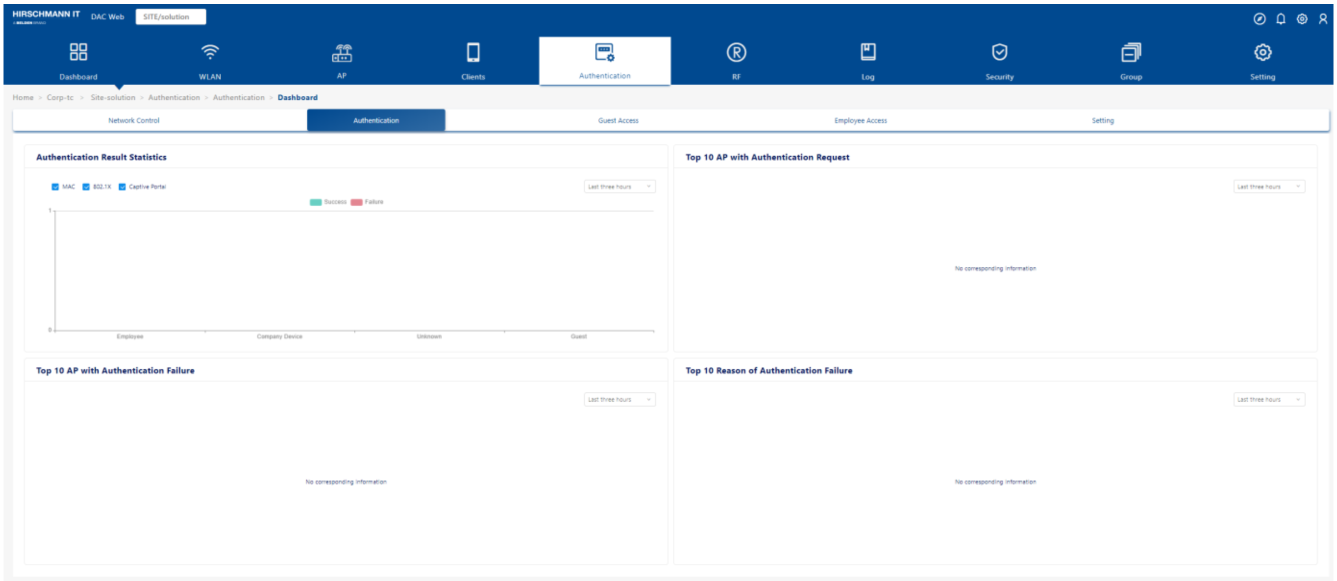

HIRSCHMANN IT
DAC Web
SITE/solution
Dashboard
WLAN
AP
Clients
Authentication
RF
Log
Security
Group
Setting
Home > Corp-tc > Site-solution > Authentication > Authentication > Dashboard
Network Control
Authentication
Guest Access
Employee Access
Setting
Authentication Result Statistics
☑ MAC ☑ 802.1X ☑ Captive Portal
Last three hours
🟩 Success 🟥 Failure
1
0
Employee
Company Device
Unknown
Guest
Top 10 AP with Authentication Request
Last three hours
No corresponding information
Top 10 AP with Authentication Failure
Last three hours
No corresponding information
Top 10 Reason of Authentication Failure
Last three hours
No corresponding information

Figure 152: Authentication Dashboard

8.3.2 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.
- ▶ **Priority:** Access Policy Priority.

  A user requesting authentication may match several access policies and the 1 with the highest priority will take effect after the authentication. (Possible values: 1..99, 1 is the highest priority and 99 is the lowest)
- ▶ **Mapping Condition:** Descriptions of conditions that you add to the policy.
- ▶ **Authentication Strategy:** Authentication strategy that will be utilized when the Access Policy is matched.

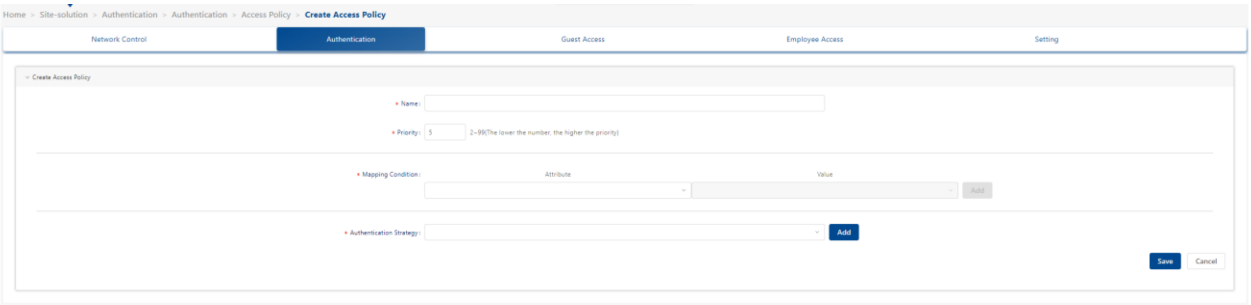
■ Creating an access policy

□ Click the **"+"** icon. Then the **"Create Access Policy"** screen appears.
□ Enter the fields as described.
□ Click the **"Save"** button.

- ▶ **Name:** User-configured policy name.
- ▶ **Priority:** Access Policy Priority.

  A user requesting authentication may match several access policies and the one with the highest priority will take effect after the authentication. (Possible values: 1..99, 1 is the highest priority and 99 is the lowest)
- ▶ **Mapping Condition:** Select an attribute and 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 for the Site.
  - ▶ **AP IP:** Enter the AP IP address or select AP IP from the drop-down list.
  - ▶ **AP Name:** Enter the AP Name or select the AP Name from the drop- down list.
  - ▶ **User MAC:** Enter the User MAC address.
- ▶ **Authentication Strategy:** Authentication strategy that will be utilized

when the Access Policy is matched.



* Name:

* Priority: 5 2~99(The lower the number, the higher the priority)

* Mapping Condition: Attribute Value

* Authentication Strategy:

Figure 153: Access Policy

- ■ **Editing an access policy**

☐ Select a policy from the Access Policy List.
☐ Click the **"Edit"** icon.
☐ Edit the field(s) as described above.
☐ Click the **"Save"** button.
Note: You cannot edit a policy name.

- ■ **Deleting an access policy**

☐ Select a policy from the Access Policy List.
☐ Click the **"Delete"** icon.
☐ Click **"Yes"** on the Confirmation Prompt.

8.3.3 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, and the **"Create Authentication Strategy"** screen appears.
☐ Enter the fields as described below.
☐ Click the **"Save"** button.

General

▶ **Strategy Name:** Authentication strategy name.

- ▶ **Authentication Source:** Specify the source of the user profile (Account or Password). The user profile can reside on different servers and is required to be 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 Account + Password or Access Code), the MAC address of the user will be stored, and the user will complete the MAC authentication. For a Guest, the devices will be displayed in **Authentication - Guest Access ➝ Guest Device ➝ Remembered Device**. For an Employee, the devices will be displayed in **Authentication - Employee Access** → **Employee Device** → **Remembered Device**.
  - **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

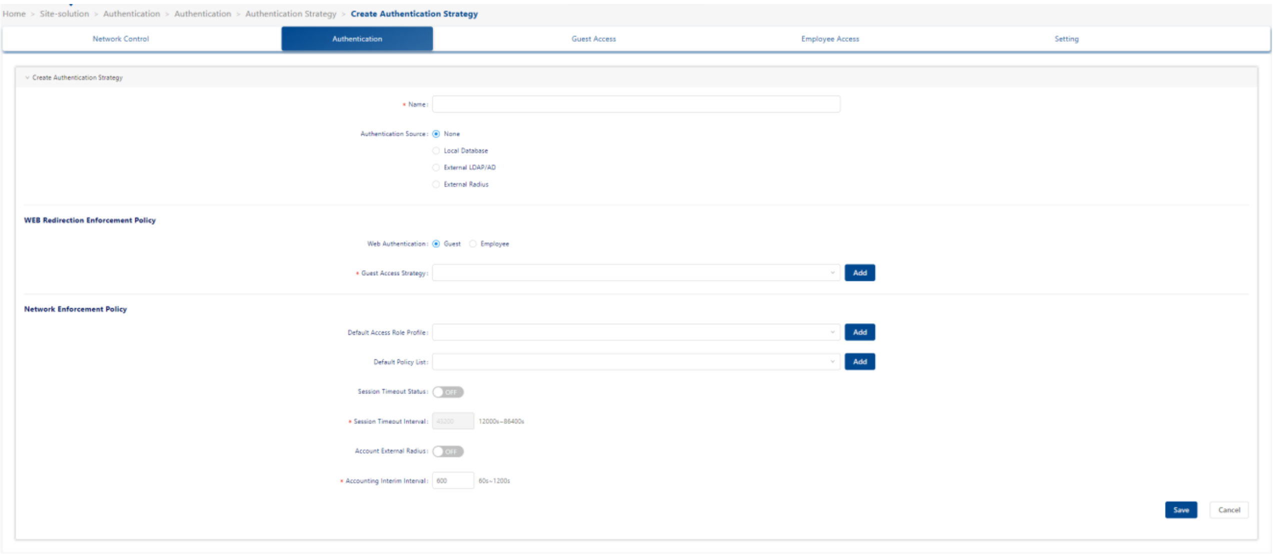
- ▶ **Web Authentication:** Specify whether or not web redirection is required and which web login page is going to be used during the authentication.
  - **Guest:** Redirect to the guest login page during authentication.
  - **Employee:** Redirect to the employee login page during the authentication.
- ▶ **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 times out.
- **Session Timeout Interval:** The Session Timeout Interval is the maximum number of consecutive seconds of connection allowed to the user before the termination of the session or prompt. If not configured, the device’s default session timeout policy will take effect. (Possible values: 2000..86400, Default Setting: 43200)
- **Account External Radius:** Whether to forward accounting messages to the external radius.
- **Accounting Interim Interval:** Interval for RADIUS accounting, in seconds. If not configured, the device’s default accounting policy will take effect. (Possible values: 60..1200, Default Setting: 600)



Home > Site-solution > Authentication > Authentication > Authentication Strategy > Create Authentication Strategy
Network Control
Authentication
Guest Access
Employee Access
Setting
Create Authentication Strategy
Add
Add
Add
Save
Cancel

* Name:

Authentication Source: ● None ○ Local Database ○ External LDAP/AD ○ External Radius

WEB Redirection Enforcement Policy

Web Authentication: ● Guest ○ Employee

* Guest Access Strategy:

Network Enforcement Policy

Default Access Role Profile:

Default Policy List:

Session Timeout Status: OFF

* Session Timeout Interval: 43200 12000s~86400s

Account External Radius: OFF

* Accounting Interim Interval: 600 60s~1200s

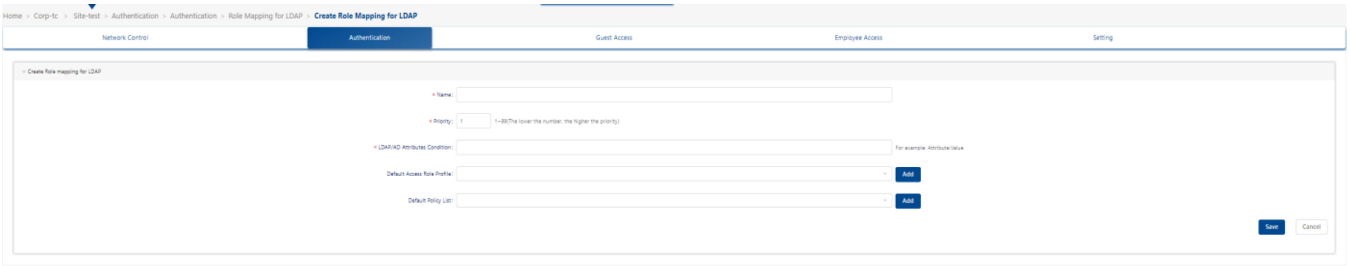
Figure 154: Authentication Strategy

8.3.4 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.

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


Home > Corp-tc > Site-test > Authentication > Authentication > Role Mapping for LDAP > Create Role Mapping for LDAP
Network Control
Authentication
Guest Access
Employee Access
Setting
Create Role mapping for LDAP
Add
Add
Save
Cancel

* Name:

* Priority: 1 1~99(The lower the number, the higher the priority)

* LDAP/AD Attributes Condition: For example: Attribute:Value

Default Access Role Profile:

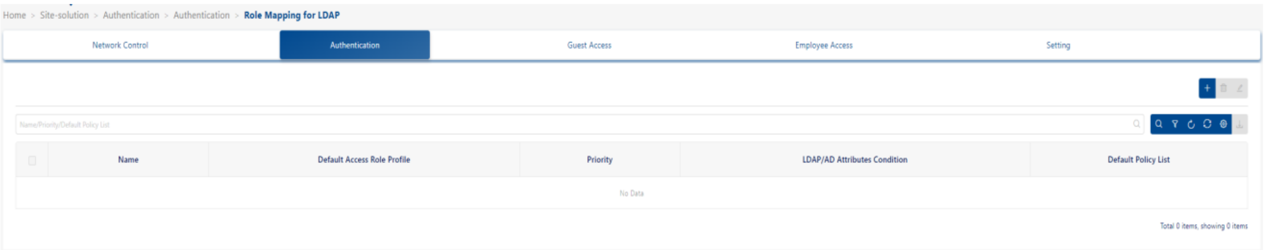
Default Policy List:

Figure 155: Role mapping for LDAP

A user requesting LDAP/AD authentication may match several role mapping rules. The 1 with the highest priority will take effect after authentication. (Possible values: 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.
  - **Default Access Role Profile:** Access Role Profile applied to the user after matching the role mapping rule.

- **Priority:** Priority of the role mapping rule. A user requesting LDAP/AD authentication may match several role mapping rules. The one with the highest priority will take effect after authentication. (Possible values: 1..99, 1 is the highest priority and 99 is the lowest).
- **LDAP/AD Attribute Condition:** Pairs of Attribute and Value for referring to an LDAP/AD account.
  - **Attribute:** LDAP/AD attributes used as role mapping rule keys.
  - **Value:** Role mapping rule value.
- **Default Policy List:** Policy List applied to the user after matching the role mapping rule.


Home > Site-solution > Authentication > Authentication > Role Mapping for LDAP
Network Control
Authentication
Guest Access
Employee Access
Setting
+

Name/Priority/Default Policy List

□	Name	Default Access Role Profile	Priority	LDAP/AD Attributes Condition	Default Policy List
No Data					

Total 0 items, showing 0 items

Figure 156: Role Mapping for LDAP

■ Editing a mapping

☐ Select a mapping in the Role Mapping List.
☐ Click the **"Edit"** icon.
☐ Edit the field(s) as described above.
☐ Click the **"Save"** button.

Note: You cannot edit a mapping name.

■ Deleting a mapping

☐ Select a mapping in the Role Mapping List.
☐ Click the **"Delete"** icon.
☐ Click **"Yes"** on the Confirmation Prompt.

8.3.5 Authentication record

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

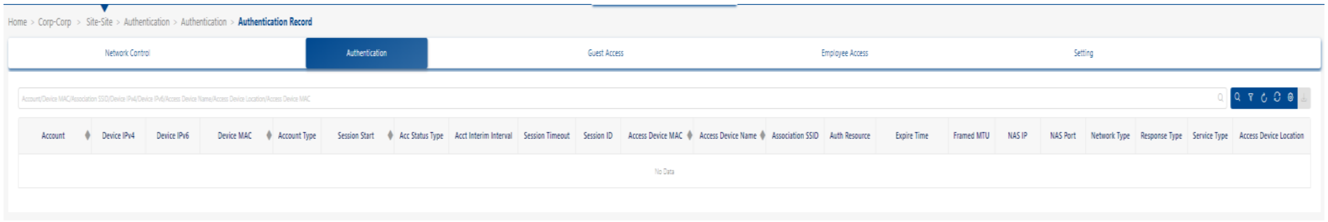
- **Account:** Indicates the user name of the user to be authenticated.

  - **MAC Authentication:** The account name is the MAC address of the user’s device.
  - **802.1X Authentication:** The account name is the user name of the employee user.
  - **Captive Portal Authentication:** The account name is the user name of the guest user or employee user.
- **Device IPv4:** The IPv4 address of the client device of the user requesting authentication.

  Note: IP addresses are displayed only if they are known at the time the RADIUS Accounting packets are sent or 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: IP addresses are displayed only if they are known at the time the RADIUS Accounting packets are sent or 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 passes authentication and a connection session is 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 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:** The system name of the NAS to which the user device is attached.
- **Association SSID:** Wireless service is broadcast by the DAP. It is connected by the user device (only valid for wireless access).
- **Auth Resource:** A user profile database used in authentication, including None, Local Database, LDAP/AD, and an external RADIUS server. Refer to the authentication strategy definition.
- **Expire Time:** The time when the account is going to expire.
- **Framed MTU:** The Maximum Transmission Unit to be configured for the user. It is a fixed value = 1400.
- **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 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 these service types and must treat unknown or unsupported Service-Types as though an Access-Reject had been received instead.
- **Access Device Location:** Location of the DAP to which the user device is attached.


Home > Corp-Corp > Site-Site > Authentication > Authentication > Authentication Record
Network Control
Authentication
Guest Access
Employee Access
Setting
Account/Device MAC/Association SSID/Device IPv4/Device IPv6/Access Device Name/Access Device Location/Access Device MAC

Account	Device IPv4	Device IPv6	Device MAC	Account Type	Session Start	Acc Status Type	Acct Interim Interval	Session Timeout	Session ID	Access Device MAC	Access Device Name	Association SSID	Auth Resource	Expire Time	Framed MTU	NAS IP	NAS Port	Network Type	Response Type	Service Type	Access Device Location
No Data																					

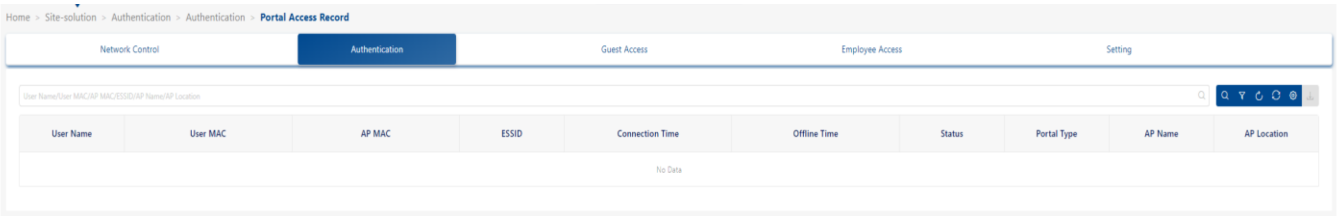
Figure 157: Authentication record

8.3.6 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 is associated.
- **Connections Time:** The portal user logs in time.
- **Offline Time:** The portal user logoff or time out time.
- **Status:** Result for the user authentication request.
    - **Online:** This Captive portal authentication is accepted.
    - **Reject:** This Captive portal authentication is rejected.
    - **Empty Value:** Captive portal authentication is not activated.
- **Portal Type:** The Captive Portal usage (Employee or Guest).
- **AP Name:** The name of the AP that the user attached.
- **AP Location:** The location of the AP that the user attached.


Home > Site-solution > Authentication > Authentication > Portal Access Record
Network Control
Authentication
Guest Access
Employee Access
Setting
User Name/User MAC/AP MAC/ESSID/AP Name/AP Location

User Name	User MAC	AP MAC	ESSID	Connection Time	Offline Time	Status	Portal Type	AP Name	AP Location
No Data									

Figure 158: Portal Access Record

8.4 Guess access

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

8.4.1 Dashboard

Dashboard consists of the following 4 sections:

- **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, mobile and so on).
- **Guest Account Creation Mode:** Pie chart of Account Creation Mode.

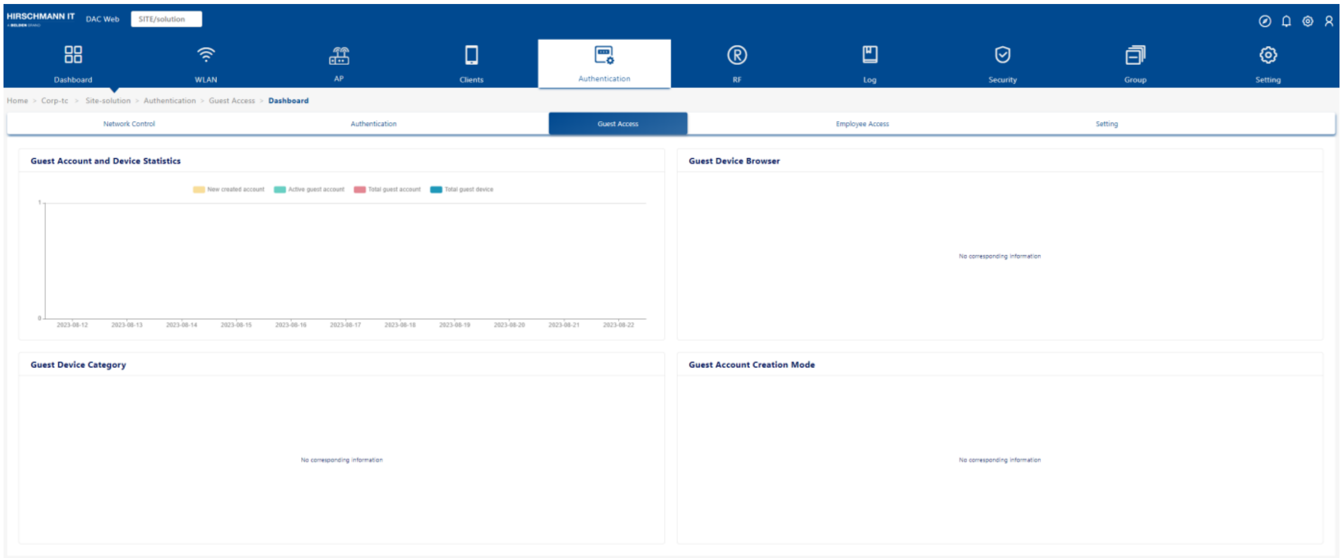


Figure 159: Guess Access Dashboard

8.4.2 Guest access strategy

The Guest Access Strategy screen is used to configure access attributes for guest users. The screen is 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 name of Guest Access Strategy.
- ▶ **Account Validity Period:** Account validity period.
- ▶ **Device Validity Period:** Device MAC authentication validity period.
- ▶ **Max Device per Account:** Limits on devices that use this guest account at the same time.
- ▶ **Fixed Access Role Profile:** The Access Role Profile is assigned to the guest user after passing authentication.
- ▶ **Fixed Policy List:** The Policy List is assigned to the guest user after passing authentication.
- ▶ **Authentication Resource:** Local Database.

■ Creating a Guest access strategy

□ Click the **“+”** icon and complete the fields as described below.
□ Click 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. (Possible values: 1..180 Days, Default Setting: 90 Days).
- ▶ **Device Validity Unit:** The classifier of Device Validity Period. It can be selected as a day or minute.
- ▶ **Device Validity Period:** The length of time that the user device is valid. (Possible values: 1..365 Days, Default Setting: 1 Day). After authentication success, it remembers the device MAC address. The MAC address check will be performed first, and the device will allow access without re-authentication.

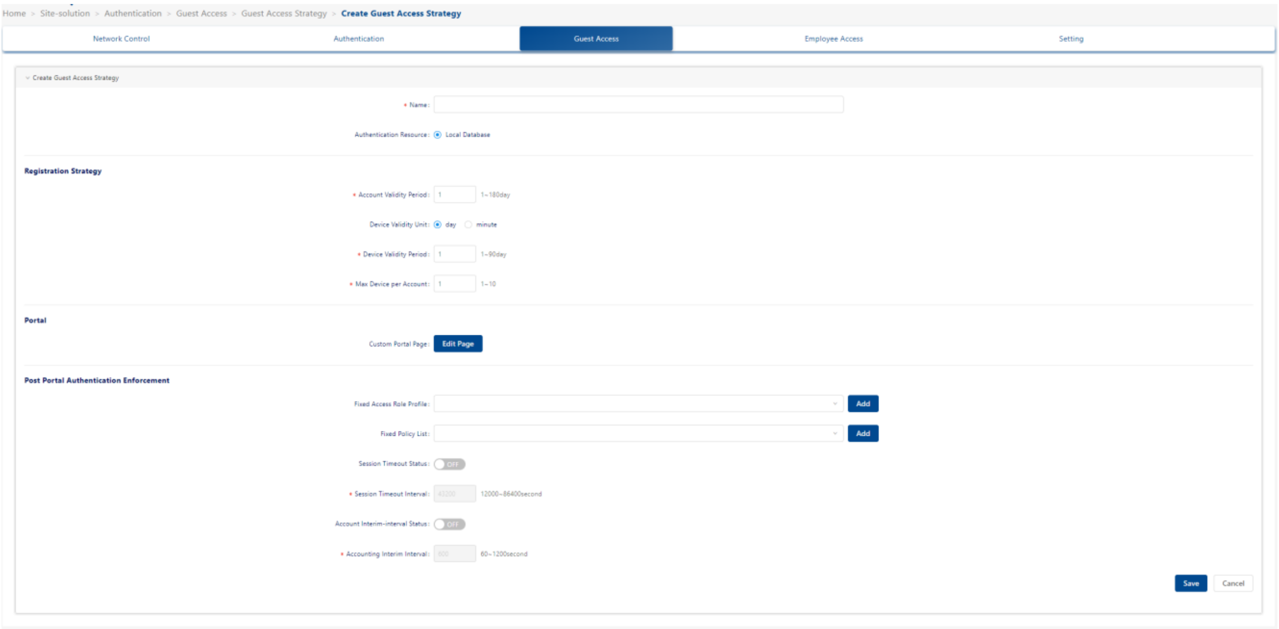
- **Max Device per Account:** The maximum number of devices that can access the network with one single account. (Possible values: 1..10, Default Setting: 1).

Portal

- **Custom Portal Page:** You can edit the page type and page style at the time of portal authentication. See “Captive portal” on page 253.

Post Portal Authentication Enforcement

- **Fixed Access Role Profile:** The Access Role Profile is 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 or 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. (Possible values: 12000..86400, Default Setting: 43200)
- **Accounting Interim Status:** Enable or disable the Accounting Interim.
- **Accounting Interim Interval:** Interval for RADIUS accounting, in seconds. (Possible values: 60..1200, Default Setting: 600)


Home > Site-solution > Authentication > Guest Access > Guest Access Strategy > Create Guest Access Strategy
Network Control
Authentication
Guest Access
Employee Access
Setting
Create Guest Access Strategy
Edit Page
Add
Add
Save
Cancel

* Name:

Authentication Resource: ● Local Database

Registration Strategy

* Account Validity Period: 1 1~180day

Device Validity Unit: ● day ○ minute

* Device Validity Period: 1 1~90day

* Max Device per Account: 1 1~10

Portal

Custom Portal Page:

Post Portal Authentication Enforcement

Fixed Access Role Profile:

Fixed Policy List:

Session Timeout Status: OFF

* Session Timeout Interval: 43200 12000~86400second

Account Interim-interval Status: OFF

* Accounting Interim Interval: 600 60~1200second

Figure 160: Guest Access Strategy

- ■ **Editing a Guest access strategy**

□ Select a strategy in the Guest Access Strategy List.
□ Click the **“Edit”** icon.
□ Edit any fields as described above.
□ Click the **“Save”** button.

Note: You cannot edit the strategy name.

- ■ **Deleting a Guest access strategy**

□ Select a strategy(ies) in the Guest Access Strategy List.
□ Click the **“Delete”** icon.
□ Click **“Yes”** on the Confirmation Prompt.

Note: You cannot delete the Default Guest Access Strategy.

8.4.3 Guest account

Guest Account is used to manage the set of guest accounts.

□ You can add one item by clicking the **“+”** icon. Or you can download the account template.

- □ Enter the guest accounts.
- □ Click the **"Batch Import"** button to import the accounts batch-wise.
- □ Click the **"Enable/disable"** button to enable or disable the guest account.

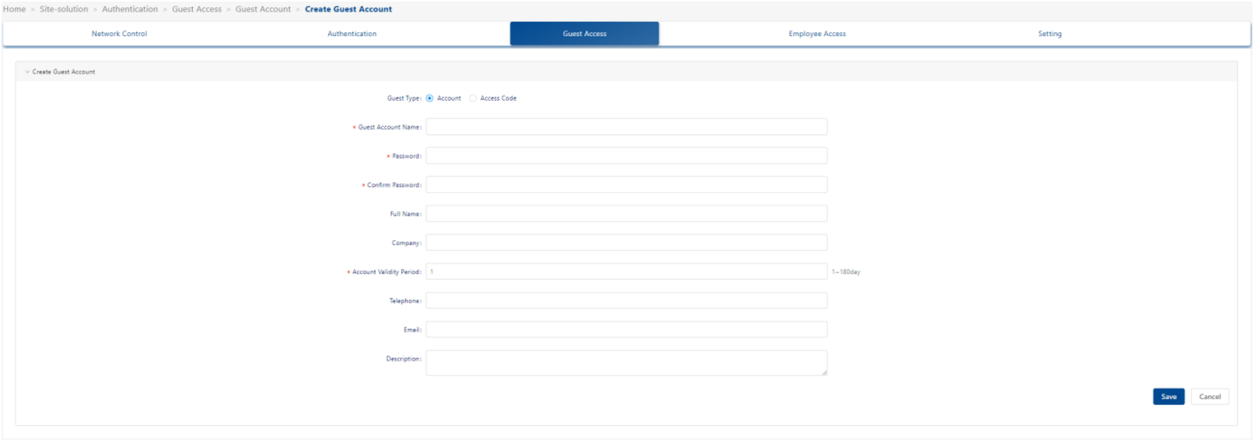
- ■ **Creating a Guest account:**

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

- □ Click the **"Add"** icon. Then the **"Create Guest Account"** screen appears.
- □ Enter the fields as described below.
- □ Click the **"Save"** button. When an account is created, it is automatically enabled.
- □ To disable an account, select the account and click the **"Disable"** icon at the top of the screen.

Guest types in account:

- ▶ **Guest Account Name:** Account identifier (e.g., name of the guest).
- ▶ **Password:** Password for the account.
- ▶ **Confirm Password:** Re-enter and confirm the account password.
- ▶ **Full Name:** The full name of the Guest User.
- ▶ **Company:** Company name.
- ▶ **Account Valid Period:** The length of time that the guest account is valid. (Possible values: 1..180 Days, Default Setting: 90 Days).
- ▶ **Telephone:** Telephone number of the Guest User.
- ▶ **Email:** The email address of the Guest User.
- ▶ **Description:** Description of the account.



Guest Type: ● Account ○ Access Code

* Guest Account Name:

* Password:

* Confirm Password:

Full Name:

Company:

* Account Validity Period: 1 1~180day

Telephone:

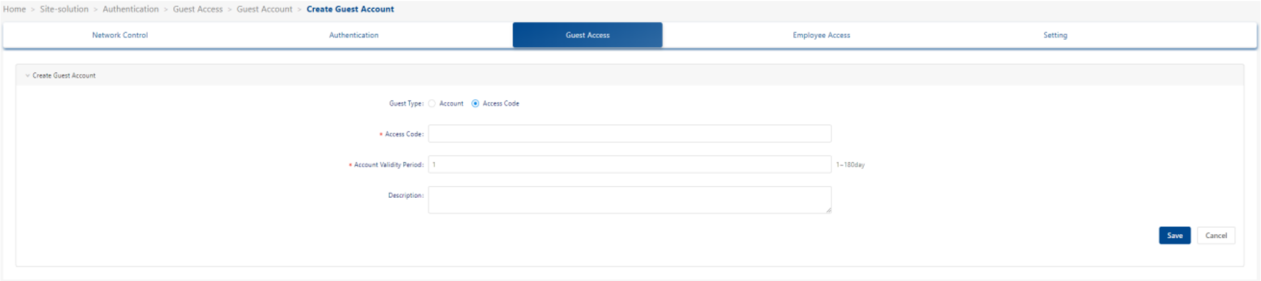
Email:

Description:

Figure 161: Guest Account – “Account” Guest Type

Guest types in access code:

- **Access Code:** Access Code.
- **Account Validity Period:** The length of time that the guest account is valid. (Possible values: 1..180 Days, Default Setting: 90 Days).
- **Description:** Description of the Access Code.



Guest Type: ○ Account ● Access Code

* Access Code:

* Account Validity Period: 1 1~180day

Description:

Figure 162: Guest Account – “Access Code” Guest Type

■ Editing a Guest account/access code

□ Select a Guest Account in the Guest Account List.

□ Click the **“Edit”** icon.

□ Edit the field(s) as described above.

□ Click the **“Save”** button.

Note: You cannot edit an account name.

■ Deleting a Guest account/access Code

□ Select a Guest Account in the Guest Account List.

☐ Click the **“Delete”** icon.
☐ Click **“Yes”** on the Confirmation Prompt.

8.4.4 Guest device

Guest device consists of the following two device lists:

- ▶ Online Devices list
- ▶ Remembered Devices list

■ **Online devices**

Online devices list the devices online currently.

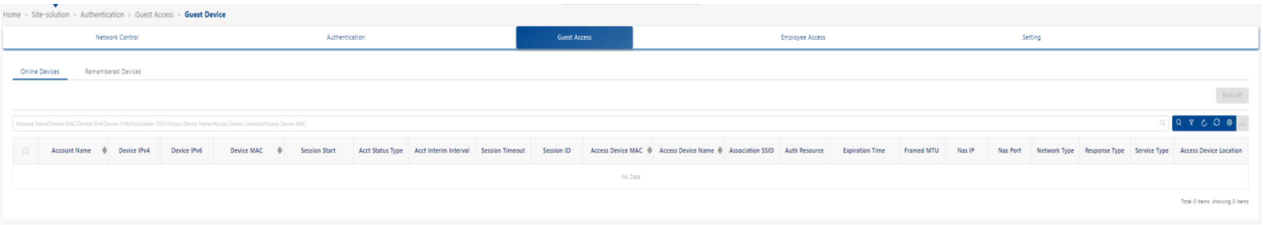
- ▶ **Account Name:** The account of the terminal access network.
- ▶ **Device IPv4:** The IPv4 address of the client device of the user requesting authentication.

  Note: IP addresses are displayed only if they are known at the time the RADIUS Accounting packets are sent or received. For MAC Authentication, the Accounting Start packets typically do not contain client IP addresses. It will update after the next Accounting Update packet is received.
- ▶ **Device IPv6:** The IPv6 address of the client of the user device requesting authentication.

  Note: IP addresses are displayed only if they are known at the time the RADIUS Accounting packets are sent or 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 passes authentication and a connection session is 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 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 the device with which the terminal is associated.
- **Access Device Name:** The name of the device with which the terminal is associated.
- **Association SSID:** The SSID that the terminal association uses.
- **Auth Resource:** The user profile database used in authentication (e.g., None, Local Database, LDAP/AD, external RADIUS server). You can refer to the authentication strategy definition.
- **Expiration Time:** Expiration time of the 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 be accessed by Login User.
- **Access Device Location:** The location of the device with which the terminal is associated.


Home > Site-solution > Authentication > Guest Access > Guest Device
Network Control
Authentication
Guest Access
Employee Access
Setting
Online Devices
Remembered Devices
Kick-off
Account Name/Device MAC/Device IPv4/Device IPv6/Association SSID/Access Device Name/Access Device Location/Access Device MAC

□	Account Name	Device IPv4	Device IPv6	Device MAC	Session Start	Acct Status Type	Acct Interim Interval	Session Timeout	Session ID	Access Device MAC	Access Device Name	Association SSID	Auth Resource	Expiration Time	Framed MTU	Nas IP	Nas Port	Network Type	Response Type	Service Type	Access Device Location
										No Data											

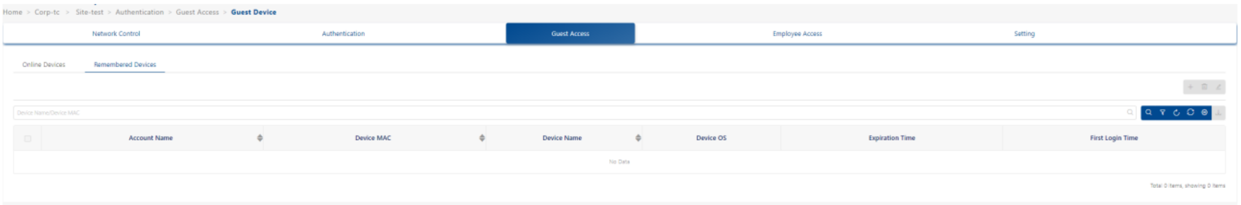
Total 0 items, showing 0 items

Figure 163: Guest Devices

- **Remembered 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 MAC:** The MAC address of the remembered device.
  - **Device Name:** The name of the remembered device.
  - **Device OS:** The OS of the remembered device.
  - **Expiration Time:** The expiration time of the device.
  - **First Login Time:** The first login time is recorded.



□	Account Name	Device MAC	Device Name	Device OS	Expiration Time	First Login Time
No Data						

Total 0 items, showing 0 items

Figure 164: Remembered Devices

8.5 Employee access

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

8.5.1 Dashboard

The Dashboard consists of the following three diagrams:

- **Remembered Employee Device:** Histogram of the remembered device and online device for last seven days.
- **Devices Category:** Pie chart of Device Category (Computer, Mobile, and so on).
- **Device Family:** Displays information by device family (e.g., Apple, IBM, Huawei, Xiaomi) in a pie chart format.

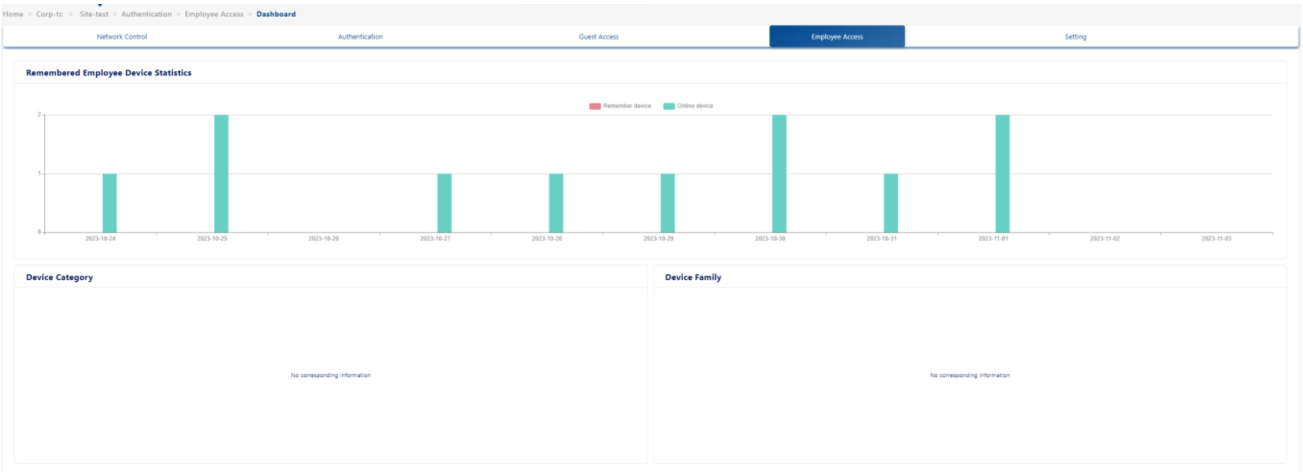
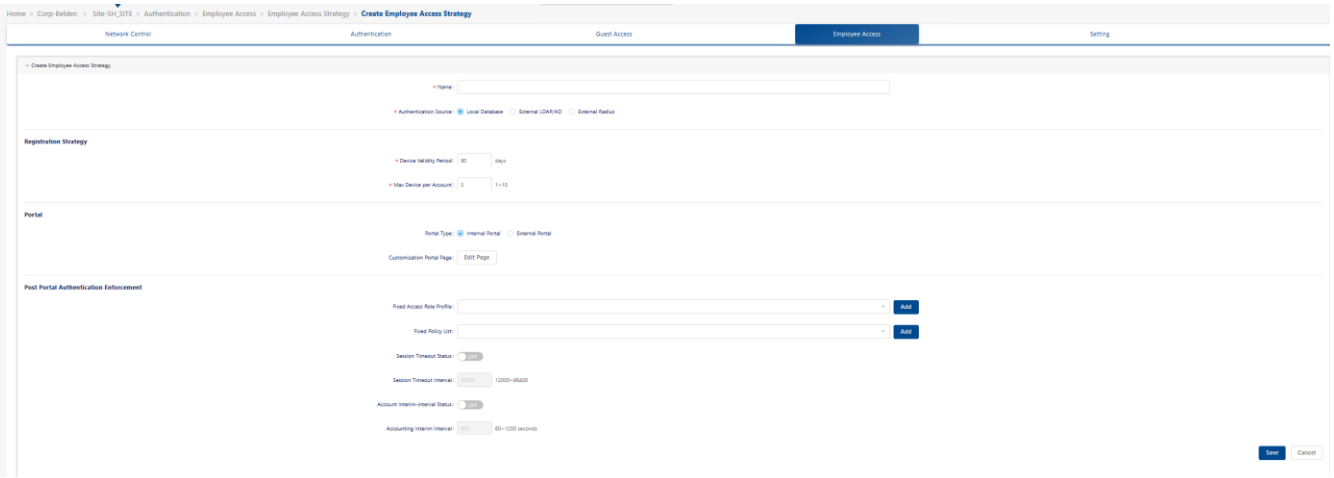


Figure 165: Employee access dashboard

8.5.2 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 or AD, and external RADIUS), account validity and device validity, the maximum number of online devices, specify Access Role Profile policies, edit portal templates, etc.

- **Name:** Employee strategy name.
- **Authentication Source:** Specify the authentication data source.
- **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 sign in the same account at the same time.
- **Portal Type:** The source of the portal. It can be given by the DAC or an external source.
- **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 completed, the Access Role Profile assigned to the terminal controls the Internet access behavior of the terminal.
- **Fixed Policy List:** When this authentication phase is over, the Policy List assigned to the AP is used to give process policy for the terminal message.
- **Session Timeout Interval:** Specify the interval for the AP to send a session message.
- **Accounting Interim Interval:** Specify the time interval that the AP sends an accounting message.


Home > Corp-Belden > Site-SH_SITE > Authentication > Employee Access > Employee Access Strategy > Create Employee Access Strategy
Network Control
Authentication
Guest Access
Employee Access
Setting
Create Employee Access Strategy
Add
Add
Save
Cancel

* Name:

* Authentication Source: ● Local Database ○ External LDAP/AD ○ External Radius

Registration Strategy

* Device Validity Period: 90 days

* Max Device per Account: 3 1~10

Portal

Portal Type: ● Internal Portal ○ External Portal

Customization Portal Page: Edit Page

Post Portal Authentication Enforcement

Fixed Access Role Profile:

Fixed Policy List:

Session Timeout Status: OFF

Session Timeout Interval: 43200 12000~86400

Account Interim-interval Status: OFF

Accounting Interim Interval: 600 60~1200 seconds

Figure 166: Employee access strategy

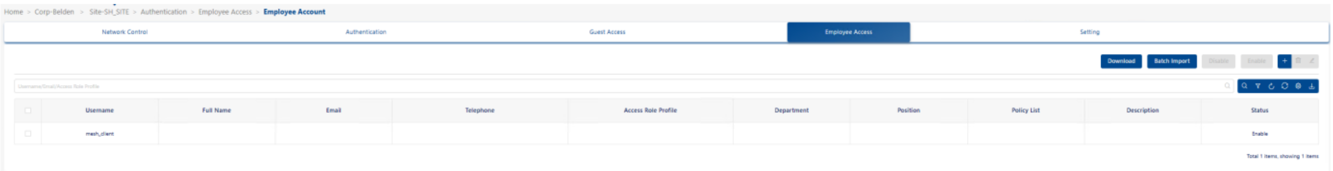
8.5.3 Employee account

Employee Account manages the set of employee terminal accounts.

- □ Click the **“+”** icon or download the account template to add one item.
- □ Enter the employee account details. The batch imported the accounts.
- □ Click the **“Enable/Disable”** button to enable or disable the employee account manually.

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

- ▶ **Username:** The username of the employee account.
- ▶ **Full Name:** The full name of the employee.
- ▶ **Email:** The email address of the employee.
- ▶ **Telephone:** The telephone number of the employee.
- ▶ **Access Role Profile:** Access Role Profile is bound to the employee account. It is prior to the Access Role Profile configured in authentication strategy.
- ▶ **Department:** Department of the employee.
- ▶ **Position:** Employee position in the company.
- ▶ **Policy List:** A Policy List is bound to the employee account. It is prior to the Policy List configured in an authentication strategy.
- ▶ **Description:** Description of the employee account.
- ▶ **Status:** The employee account is enabled or disabled.


Home > Corp-Belden > Site-SH_SITE > Authentication > Employee Access > Employee Account
Network Control
Authentication
Guest Access
Employee Access
Setting
Download
Batch Import
Disable
Enable
+
Username/Email/Access Role Profile

□	Username	Full Name	Email	Telephone	Access Role Profile	Department	Position	Policy List	Description	Status
□	mesh_client									Enable

Total 1 items, showing 1 items

Figure 167: Employee account

- ■ **Create an employee account:**
  - ▶ **Username:** The username of the employee account.
  - ▶ **Password:** Password of the employee account.
  - ▶ **Repeat Password:** Re-enter to confirm the employee password.

- ▶ **Telephone:** The telephone number of the employee.
- ▶ **Email:** The email address of the employee.
- ▶ **Access Role Profile:** Access Role Profile is bound to the employee account. It is prior to the Access Role Profile configured in authentication Strategy.
- ▶ **Policy List:** A Policy List is bound to the employee account. It is prior to the Policy List configured in an authentication Strategy.
- ▶ **Full Name:** The full name of the employee.
- ▶ **Department:** Department of the employee.
- ▶ **Position:** Employee position in the company.
- ▶ **Description:** Description of the employee account.

■ **Edit an employee account**

□ Select an employee account in the Employee Account List.
□ Click the **“Edit”** icon.
□ Edit the field(s) described above.
□ Click the **“Save”** button.
Note: You cannot edit a username.

■ **Delete an employee account**

□ Select an employee account in the Employee Account List.
□ Click the **“Delete”** icon.
□ Click **“Yes”** on the confirmation prompt.

8.5.4 Employee devices

Employee Devices consist of the following two types:

- ▶ Online Device
- ▶ Remember Device

Online Device lists the devices online.

Remembered Device lists the devices that are authentication-free in the next access process during the device validity period.

■ **Online device**

The Online Devices List displays information about devices associated with an employee account that have accessed the network.

☐ Select a device from the list.
☐ Click the **“Kick-off”** button to log the user out immediately.
☐ The user will have to log in again to connect to the network.

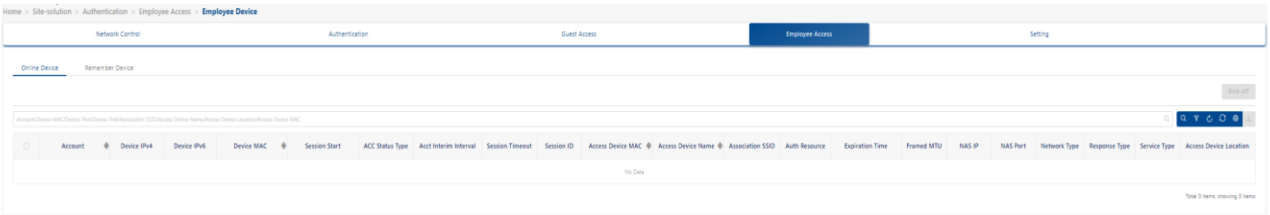
- **Account:** The employee account with which the company device is associated.
- **Device IPv4:** The IPv4 address of the client device that the user requests authentication.

  Note: IP addresses are displayed only if they are known when the RADIUS Accounting packets are sent or received. For MAC Authentication, the Accounting Start packets typically do not contain client IP addresses.
- **Device IPv6:** The IPv6 address of the client device that the user requests authentication.

  Note: IP addresses are displayed only if they are known when the RADIUS Accounting packets are sent or 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 passes authentication and a connection session is created.
- **Acct Status Type:** Indicates whether this Accounting Request message marks the beginning of the user’s service or the end.
- **Acct Interim Interval:** The time between each interim update, in seconds, for this specific session.
- **Session Timeout:** The maximum number of consecutive seconds that a connection is allowed to the user before termination of the session or prompt.
- **Session ID:** Session ID 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 the device with which the terminal is associated.
- **Access Device Name:** The name of device that is associated with

the terminal.

- **Association SSID:** The SSID of the terminal association uses.
- **Auth Resource:** The user profile database used in authentication (e.g., None, Local Database, LDAP/AD, and external RADIUS server). It can refer to the authentication strategy definition.
- **Expiration Time:** The expiration time of this device.
- **Framed MTU:** The Maximum Transmission Unit is configured for the user when it is not negotiated by some other means (e.g., PPP). It has a fixed value = 1400.
- **NAS IP:** The IP Address of the DAP.
- **NAS Port:** The physical port number of the NAS authentication 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 be accessed by login user.
- **Access Device Location:** The location of the device with which the terminal is associated.


Home > Site-solution > Authentication > Employee Access > Employee Device
Network Control
Authentication
Guest Access
Employee Access
Setting
Online Device
Remember Device
Kick-off
Account/Device MAC/Device IPv4/Device IPv6/Association SSID/Access Device Name/Access Device Location/Access Device MAC

□	Account	Device IPv4	Device IPv6	Device MAC	Session Start	ACC Status Type	Acct Interim Interval	Session Timeout	Session ID	Access Device MAC	Access Device Name	Association SSID	Auth Resource	Expiration Time	Framed MTU	NAS IP	NAS Port	Network Type	Response Type	Service Type	Access Device Location
										No Data											

Total 0 items, showing 0 items

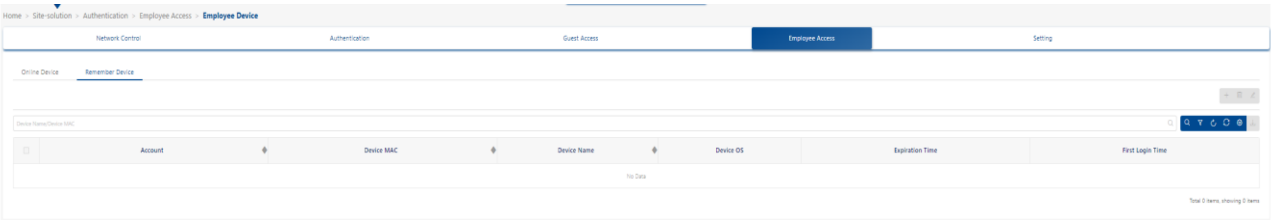
Figure 168: Employee device - Online Device

- **Remember device**

Remember Device lists the devices that are authentication-free in the next access process during the device validity period.

- **Account:** The account of the remembered device.
- **Device MAC:** The MAC address of the remembered device.
- **Device Name:** The name of the remembered device.
- **Device OS:** The OS of the remembered device.

- **Expiration Time:** The expiration time of the remembered device.
- **First Login Time:** The first login time recorded.



□	Account	Device MAC	Device Name	Device OS	Expiration Time	First Login Time
			No Data			

Total 0 items, showing 0 items

Figure 169: Employee device - Remember Device

8.6 Settings

The **Settings** include the following configurations.

8.6.1 Company device

Company device is used to manage the set of devices owned by a company, such as printers, IP phones, laptops, and tablets.

□ Click the **"+"** icon or download the account template to add one item.
□ Enter the fields with the name of the company device. The batch imports the accounts. You can export all the company device in .xlsx format.

- **Create a company device**
  - ▶ **Device MAC:** MAC address of the company device.
  - ▶ **Device Name:** The system name of the company's device.
  - ▶ **Account:** The employee account with 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:** The operation system of the company device (e.g., Linux, Windows, iOS).
  - ▶ **Device Specific PSK:** If enabled, you must set the password and Passphrase Validity Period. This function needs to work with the WLAN settings of Device Specific PSK.
  - ▶ **Access Role Profile:** Access Role Profile is bound to the company device. It is prior to the ARP configured in the authentication strategy.
  - ▶ **Policy List:** Policy List is bound to the company device. It is prior to the policy list configured in the authentication strategy.

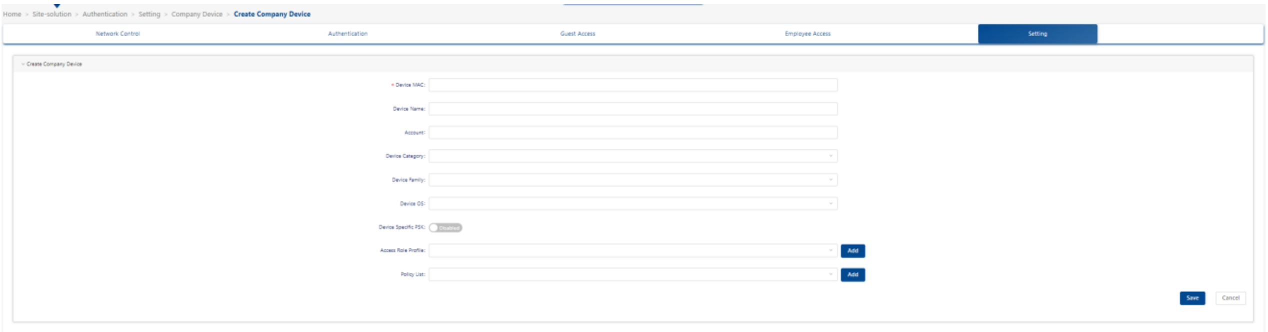


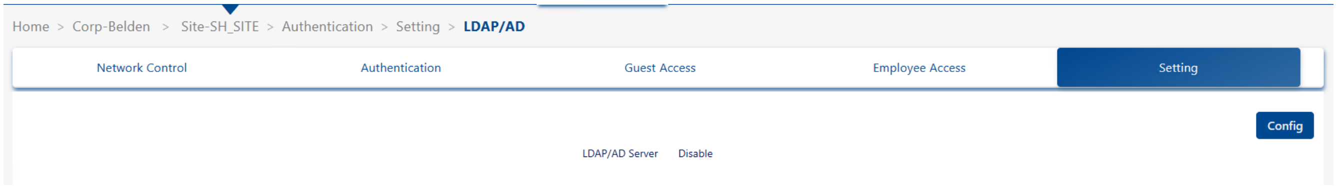
Figure 170: Create Company Device

- ■ **Delete a company device**
- ☐ Select a Company Device to delete.
- ☐ Click the **“Delete”** icon.
- ☐ Click the **“Yes”** button on the confirmation prompt.

8.6.2 LDAP/AD configuration

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

Click the **“Config”** button to set the following:


Home > Corp-Belden > Site-SH_SITE > Authentication > Setting > LDAP/AD
Network Control
Authentication
Guest Access
Employee Access
Setting
Config

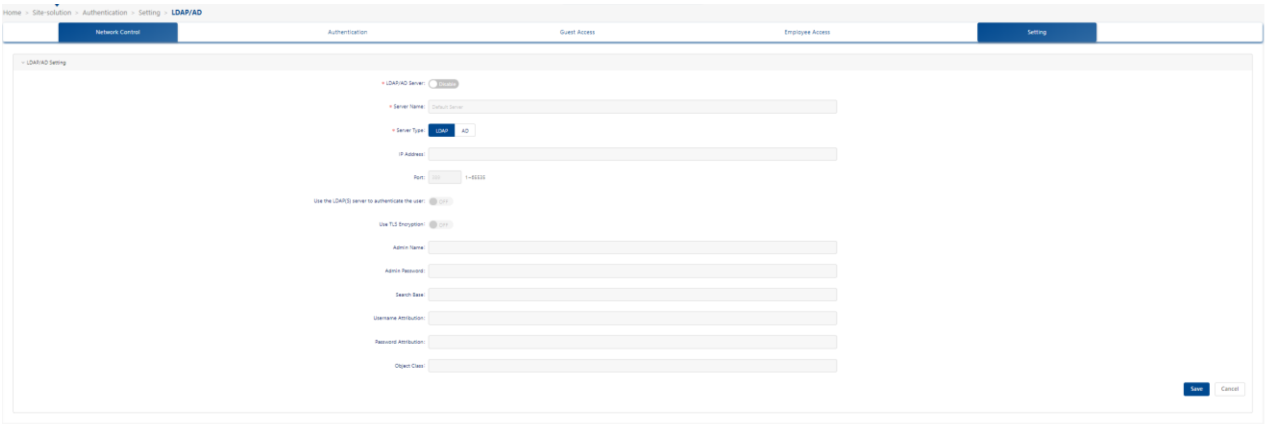
LDAP/AD Server Disable

Figure 171: LDAP/AD configuration

- ■ **LDAP configuration**
  - ▶ **LDAP/AD Server:** Enable or disable an LDAP or AD server.
  - ▶ **Server Type:** Selector of an LDAP or AD server**.**
  - ▶ **IP Address:** The IP address of the LDAP server.
  - ▶ **Port:** The port of the LDAP server.
  - ▶ **Use TLS Encryption:** The switch of using TLS. If turn it on, you

should upload the certification.

- **Certificate:** To upload the certification used by TLS, you should get the certification from the external LDAP server.
- **Admin Name:** Administrator account used to log in to the LDAP server. (Format: cn=, DC: < 8-64 characters >)
- **Admin Password:** Administrator password used to log in to 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)



Home > Site-solution > Authentication > Setting > LDAP/AD

LDAP/AD Setting

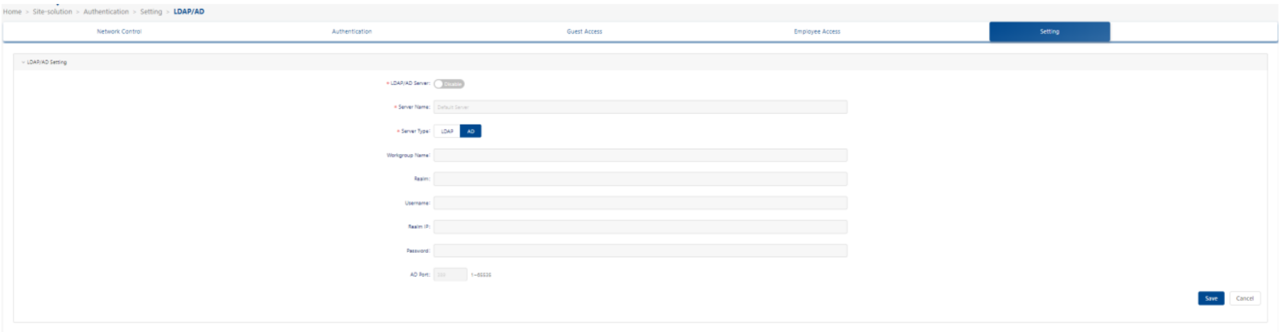
* LDAP/AD Server: Disable
* Server Name: Default Server
* Server Type: LDAP AD
IP Address:
Port: 389 1~65535
Use the LDAP(S) server to authenticate the user: OFF
Use TLS Encryption: OFF
Admin Name:
Admin Password:
Search Base:
Username Attribution:
Password Attribution:
Object Class:

Figure 172: LDAP/AD Setting – “LDAP” Server Type

AD configuration

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

Note: Configure DNS settings for the Ubuntu system or VM initialization to load the Windows AD server configuration.



LDAP/AD Setting

* LDAP/AD Server: Disable

* Server Name: Default Server

* Server Type: LDAP [✓ AD]

Workgroup Name:

Realm:

Username:

Realm IP:

Password:

AD Port: 1~65535

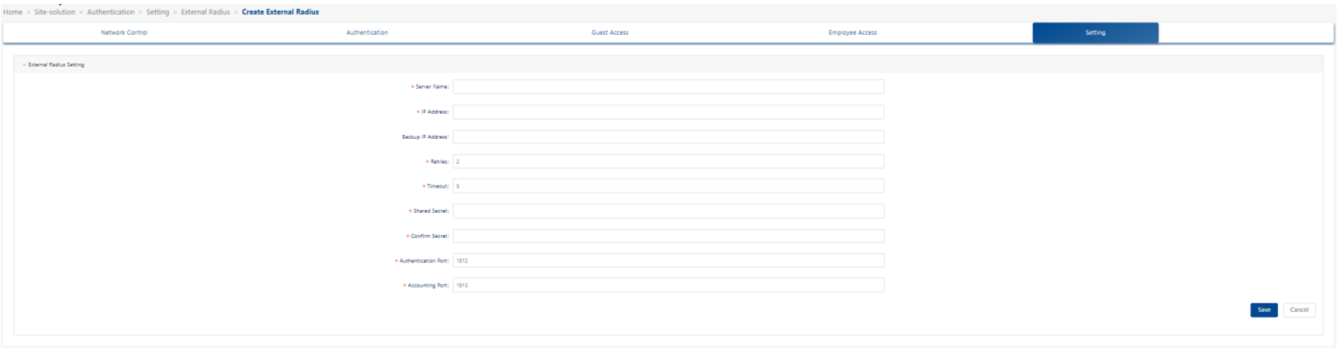
Figure 173: LDAP/AP Setting – "AD" Server Type

8.6.3 External RADIUS

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

Click the **"+"** icon to open the "**External Radius Setting"** window.

- **Server Name:** Name of the RADIUS server.
- **IP Address:** Host name/IP address of external Radius server.
- **Backup IP Address:** Back up the host name or IP address of external radius server.
- **Retries:** The number of times DAC will attempt to reconnect to the external Radius server when the connection timeout occurs. If the number of connection attempts reaches the maximum number of connection attempts and the connection is not successful, the external RADIUS service is deemed unreachable. (Possible values: 1..3, Default Setting: 3)
- **Timeout:** The amount of time in seconds that the DAC will attempt a connection to the external Radius server before timing out. (Possible values: 1..30, Default Setting: 5)
- **Shared Secret:** A shared key that DAC uses to communicate with the 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. (Possible values: 1..65535, Default value: 1812)
- **Accounting Port:** TCP/UDP port used to perform accounting. (Possible values: 1..65535, Default value: 1813)



Home > Site-solution > Authentication > Setting > External Radius > **Create External Radius**

External Radius Setting

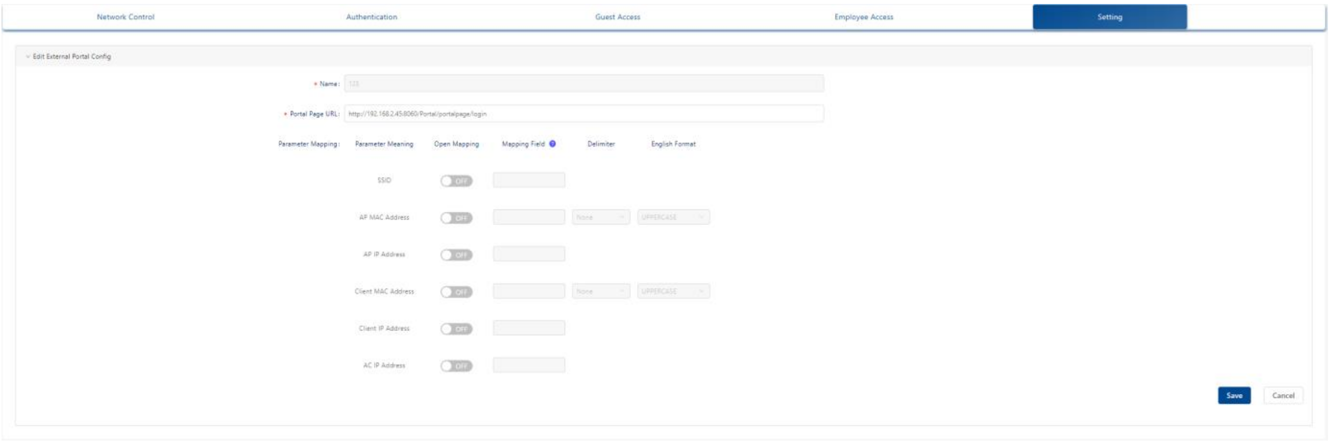
- * Server Name:
- * IP Address:
- Backup IP Address:
- * Retries: 2
- * Timeout: 5
- * Shared Secret:
- * Confirm Secret:
- * Authentication Port: 1812
- * Accounting Port: 1813

Figure 174: External RADIUS

8.6.4 External Portal

The DAC allows the user to indicate the external portal which is only used in the **Employee Access Strategy**.

- **For External Portal configuration**
  - **Name:** The name of the External Portal configuration. Cannot be changed once the configuration is created.
  - **Portal Page URL:** The URL of the external portal.
  - **Parameter Mapping:** The parameters of the DAC used are mapped to the parameters of the external portal.



Edit External Portal Config

- * Name: 123
- * Portal Page URL: http://192.168.2.45:8060/Portal/portalpage/login

Parameter Mapping:

Parameter Meaning	Open Mapping	Mapping Field	Delimiter	English Format
SSID	OFF			
AP MAC Address	OFF		None	UPPERCASE
AP IP Address	OFF			
Client MAC Address	OFF		None	UPPERCASE
Client IP Address	OFF			
AC IP Address	OFF			

Figure 175: External Portal

8.6.5 Allowed IP

An allowed IP is one that a terminal can access before logging in from the captive portal. Usually, you should add the portal server’s IP to the Allowed IP.

- **Create an allowed IP**

- □ Click the **“+”** icon. Then the **“Create Allowed IP”** appears**.**
- □ Specify **“Name”** and **“IP Address”** fields.
- □ Click the **“Save”** button to save the allowed IP.
  - ▶ **Name:** The name of the allowed IP.
  - ▶ **IP Address:** The settings of the IP address.

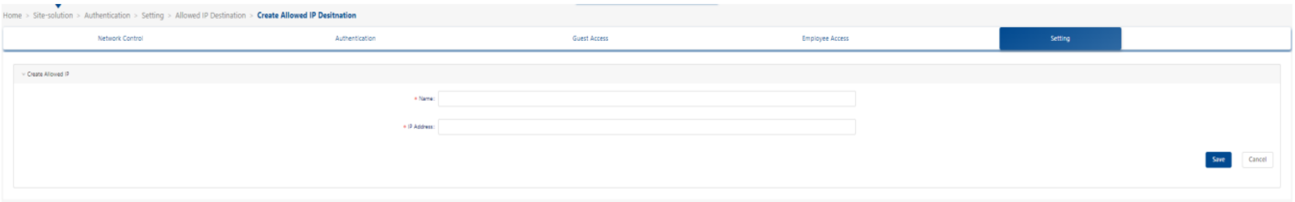


Figure 176: Create Allowed IP

- **Edit an allowed IP**

- □ Select an allowed IP from the list.
- □ Click the **“Edit”** icon, and the **“Edit Allowed IP”** screen appears.
- □ Specify the “**IP Address”** field.
- □ Click the **“Save”** button to save the settings.

Note: The **Name** field cannot be changed.

- **Delete an allowed IP**

- □ Select the allowed IP that you want to delete.
- □ Click the **“Delete”** icon.
- □ Click the **“Yes”** button on the confirmation prompt.

8.6.6 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 to create various policy conditions, such as source MAC Group conditions and destination MAC Group conditions.

- **Create a MAC Group**

- □ Click the **“+”** icon. Then the “**Create MAC Group”** screen appears.

- ☐ Enter **“Name”** for the MAC Group.
- ☐ Enter the **“MAC Address”**.
- ☐ Click the **“Add”** button.
- ☐ Repeat to add additional addresses.
- ☐ Click the **“Add”** button at the bottom. The MAC Group appears in MAC Groups List.

Note: You must enter at least one MAC Address.

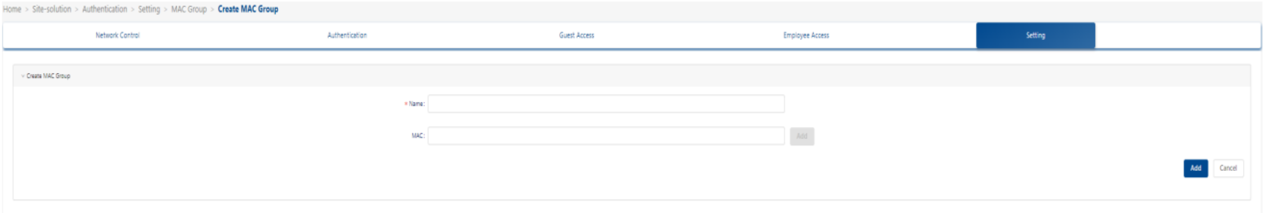


Figure 177: Create MAC Group

■ Edit a MAC Group

- ☐ Select the MAC Group that you want to edit.
- ☐ Click the **“Edit”** icon, and the **“Edit MAC Group”** screen appears.

Note: You cannot edit a MAC Group name. To edit a MAC Group name, you must delete the MAC Group and create a new one.

Add a MAC address to the Group:

- ☐ Enter the MAC Address.
- ☐ Click the **“Add”** button.
- ☐ Repeat to add additional addresses.
- ☐ When you complete, click the **“Edit”** button.

Delete a MAC address:

- ☐ Click the **“Delete”** icon next to the MAC Address you want to delete.
- ☐ Repeat to delete additional addresses.
- ☐ When you finish, click the **Edit** button.

Edit a MAC address:

- ☐ Delete the MAC Address.
- ☐ Add a new MAC Address.

■ Delete a MAC Group

- □ To delete a MAC Group, select the checkbox next to the Group in the list.
- □ Click the **“Delete”** icon.
- □ Click **“Yes”** on the confirmation prompt.

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

8.6.7 IP Groups

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

■ Create an IP Group

- □ Click the **“+”** icon.
- □ Enter the **“Name”** for the IP Group.
- □ Enter the **“Subnet IP/Subnet Mask”** field.
- □ Click the **“Add”** button.
- □ Repeat to add additional subnets. When you finish, click the **“Add”** button at the bottom.

  The IP Group appears in the IP Groups List.

Note: You must enter at least one Subnet IP/Subnet Mask.

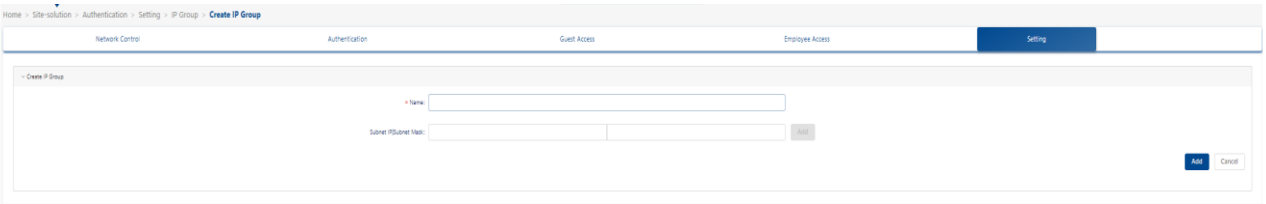


Figure 178: Create IP Group

■ Edit an IP Group

- □ Click the IP Group that you want to edit to view the Subnets in the IP Group.

Note: You cannot edit an IP Group name. To edit an IP Group name, you must delete the Network Group and create a new one.

Add a Subnet address to the Group:

□ Enter the **“Subnet IP/Subnet Mask”** field.
□ Click the **“Add”** icon.
□ Repeat to add additional subnets. When you finish, click the **“Edit”** button.

Delete a Subnet:

□ Click the **“Delete”** icon next to the Subnet you want to delete.
□ Repeat to delete Subnets.
□ When you finish, click the **“Edit”** button.

Edit a Subnet:

□ Delete the Subnet.
□ Add a new one.
□ When you finish, click the **“Edit”** button.

■ **Delete a IP Group**

□ To delete a IP Group(s), select the checkbox next to the Group(s) in the list.
□ Click the **“Delete”** icon.
□ Click **“Yes”** on the confirmation prompt.

IP Groups that are used under policy conditions cannot be deleted. To delete these IP groups, remove them from the policy conditions.

8.6.8 Service

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

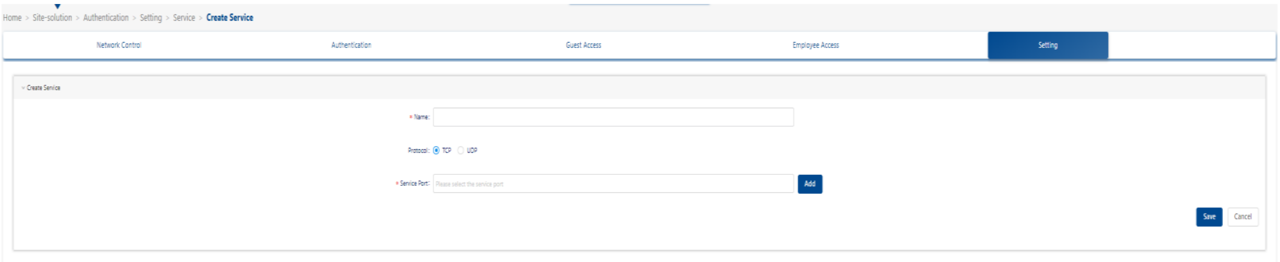
■ **Create a service**

□ Click the **“+”** icon.
□ Edit the fields as described below.
□ Click the **“Save”** button.

- ▶ **Name:** User-configured name for the Service.
- ▶ **Protocol:** Select a protocol for the service. By default, the TCP is

selected, and TCP ports are displayed. Click the UDP to display UDP ports.

- ▶ **Service Port:** Select a service port from the drop-down list. If you want to create a new service port, then click the **“Add”** icon which appears the **“Service Port”** screen and create a new service port. When you click the **“Save”** button on the **“Service Port”** screen you will be returned to the **“Create Service”** screen to finish creating the service.



* Name:

Protocol: ● TCP ○ UDP

* Service Port: Please select the service port

Figure 179: Create Service

■ Edit a service

- □ Click the service that you want to edit.
- □ Click the **“Edit”** icon.
- □ Edit the fields as described above.
- □ Click the **“Save”** button.

Note: You cannot edit a service name. To edit a service name, you must delete the service and create a new one.

■ Delete a service

- □ To delete a service, select the checkbox next to the Service in the list.
- □ Click the **“Delete”** icon.
- □ Click **“Yes”** on 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.

8.6.9 Service Groups

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

- **Create a Service Group**

☐ Click the **"+"** icon.
☐ Enter the **"Group Name"** for the Service Group.
☐ Select a service and click the **"Save"** button.
☐ Click the **"Add"** Icon, and the **"Services"** screen appears. You can create the Service.
☐ Click the **"Save"** button, and the **"Create Service Group"** screen appears.

Note: You must enter at least one service.

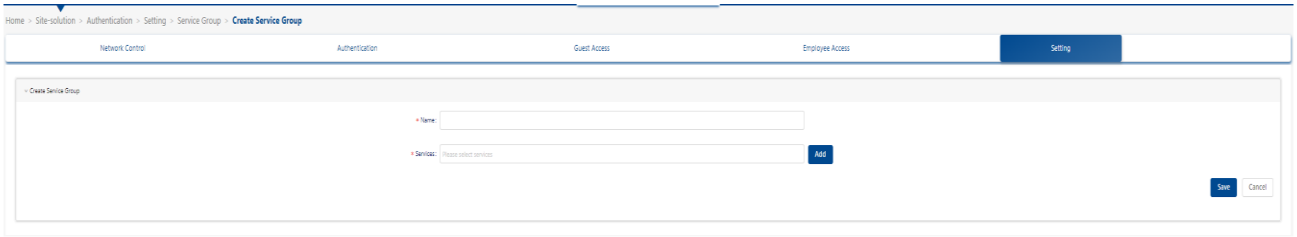


Figure 180: Create Service Group

- **Edit a Service Group**

☐ Click the Service Group that you want to edit.
☐ Click the **"Edit"** Icon.
☐ Add or remove services.
☐ Click the **"Edit"** button.

Note: You cannot edit a Service Group name. To edit a Service Group name, you must delete the Service Group and create a new one.

- **Delete a Service Group**

☐ To delete a Service Group, select the checkbox next to the Group in the list.
☐ Click the **"Delete"** icon.
☐ Click **"Yes"** on the confirmation prompt.

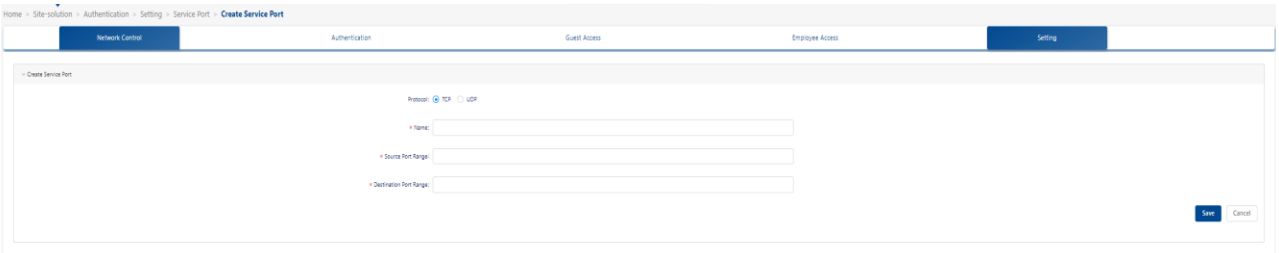
Note: Service Groups that are used in policy conditions cannot be deleted. To delete these Service Groups, remove them from the policy conditions.

8.6.10 Service port

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

■ Create a service port

- □ Click the **“+”** icon.
- □ Edit the fields as described below.
- □ Click the **“Save”** button.
  - ▶ **Protocol:** TCP or UDP.
  - ▶ **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.



Protocol: ● TCP ○ UDP

* Name:

* Source Port Range:

* Destination Port Range:

Figure 181: Create Service Port

■ Edit a service port

- □ Click the service port that you want to edit.
- □ Click the **“Edit”** icon.
- □ Edit the field(s) as described above.
- □ Click the **“Save”** button.

You cannot edit the service port name and the protocol. To edit the name of service port, you must delete the service port and create a new one.

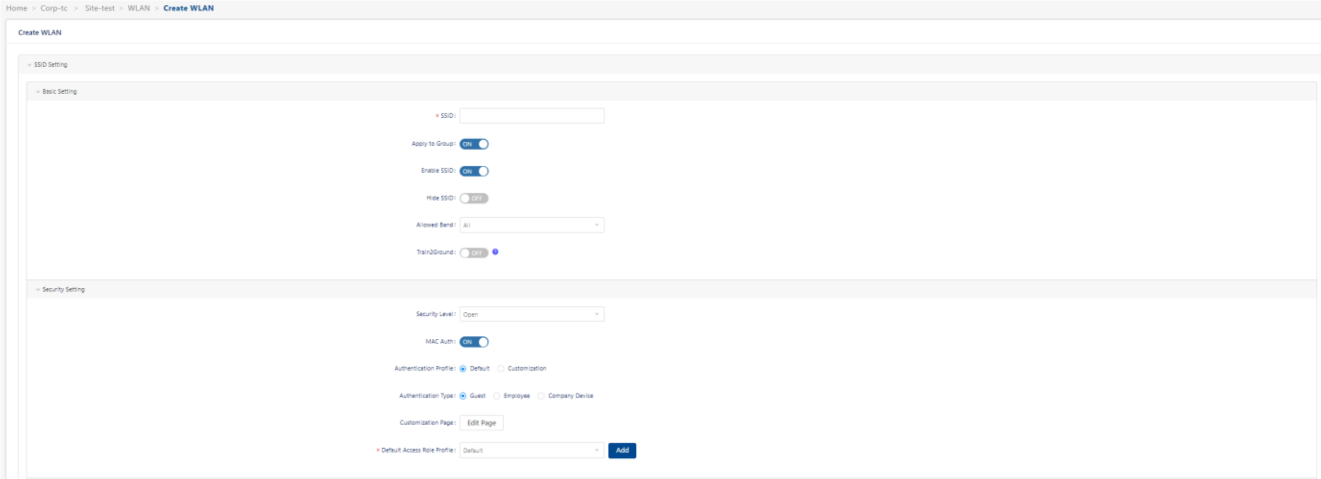
■ Delete a service port

- □ To delete a Service Port, select the checkbox next to the port in the list.
- □ Click the **“Delete”** icon.
- □ Click **“Yes”** on the confirmation prompt.

Service ports that are used by services cannot be deleted. To delete these Service Ports, remove them from the services.

8.7 Default config and quick entrance

All the above configurations are indirectly bound to WLAN. To simplify the configuration, you 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:



* SSID:
Apply to Group: ON
Enable SSID: ON
Hide SSID: OFF
Allowed Band: All
Train2Ground: OFF
Security Level: Open
MAC Auth: ON
Authentication Profile: ● Default ○ Customization
Authentication Type: ● Guest ○ Employee ○ Company Device
Customization Page: Edit Page
* Default Access Role Profile: Default

Figure 182: Create WLAN

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 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 cannot view or edit these configurations directly.

The default authentication configurations automatically generated is the following:

- When you select **“Guest”** for authentication type, an authentication strategy will generate automatically 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 Customization Page.
- When you select **“Employee”** as 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 bound to the authentication strategy. You can customize the portal page in Customization Page.

□ When you select **“Company Device”** as authentication type, an authentication strategy with a local database as the data source will be automatically generated.

□ At last, it will generate an access policy with SSID as the mapping condition, with the highest priority and bind it with the authentication strategy mentioned previously.

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

8.8 Configuration instance for authentication

Before introducing specific configuration instances, you should understand the basic concepts of authentication in DAC. See “Authentication” on page 139.

8.8.1 Configure default 802.1X authentication

☐ On the **“Site”** view page, click the **“WLAN”** tab to view the WLAN list.

☐ Click the **“+”** button to open the **“Create WLAN”** page.

☐ Enter the **SSID** field.

☐ Select **“Enterprise”** as **Security Level** from the drop-down list.

☐ Select the **Encryption Mode** that you want. See “SSID setting” on page 91.

☐ Set the authentication configuration as **Default**, which means it will create the **Access Policy**, **Authentication Strategy,** and **Employee Access Strategy** automatically (if necessary). These policies and strategies are not viewable. But you can see that there are three authentication sources: **Local Database**, **External LDAP/AD**, and **External RADIUS**. These authentication sources are exported from the **Authentication Strategy** created by default. We use this method to simplify some user configurations.

☐ If you select **Local Database** as authentication source, you can add users at the page **Authentication** → **Employee Access** → **Employee Account**. See “Employee account” on page 184.

☐ If you select **LDAP/AD** as authentication source, you should configure LDAP/AD at the page **Authentication** → **Setting** → **LDAP/AD Configuration.** See “LDAP/AD configuration” on page 190. If you want to set a specific **Access Role Profile** to the terminal authenticated by LDAP, then you can set the corresponding mapping rules in **Authentication** → **Authentication** → **Role Mapping for LDAP**.

☐ If you select **External Radius** as authentication source, then you can select an external RADIUS server from the drop-down list. Or click the **“Add”** button to add a new external RADIUS server. You can also add a new external RADIUS server at **Authentication page**→ **Settings** → **External Radius**. See “External RADIUS” on page 192.

☐ At the **Default Access Role Profile**, select a profile from the drop-down list. Or you can add a new access role profile by clicking the **“Add”** button next to it. See “Access role profile” on page 147.

8.8.2 Configure portal authentication simple model

□ On the **“Site”** view page, click the **“WLAN”** tab to view the WLAN list.

□ Click the **“+”** button to open the create WLAN page.

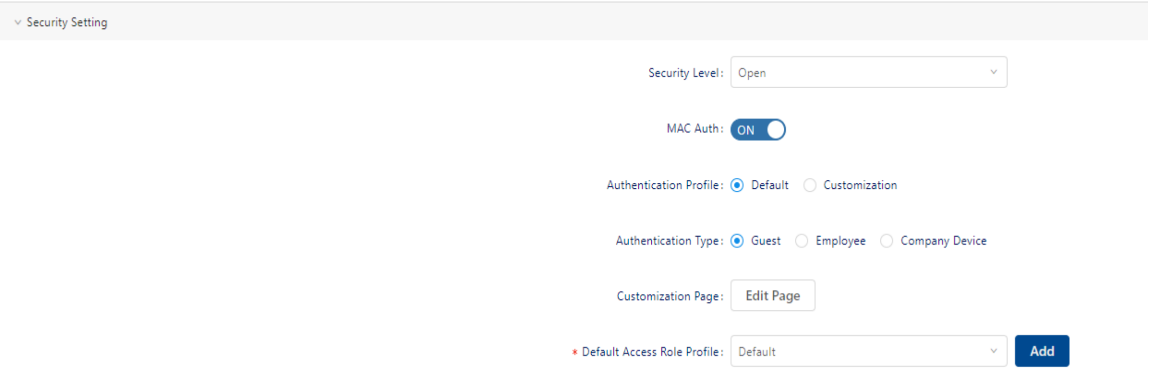
□ Enter the **“SSID**” field.

□ Select **“Open”** from the **Security Level** drop-down list.

□ Set the **Mac Auth** to **“ON”** status.

□ Select **“Default**” in the authentication configuration.

Note: The Authentication source cannot be changed for the **“Open”** security level. The local database of DAC is used by default.



Security Setting

Security Level: Open

MAC Auth: ON

Authentication Profile: ● Default ○ Customization

Authentication Type: ● Guest ○ Employee ○ Company Device

Customization Page: Edit Page

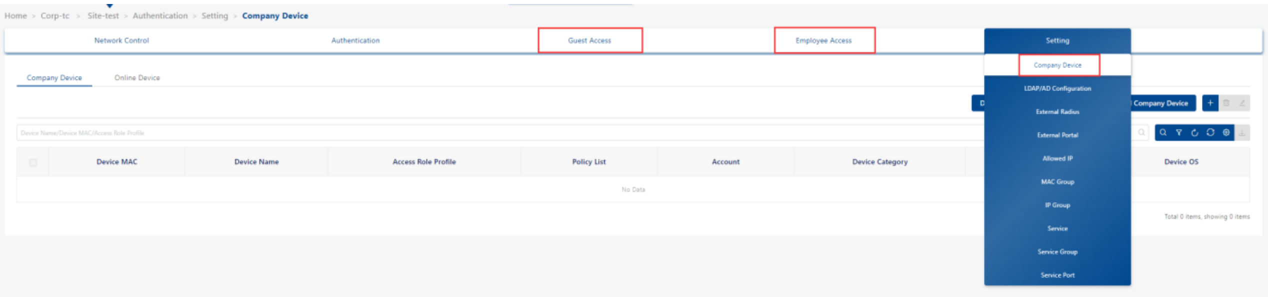
* Default Access Role Profile: Default Add

Figure 183: Configure portal authentication - WLAN Configuration

□ Select **“Guest**” for guest authentication. You can add guest accounts at **Authentication → Guest Access → Guest Account**. See “Guest account” on page 176.

□ Select **“Employee”** for the **“Employee Authentication Strategy”.** You can add employee accounts at **Authentication → Employee Access → Employee Account.** See “Employee account”.

□ **Company device** authentication type is not used in portal authentication. There are some devices without an interactive interface in the enterprise that cannot carry out portal authentication but need to be connected to the wireless network, such as printers. These devices can access WLAN by entering a password in personal mode or MAC authentication. You can add the MAC address of **Company Devices** in page **Authentication → Setting → Company Device**. See “Company device on page 189”.



	Device MAC	Device Name	Access Role Profile	Policy List	Account	Device Category	Device OS
				No Data			

Figure 184: Configure portal authentication - Guest Access/Employee Access/Company Device

- ☐ Click the **“Edit Page”** button to open the **“Portal”** page edit view with an Employee account or a Guest account. See “Captive portal” on page 253 for details about captive portal.
- ☐ At the **Default Access Role Profile**, select a profile from the drop-down list. Or you can add a new **Access Role Profile** by clicking the **“Add”** button next to it. See “Access role profile” on page 147.

8.8.3 Configure customized 802.1X authentication

- ☐ On the **“Site”** view page, click the **“WLAN”** tab to view the WLAN list.
- ☐ Click the **“+”** button to open the create WLAN page.
- ☐ Enter the **“SSID”** field.
- ☐ Select **“Enterprise”** from the **“Security Level”** drop-down list.
- ☐ Select the **“Encryption Mode”** that you want. See “SSID setting” on page 91.
- ☐ Set the authentication configuration to **Customization**, which means you should create the **Access Policy**, **Authentication Strategy**, and **Employee Access Strategy** by yourself.
- ☐ Set the **Mac Auth** to **“OFF”** status.
- ☐ Click **“Effect Now”** to save WLAN and re-enter this page by editing it before continuing. Otherwise, you cannot select an SSID in next step.
- ☐ Click the **“Configuration Wizard”** button. The wizard will show up on the right side. Based on the information in “Access policy” on page 163, we need to create an **Access Policy** and an **Authentication Strategy** respectively. In this wizard, we will create these profiles in turn. Because of the reference relationship in 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**.

☐ After clicking the **"Configuration Wizard"** button, first, click the **"Create Access Policy"** tab and set a **"Name"**. For current 802.1X Authentication, it's better to set the mapping conditions for **SSID** and **Authentication Type**. Select **SSID** in mapping condition's attribute drop-down list and select the **SSID** that you just created in the **Value** drop down list. Then, click the **Add** button to add the condition. 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 the **Add** button to add a new one. See "Access policy" on page 144.

☐ Second, click the **Add** button to add a new **Authentication Strategy**, and 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 have to select a guest or employee access strategy for it. This is no use to our current use case.
- 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 to **None**, which means that this **Authentication Strategy** will be used for 802.1x authentication.
- If you select **External LDAP / AD** as the authentication source, you can see that **Web Authentication** can only be set to **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.
- If you select **External Radius** as the authentication source, you should select one external RADIUS or click the **Add** button to add a new external RADIUS. You should select Web authentication as **None**, which means you can use this authentication strategy for 802.1X authentication. See "Authentication strategy" on page 147.

☐ 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 the **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 during the interval of the **Accounting Interim Interval**.

8.8.4 Configure web portal authentication

- ☐ On the **"Site"** view page, click the **"WLAN"** tab to view the WLAN list.
- ☐ Click the **"+"** button to open the **"Create WLAN"** page.
- ☐ Enter the **"SSID"** field.
- ☐ Choose **"Open"** at security level from the drop-down list.
- ☐ Set the **Mac Auth** to **"ON"** status.
- ☐ Select **"Customization"** at the authentication configuration, which means you should create the **Access Policy**, **Authentication Strategy,** and **Employee Access Strategy** by yourself.
- ☐ Click **"Effect Now"** to save the WLAN and re-enter this page by editing this WLAN before continuing. Otherwise, you cannot select a SSID in next step.
- ☐ Click the **"Configuration Wizard"** button, and the wizard will show up on the right side. Based on the information in Figure 182, you need to create an **Access Policy**, an **Authentication Strategy,** and an **Employee Access Strategy** respectively. In this wizard, you will create these profiles in turn. Because of the reference relationship in the profile, you need to create an **Authentication Strategy** before saving the **Access Policy**. 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 way to operate is to create an **Employee Access Strategy** in **Authentication** → **Employee Access** → **Employee Access Strategy** 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**.

- □ First, you will see the **"Create Access Policy"** tab, and you should set a **"Name". For** current Web portal authentication, you'd better set the mapping conditions for **"SSID"** and **"Authentication Type"**. Select **"SSID"** in mapping condition's **"Attribute"** drop-down list and select the **"SSID"** that you just created in the **"Value"** drop-down list. Then, click the **"Add"** button to add the condition. Then select authentication type in mapping condition's attribute drop-down list and select **"MAC"**. Then you should select an **Authentication Strategy** or click the **"Add"** button to add a new one. See "Access policy" on page 163.
- □ 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"**. Select **"None"** as the Authentication Source, which means this **Authentication Strategy** is used for MAC authentication, and you should select a "**Guest Access Strategy"** or **"Employee Access Strategy"** or add a new one for it. Before selecting **Access Strategy**, you need to check whether to use **"Guest"** or "**Employee"**.

  See "Authentication strategy" on page 165.
- □ Third, if you select to create **"Guest Access Strategy"**, you can only use **Local Database** as the authentication source. See "Guest access strategy" on page 173. 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 choose to create **"Employee Access Strategy"**, you can select **"Local Database"**, **"External LDAP/AD"** or **"External Radius"**.
- □ Fourth, 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 the **Default Access Role Profile** in WLAN. It is the same for the default policy list. If you turn on the **"Session Timeout Status"**, then 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”** button, it means that when using external RADIUS, the RADIUS accounting interval package will be sent during the interval of the **Accounting Interim Interval**.

9 RF

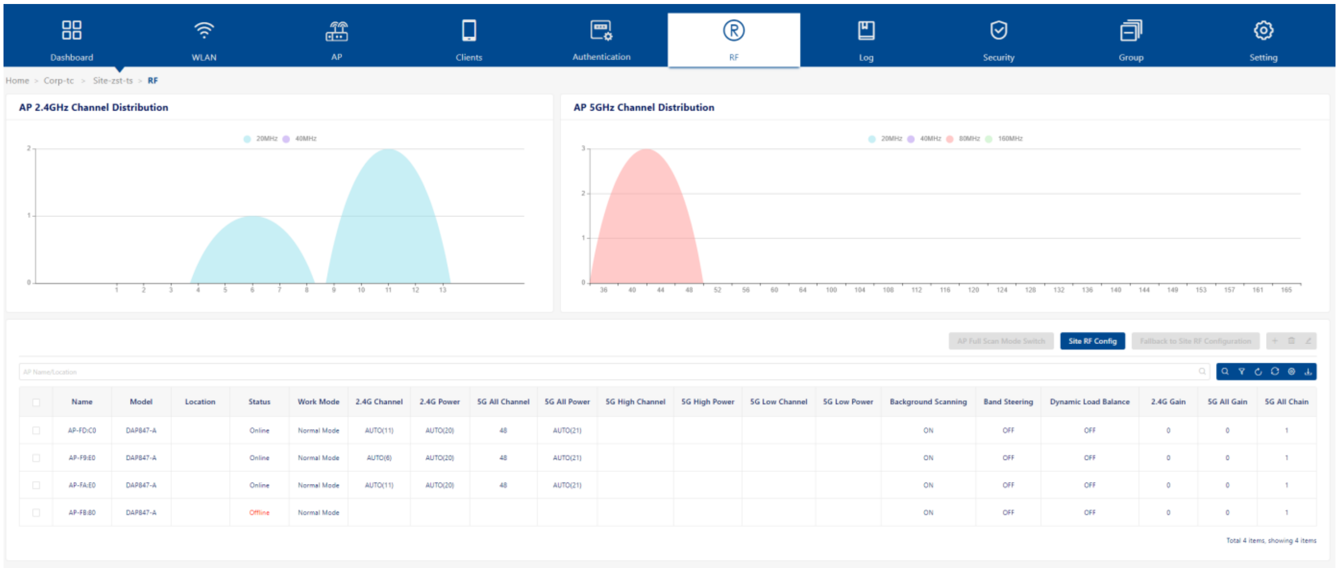
The RF management system ensures that transmit power and operating frequencies meet the requirements of global regulatory agencies and individual countries. The profiles allow users to adjust the wireless parameters and functions according to the real network environment to improve the user experience of wireless networks. You can manage the RF configuration for a specific site or DAP.

This chapter contains the following topics:

9.1 RF overview

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

Here are two charts showing the distribution of equipment channels. Place the mouse over the corresponding chart to obtain the AP number of each channel and bandwidth.



□	Name	Model	Location	Status	Work Mode	2.4G Channel	2.4G Power	5G All Channel	5G All Power	5G High Channel	5G High Power	5G Low Channel	5G Low Power	Background Scanning	Band Steering	Dynamic Load Balance	2.4G Gain	5G All Gain	5G All Chain
□	AP-FD:C0	DAP847-A		Online	Normal Mode	AUTO(11)	AUTO(20)	48	AUTO(21)					ON	OFF	OFF	0	0	1
□	AP-F9:E0	DAP847-A		Online	Normal Mode	AUTO(6)	AUTO(20)	48	AUTO(21)					ON	OFF	OFF	0	0	1
□	AP-FA:E0	DAP847-A		Online	Normal Mode	AUTO(11)	AUTO(20)	48	AUTO(21)					ON	OFF	OFF	0	0	1
□	AP-FB:80	DAP847-A		Offline	Normal Mode									ON	OFF	OFF	0	0	1

Total 4 items, showing 4 items

Figure 185: RF

Below charts are a list of detailed RF information for each AP. You can search the AP name or use the drop-down list to filter the display by AP status or AP mode.

- **Name**: AP Name
- **Model:** The model of AP
- **Location**: Location of AP
- **Status**: AP status online or offline
- **Work Mode:**
  - **Normal Mode:** AP serving wireless clients.
  - **Full Scan Mode:** In this mode, all radios under the AP will not broadcast an SSID.
- **2.4G Channel:** Channel of the 2.4G band.
  - If the configuration is auto, then it shows the actual 2.4G channel of

the AP.

- ▶ **2.4G Power:** Power of the 2.4G band.
  - If the configuration is auto, then it shows the actual 2.4G power of the AP.
- ▶ **5G All Channel:** Channel of the 5G band.
  - If the configuration is auto, then it shows the actual 5G channel of the AP.
  - The optional channels vary according to the local laws of different countries or regions.
- ▶ **5G All Power:** Power of the 5G all channel band.
  - If the configuration is auto, then it shows the actual 5G power of the AP.
- ▶ **5G High Channel:** Channel of the 5G high.
  - If the configuration is Auto, it shows the actual 5G High channel of the AP.
- ▶ **5G High Power:** Power of the 5G high channel.
  - If the configuration is auto, it shows the actual 5G high power of the AP.
- ▶ **5G Low Channel:** Channel of the 5G low.
  - If the configuration is auto, it shows the actual 5G low channel of the AP.
- ▶ **5G Low Power:** Power of the 5G low channel.
  - If the configuration is auto, it shows actual 5G low power of the AP.
- ▶ **Background Scanning:**
  - Enable or disable 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 and WIPS.
  - If you want to utilize these advanced functions, then verify that **"Background Scanning"** is enabled. By default, it is enabled.
- ▶ **Band Steering:** Band steering status. It is enabled by default.
  - Band steering controls the behavior of dual-band clients according to the utilization of a wireless channel and the number of users

connected to the AP.

  - It guides a client accessing the network to the optimal 5 GHz band or another AP.

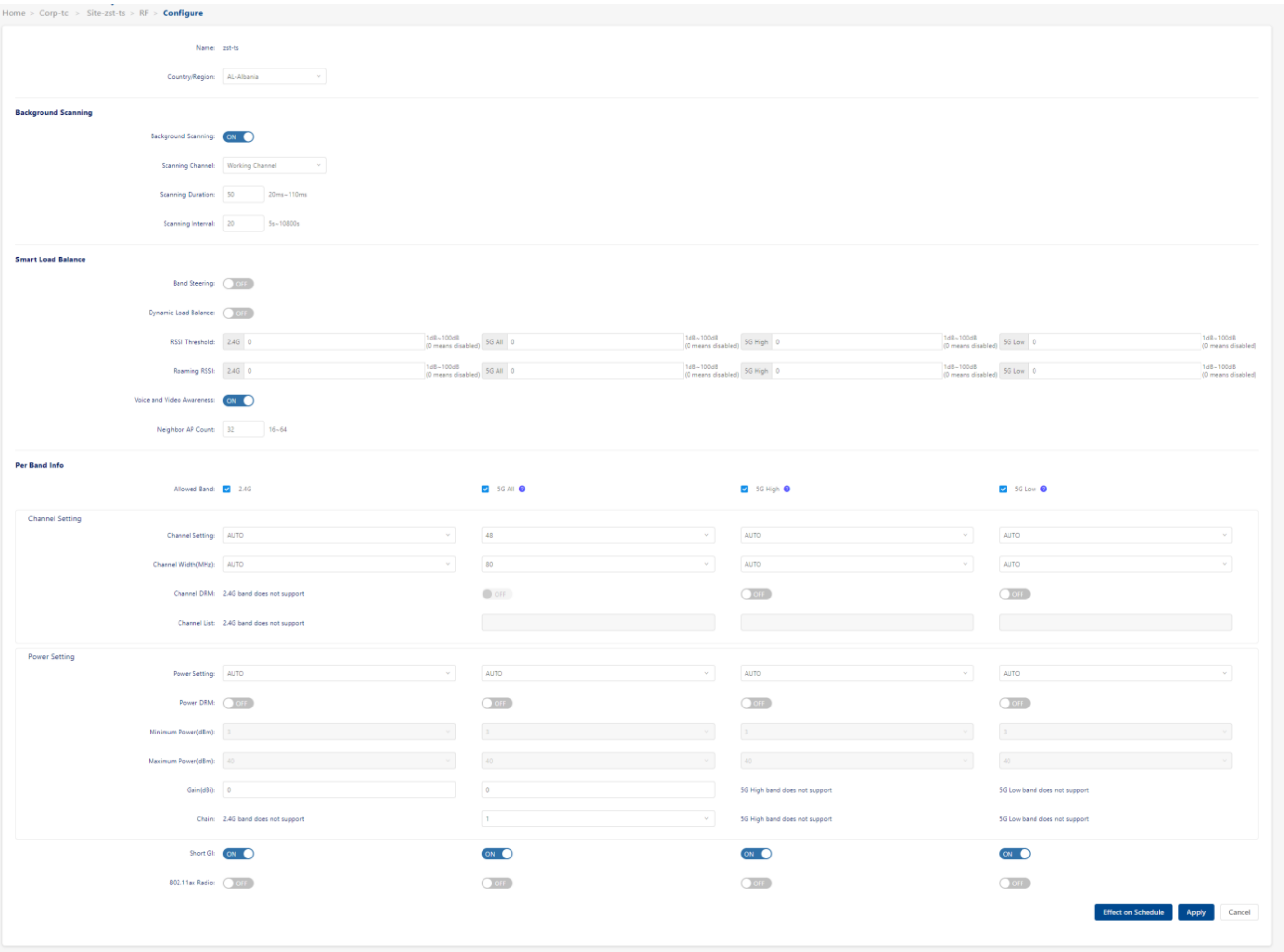
- **Dynamic Load Balance:** It is disabled by default.

  - Enable or disable clients load balance to provide fair distribution of clients among neighboring APs based on the client density, channel utilization on adjacent APs, and associating clients RSSI value.
  - Client information such as client numbers, is synchronized in the wireless network so that an AP can know the load of its neighbor AP and decide whether to permit client access.

- **2.4G Gain:** The antenna gain of AP for 2.4G band, only for DAP847-A.
- **5G All Gain:** The antenna gain of AP for 5G All band, only for DAP847-A.
- **5G All Chain:** The antenna chain of AP for 5G All band, only for DAP847-A.

9.2 Set RF configurations of Site

Click the **“Site RF Config”** button to enter the RF edit view.



Name: zst-ts

Country/Region: AL-Albania

Background Scanning

Background Scanning: ON

Scanning Channel: Working Channel

Scanning Duration: 50 20ms~110ms

Scanning Interval: 20 5s~10800s

Smart Load Balance

Band Steering: OFF

Dynamic Load Balance: OFF

RSSI Threshold: 2.4G 0 1dB~100dB (0 means disabled) 5G All 0 1dB~100dB (0 means disabled) 5G High 0 1dB~100dB (0 means disabled) 5G Low 0 1dB~100dB (0 means disabled)

Roaming RSSI: 2.4G 0 1dB~100dB (0 means disabled) 5G All 0 1dB~100dB (0 means disabled) 5G High 0 1dB~100dB (0 means disabled) 5G Low 0 1dB~100dB (0 means disabled)

Voice and Video Awareness: ON

Neighbor AP Count: 32 16~64

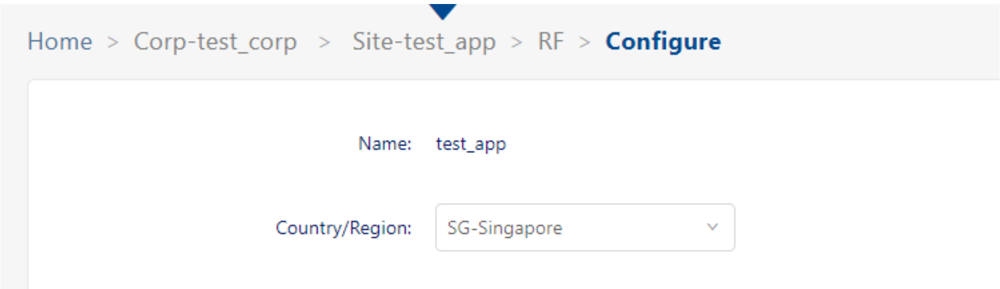
Per Band Info

Allowed Band:	☑ 2.4G	☑ 5G All	☑ 5G High	☑ 5G Low
Channel Setting				
Channel Setting:	AUTO	48	AUTO	AUTO
Channel Width(MHz):	AUTO	80	AUTO	AUTO
Channel DRM:	2.4G band does not support	OFF	OFF	OFF
Channel List:	2.4G band does not support			
Power Setting				
Power Setting:	AUTO	AUTO	AUTO	AUTO
Power DRM:	OFF	OFF	OFF	OFF
Minimum Power(dBm):	3	3	3	3
Maximum Power(dBm):	40	40	40	40
Gain(dBi):	0	0	5G High band does not support	5G Low band does not support
Chain:	2.4G band does not support	1	5G High band does not support	5G Low band does not support
Short GI:	ON	ON	ON	ON
802.11ax Radio:	OFF	OFF	OFF	OFF

Figure 186: RF Configuration

9.2.1 General information

- **Name:** Inherit from site name
- **Country/Region:**
  - A country or region is a short alphabetic geographical code that represents a country or dependent area which is used in data processing and communications.
  - The wireless transmitting power and operating frequencies (channels) vary by country or region.
  - Select the country or region where the APs are located.


Home > Corp-test_corp > Site-test_app > RF > Configure

Name: test_app

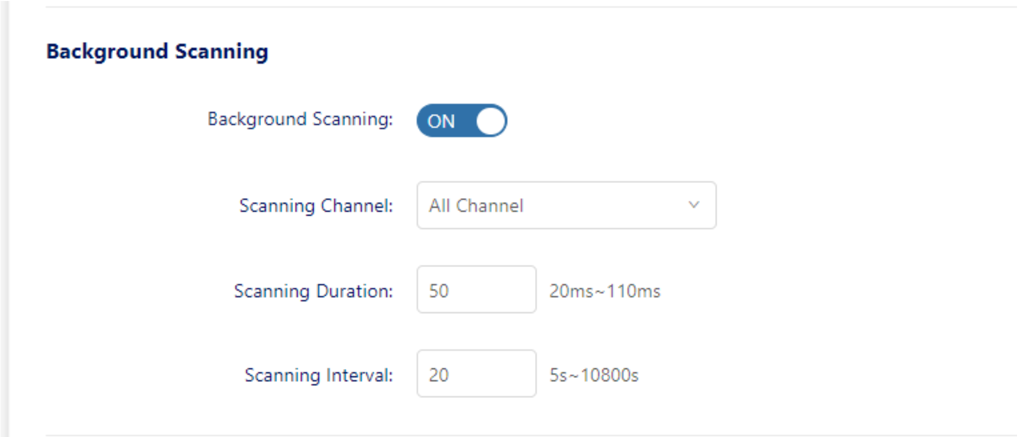
Country/Region: SG-Singapore

Figure 187: Configure Site RF - General information

9.2.2 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 and RDA (ACS/APC). If you want to utilize these advanced functions, then verify that **"Background Scanning"** is enabled. By default, it is enabled.

- **Background Scanning:** Enable or disable background scanning.
- **Scanning Channel**:
  - **Working Channel:** AP scans the working channel.
  - **All Channel:** AP scans all channels.
- **Scanning Duration:** The background scanning duration is given in milliseconds. (Default value: 50)
- **Scanning Interval:** The background scanning interval, in seconds. (Default value: 20)


Background Scanning

Background Scanning: ON

Scanning Channel: All Channel

Scanning Duration: 50 20ms~110ms

Scanning Interval: 20 5s~10800s

Figure 188: Configure Site RF - Background scanning

9.2.3 Smart load balance

The Smart Load Balance (SLB) feature improves the user experience when accessing wireless connectivity. It guides a user's client device to connect to a free wireless channel or AP and denies access to APs with weak signals.

Smart load balance includes:

- **Band Steering:** Enable or disable band steering.

  Band steering controls the behavior of dual-band clients according to the utilization of a wireless channel and the number of users connected to the AP. It guides a client accessing the network to the optimal AP.
- **Dynamic Load Balance:** Enable or disable client load balancing among APs in a group or groups in the same wireless network.

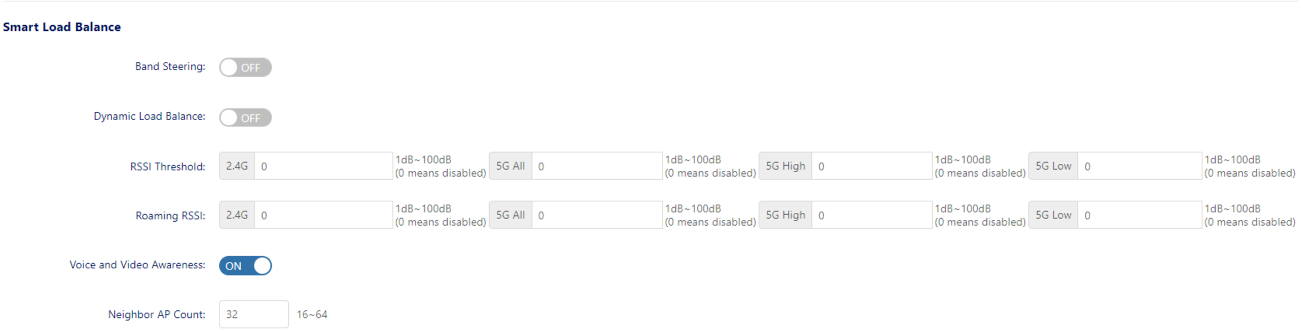
  Client information, such as client numbers, is synchronized in the wireless network so that an AP can determine the load of its neighbor AP and decide whether to permit client access.
- **RSSI Threshold:** Associate RSSI Threshold**.** It is used to set thresholds to optimize connectivity when associating with an AP by forbidding client access to networks with a weak wireless signal (RSSI). Clients with an RSSI value lower than the Association RSSI Threshold are not allowed to connect to the AP.

  By default, the **“RSSI threshold”** is disabled (0). The RSSI threshold can be applied to the 2.4G band or 5G band separately. Recommend values are 2.4G (5), 5G (10). RSSI threshold is recommended to be set in a high density scenario.
- **Roaming RSSI:** Roaming RSSI Threshold**.**

  It is 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 the 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 which AP to roam to when the threshold is breached. When 802.11k and 802.11v are enabled, The recommend values are 2.4G (10), 5G (15).

- **Voice and Video Awareness:** Enable or disable voice and video awareness. It is enabled by default. Background scanning must be aware of existing traffic on APs.

  If there is an ongoing voice or video service, scanning should not be performed to ensure uninterrupted traffic, and scanning should resume that there is no active voice or video session.
- **Neighbor AP Count:** This is used to limit the number of neighbor APs that an AP can connect to. (Default value: 32)



Smart Load Balance

Band Steering: OFF

Dynamic Load Balance: OFF

RSSI Threshold: 2.4G 0 1dB~100dB (0 means disabled) 5G All 0 1dB~100dB (0 means disabled) 5G High 0 1dB~100dB (0 means disabled) 5G Low 0 1dB~100dB (0 means disabled)

Roaming RSSI: 2.4G 0 1dB~100dB (0 means disabled) 5G All 0 1dB~100dB (0 means disabled) 5G High 0 1dB~100dB (0 means disabled) 5G Low 0 1dB~100dB (0 means disabled)

Voice and Video Awareness: ON

Neighbor AP Count: 32 16~64

Figure 189: Configure Site RF - Smart Load Balance

9.2.4 Per band info

Configure the wireless settings 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:** Activate the 2.4G band radio.
  - **5G All:** Activate the 5G band radio. Only for dual-radio devices.
  - **5G High:** Activate the 5.2G band radio. Only for three-radio devices.
  - **5G Low:** Activate the 5.8G band radio. Only for three-radio devices.
- **Channel Setting:** Configure the working channel of the radio.
  - **Auto:** Dynamically assign the working channel by ACS (Auto Channel Selection).
  - **Number:** Manually specify the channel (allowed channels vary by country or region).
- **Channel Width(MHz):** Configure the channel width for 2.4G 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, a 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:** 20 MHz or 40 MHz
- **5G All/5G High/5G Low:** 20 MHz, 40 MHz, 80 MHz, or 160 MHz. The value displayed in the list depends on the **Channel Setting**. Some high-frequency channels do not support 160 MHz. For example, 160 MHz is only supported on channel settings 36 through 128.

▶ **Channel DRM:** Specify the channel scope for DRM. In some regions, specific unwanted channels can be scoped out automatically in channel selection to avoid conflicts or law violations. Unsupported only on the 2.4G Band.

▶ **Channel List:** Specify the available channels that can be selected by DRM. Unsupported only on the 2.4G Band.

▶ **Power Setting:** Configure the transmit power of the wireless radio. The power range varies for different radios.

- **Auto:** Dynamically assigned the transmit power by APC (Auto Power Control).
- **Number:** Manually specify the power setting (3 dBm - 40 dBm).

▶ **Power DRM**: Specify the power range for DRM. Disabled by default. If enabled, then you can select the Minimum Power and Maximum Power.

▶ **Minimum Power**: Specify the minimum transmit power for the Power DRM setting. This can prevent the AP from selecting a low transmit power, resulting in poor quality transmission.

▶ **Maximum Power:** Specify the maximum transmit power for the power DRM setting.

▶ **Gain:** Antenna Gain can be set for 2.4G or 5G All band separately, range: 0-16 dBi.

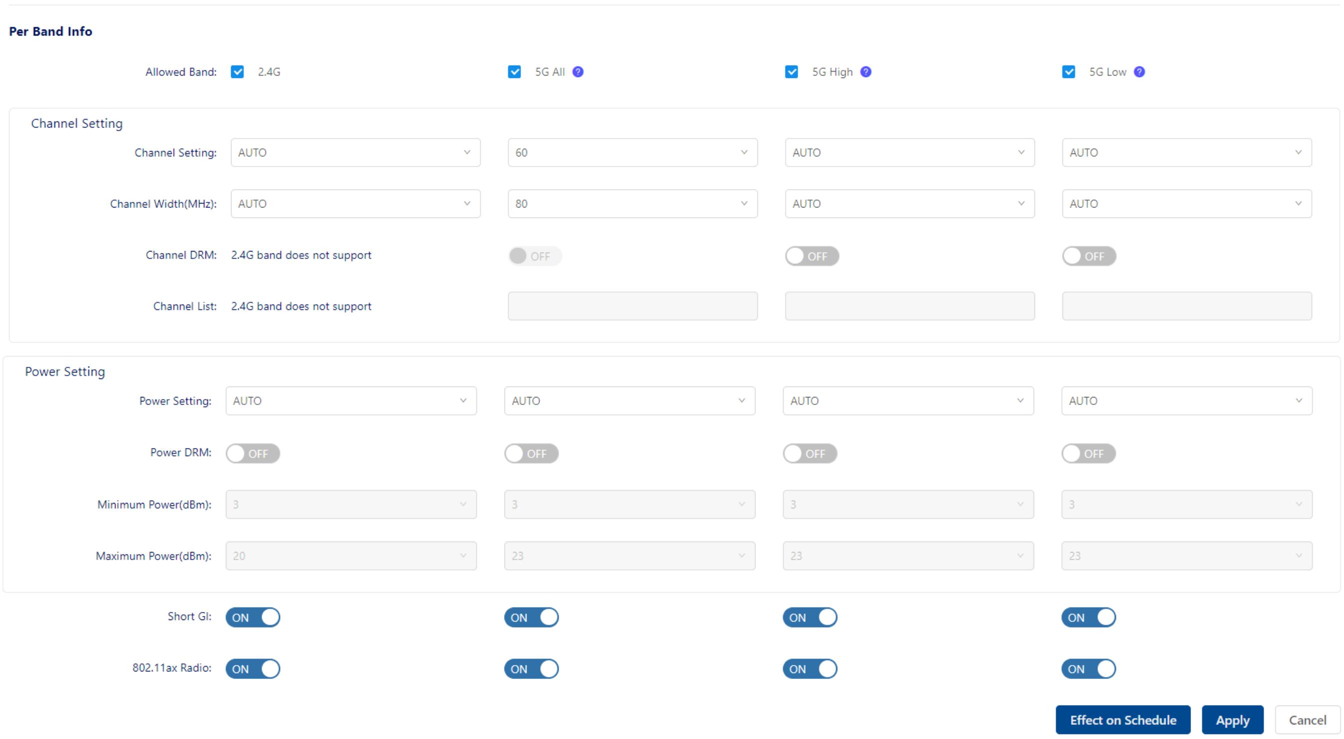
- **Chain:** Antenna Chain, only for 5G, represents the antenna interface corresponding to MIMO. the values of antenna chain can be as follows:

Bandwidth	MIMO	Chain
20/40/80	1x1	0
		1
		2
		3
	2x2	0+1
		0+3
	3x3	0+1+2
	4x4	0+1+2+3

Table 7: Antenna Chain & MIMO table for DAP847-A

- **Short GI:** Enable or disable short guard interval.

  In IEEE 802.11 OFDM based communications, the guard interval is used to verify that distinct transmissions are occurred between the successive data symbols which is 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 detection 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 GI"** is disabled on the wireless radio.
- **802.11ax Radio:** Enable or disable 802.11ax (Wi-Fi6) features. Enabled by default. If disabled, the AP can work on 802.11ac or earlier protocols.



Per Band Info

Allowed Band:	☑ 2.4G	☑ 5G All	☑ 5G High	☑ 5G Low
Channel Setting				
Channel Setting:	AUTO	60	AUTO	AUTO
Channel Width(MHz):	AUTO	80	AUTO	AUTO
Channel DRM:	2.4G band does not support	OFF	OFF	OFF
Channel List:	2.4G band does not support			
Power Setting				
Power Setting:	AUTO	AUTO	AUTO	AUTO
Power DRM:	OFF	OFF	OFF	OFF
Minimum Power(dBm):	3	3	3	3
Maximum Power(dBm):	20	23	23	23
Short GI:	ON	ON	ON	ON
802.11ax Radio:	ON	ON	ON	ON

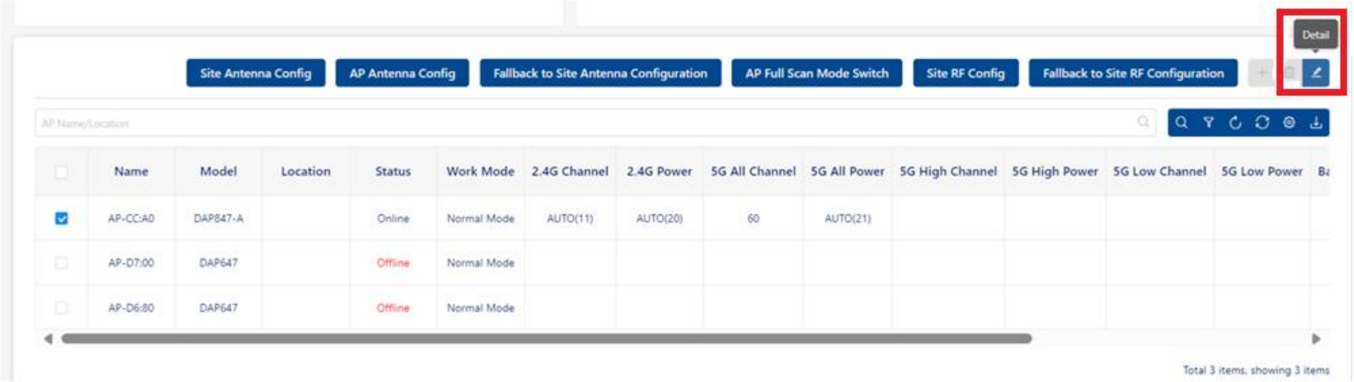
Figure 190: Per band info

9.3 Set RF configurations for a selected DAP

Sometimes, you need to adjust the RF configurations of a selected AP to give users a better experience. Before setting RF configurations for a certain AP, you must set the RF configurations of the corresponding Site first. The RF configurations of the AP have a higher priority than the RF configurations of the Site.

9.3.1 Single AP RF configuration

- ☐ Select a single AP.
- ☐ Click the " ✎ " icon to enter the AP details page.

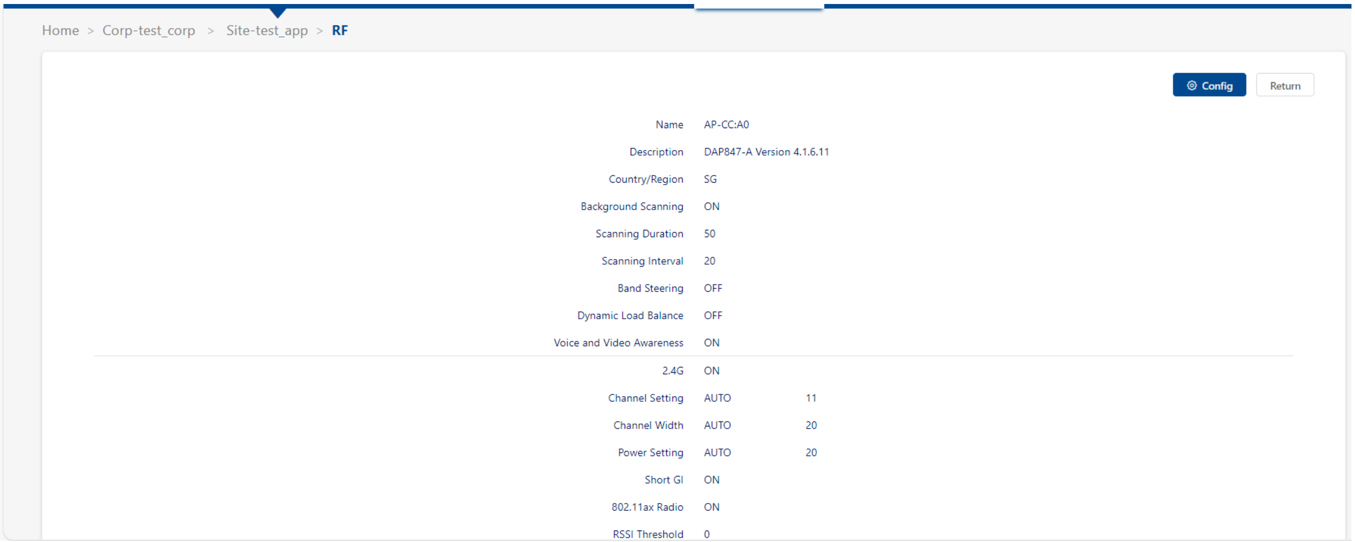


☐	Name	Model	Location	Status	Work Mode	2.4G Channel	2.4G Power	5G All Channel	5G All Power	5G High Channel	5G High Power	5G Low Channel	5G Low Power	Ba
☑	AP-CC:A0	DAP847-A		Online	Normal Mode	AUTO(11)	AUTO(20)	60	AUTO(21)					
☐	AP-D7:00	DAP647		Offline	Normal Mode									
☐	AP-D6:80	DAP647		Offline	Normal Mode									

Total 3 items, showing 3 items

Figure 191: Detail icon

- ☐ Click the **"Config"** button to set the RF configuration of the selected AP.



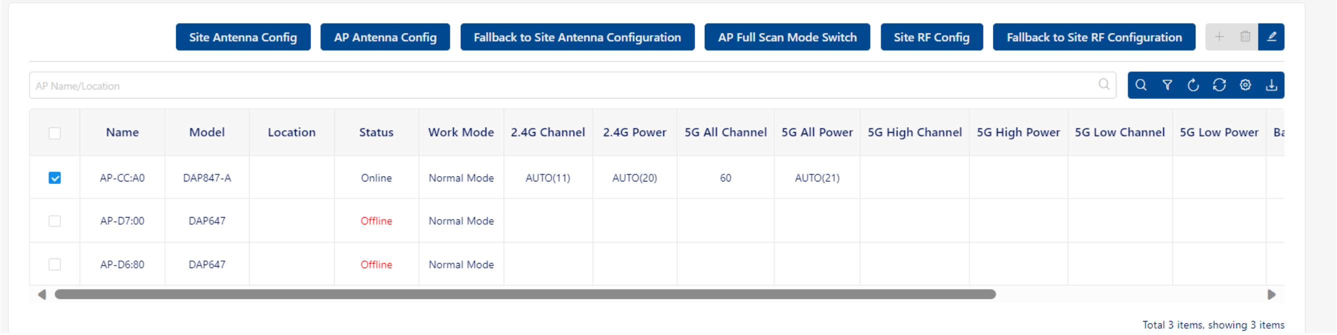
Name	AP-CC:A0	
Description	DAP847-A Version 4.1.6.11	
Country/Region	SG	
Background Scanning	ON	
Scanning Duration	50	
Scanning Interval	20	
Band Steering	OFF	
Dynamic Load Balance	OFF	
Voice and Video Awareness	ON	
2.4G	ON	
Channel Setting	AUTO	11
Channel Width	AUTO	20
Power Setting	AUTO	20
Short GI	ON	
802.11ax Radio	ON	
RSSI Threshold	0	

Figure 192: RF configuration

9.3.2 Fallback to Site RF configuration

- ☐ Select a single or multiple APs.
- ☐ Click the **“Fallback to Site RF Configuration”** button.

The RF configuration of the selected APs will be cleared, and the RF configuration of the selected APs will be consistent with the Site.



☐	Name	Model	Location	Status	Work Mode	2.4G Channel	2.4G Power	5G All Channel	5G All Power	5G High Channel	5G High Power	5G Low Channel	5G Low Power	Ba
☑	AP-CC:A0	DAP847-A		Online	Normal Mode	AUTO(11)	AUTO(20)	60	AUTO(21)					
☐	AP-D7:00	DAP647		Offline	Normal Mode									
☐	AP-D6:80	DAP647		Offline	Normal Mode									

Total 3 items, showing 3 items

Figure 193: Fallback to Site RF configuration

9.3.3 AP full scan mode

- ☐ Select single or multiple APs.
- ☐ Click the **“AP Full Scan Mode Switch”** button, and the selected AP will enter **“full scan mode”**. In this mode, all radios under the AP will not broadcast an SSID.

Note: Enabling **“AP Full Scan Mode”** will cause the AP to close the currently working WLAN. All terminals associated with the AP will be offline.

10 Log

Log contains 2 major parts:

- System log
- Device log

The system log contains the key events of the device and the operation log of the DAC. The platform collects the log files 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 and locate problems in time.

This chapter contains the following topics:

- System log
- Device log

10.1 System log

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

10.1.1 Log list

The list shows recent logs. You can filter logs by log type, log level, or AP Group.

- **Severity:** Severity of log. It can be an Emergency, Alert, Critical, Error, Warning, Notice, Informational or Debug.
  - **Emergency:** The system is unusable.
  - **Alert:** Action must be taken immediately.
  - **Critical:** A critical condition.
  - **Error:** An error condition.
  - **Warning:** Indicates 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.
  - **Debug:** The messages that aid developers in identifying issues.

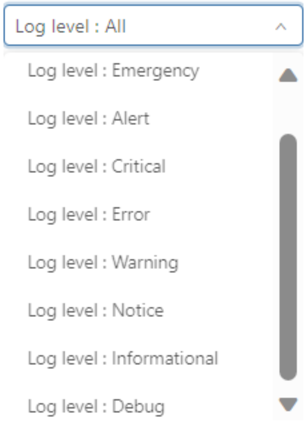


Figure 194: Severity

- **Type:** Log type. It can be Trap-Hardware, Trap-Upgrade, Trap-Security, Trap-Network, Trap Authentication, Switch Trap-Network, or Operator.
  - **Trap-Hardware:** Hardware reporting information. It mainly focuses on

the CPU, RAM, and flash performance of the AP, and it monitors the hot and cold start behaviors of the AP.

- **Trap-Upgrade:** Firmware upgrade information, mainly include AP upgrade behaviors.
- **Trap-Security:** Wireless security information that mainly includes the operation information of the Blocklist.
- **Trap-Network:** Network related reporting information that mainly includes the creation and deletion of layer-2 VLANs.
- **Trap-Authentication:** Authentication information of the clients' authentication behavior and link status information from the AP to the RADIUS server.
- **Switch Trap-Network:** The reported information about the switch network.
- **Operator:** User operation record information for that DAC. Record the operation of DAC with the combination of operator and operation actions.

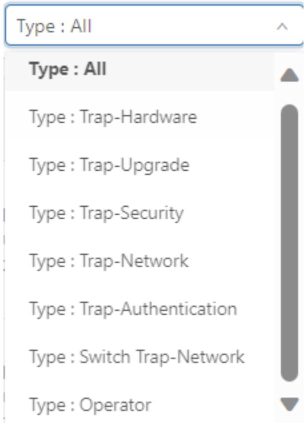
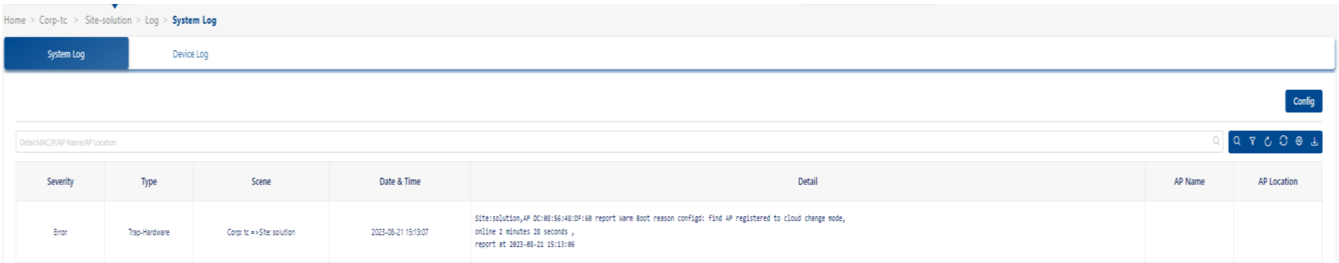


Figure 195: Type

- **Scene:** The log occurs at which Corporate, Site, or Group.
- **Date & Time:** The log occurs currently.
- **Detail:** The detailed information of the log.
- **AP Name:** If the log is produced by an AP, then this field shows the Name of the AP.
- **AP Location:** If the log is produced by an AP, then this field shows the Location of the AP.

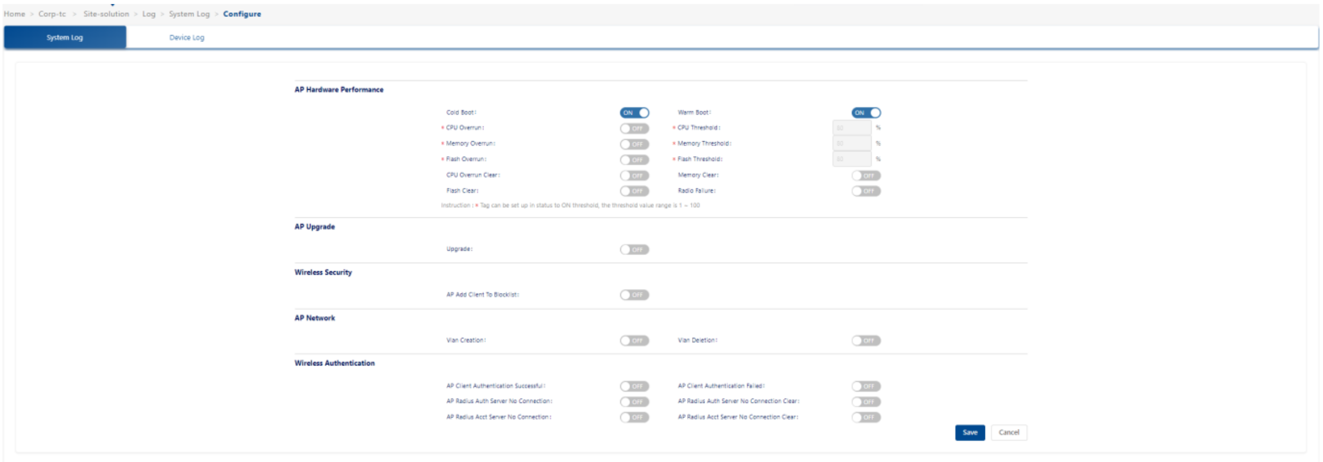

Home > Corp-tc > Site-solution > Log > System Log
System Log
Device Log
Config
Detail:MAC,IP/AP Name/AP Location

Severity	Type	Scene	Date & Time	Detail	AP Name	AP Location
Error	Trap-Hardware	Corp: tc =>Site: solution	2023-08-21 15:13:07	Site:solution,AP DC:08:56:48:DF:60 report Warm Boot reason configd: find AP registered to cloud change mode, online 2 minutes 28 seconds , report at 2023-08-21 15:13:06		

Figure 196: Log list

10.1.2 Config of AP event log

Click the **"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 with which you are concerned on this page.


Home > Corp-tc > Site-solution > Log > System Log > Configure
System Log
Device Log

AP Hardware Performance

Cold Boot:	ON	Warm Boot:	ON
* CPU Overrun:	OFF	* CPU Threshold:	80 %
* Memory Overrun:	OFF	* Memory Threshold:	80 %
* Flash Overrun:	OFF	* Flash Threshold:	80 %
CPU Overrun Clear:	OFF	Memory Clear:	OFF
Flash Clear:	OFF	Radio Failure:	OFF

Instruction : * Tag can be set up in status to ON threshold, the threshold value range is 1 ~ 100

AP Upgrade

Upgrade: OFF

Wireless Security

AP Add Client To Blocklist: OFF

AP Network

Vlan Creation: OFF — Vlan Deletion: OFF

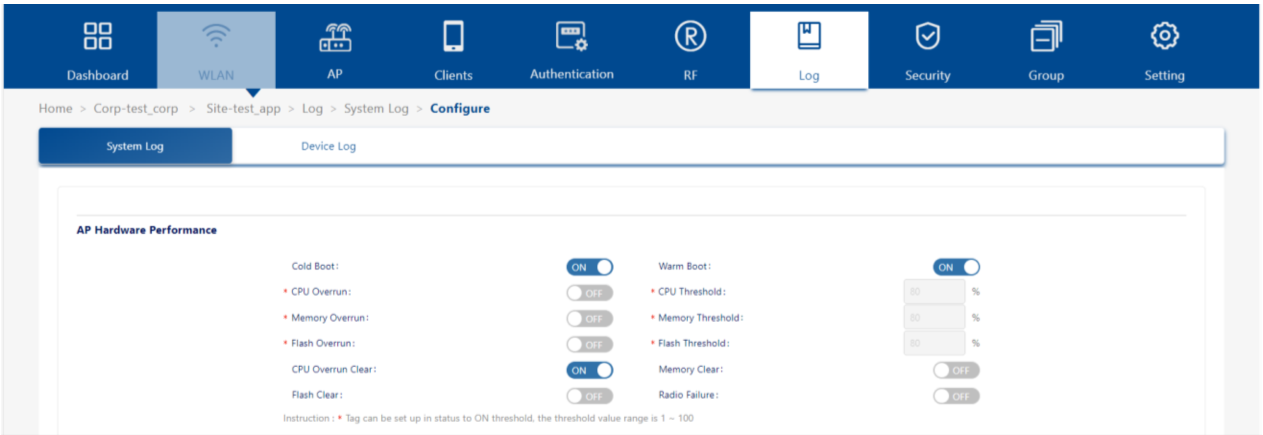
Wireless Authentication

AP Client Authentication Successful:	OFF	AP Client Authentication Failed:	OFF
AP Radius Auth Server No Connection:	OFF	AP Radius Auth Server No Connection Clear:	OFF
AP Radius Acct Server No Connection:	OFF	AP Radius Acct Server No Connection Clear:	OFF

Figure 197: Log configuration

- **AP hardware performance**
  - **Cold Boot:** Cold boot is the process of starting an AP from shutdown or a powerless state and setting it to a 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 an AP. It may be used in contrast to a cold boot.
  - **CPU Overrun:** This log occurs when the AP CPU load exceeds the CPU threshold.
  - **CPU Threshold:** When AP CPU usage exceeds this percent, an AP CPU Overrun Log will occur.
  - **Memory Overrun:** It occurs when the AP RAM memory usage exceeds the MEM threshold.

- ▶ **Memory Threshold:** When AP memory usage exceeds this percent, an AP MEM Overrun log occurs.
- ▶ **Flash Overrun:** It occurs when the AP Flash memory usage exceeds the Flash threshold.
- ▶ **Flash Threshold:** When AP Flash memory usage exceeds this percent, an AP Flash overrun log occurs.
- ▶ **CPU Overrun Clear:** When the CPU utilization of the AP decreases from exceeding the threshold to the normal state.
- ▶ **Memory Clear:** When the RAM memory utilization of the AP decreases from exceeding the threshold to the normal state.
- ▶ **Flash Clear:** When the Flush memory utilization of the AP decreases from exceeding the threshold to the normal state.
- ▶ **Radio Failure:** When the Wi-Fi fails to load. For example, the 2G chip of the AP is broken and leads to Wi-Fi release failure.



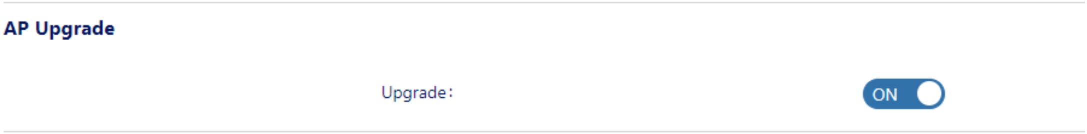
AP Hardware Performance

Cold Boot:	ON	Warm Boot:	ON
* CPU Overrun:	OFF	* CPU Threshold:	80 %
* Memory Overrun:	OFF	* Memory Threshold:	80 %
* Flash Overrun:	OFF	* Flash Threshold:	80 %
CPU Overrun Clear:	ON	Memory Clear:	OFF
Flash Clear:	OFF	Radio Failure:	OFF

Instruction : * Tag can be set up in status to ON threshold, the threshold value range is 1 ~ 100

Figure 198: AP hardware performance

- ■ **AP upgrade**
  - ▶ **Upgrade:** Logs of the AP Upgrade.



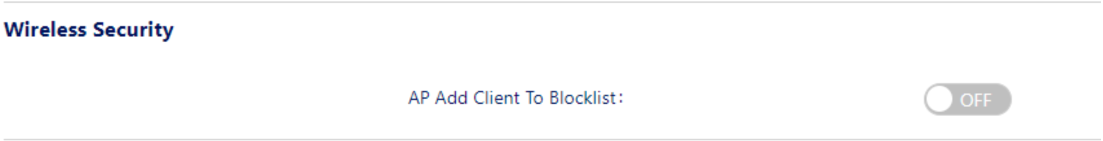
AP Upgrade

Upgrade: ON

Figure 199: AP Upgrade

- ■ **Wireless security**
  - ▶ **AP Add Client to Blocklist:** The Log of a client is added to the

blocklist by the WIPS policy, either dynamically or manually.

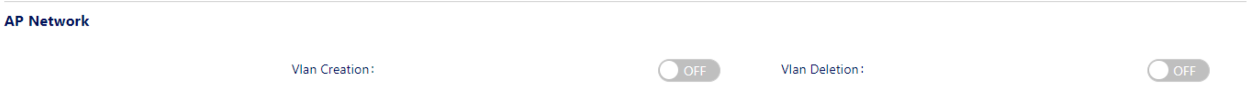


Wireless Security

AP Add Client To Blocklist: OFF

Figure 200: Wireless Security

- **AP network**
  - **Vlan Creation:** AP VLAN Creation Log
  - **Vlan Deletion:** AP VLAN Deletion Log



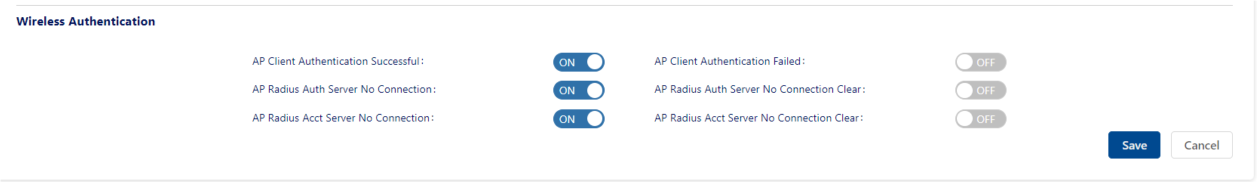
AP Network

Vlan Creation: OFF

Vlan Deletion: OFF

Figure 201: AP Network

- **Wireless authentication**
  - **AP Client Authentication Successful:** The Log of client authenticating successfully.
  - **AP Client Authentication Failed:** The Log of client authentication failed.
  - **AP Radius Auth Server No Connection:** Log of authentication server unreachable.
  - **AP Radius Auth Server No Connection Clear:** Log of authentication server recovered 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.



Wireless Authentication

AP Client Authentication Successful: ON

AP Client Authentication Failed: OFF

AP Radius Auth Server No Connection: ON

AP Radius Auth Server No Connection Clear: OFF

AP Radius Acct Server No Connection: ON

AP Radius Acct Server No Connection Clear: OFF

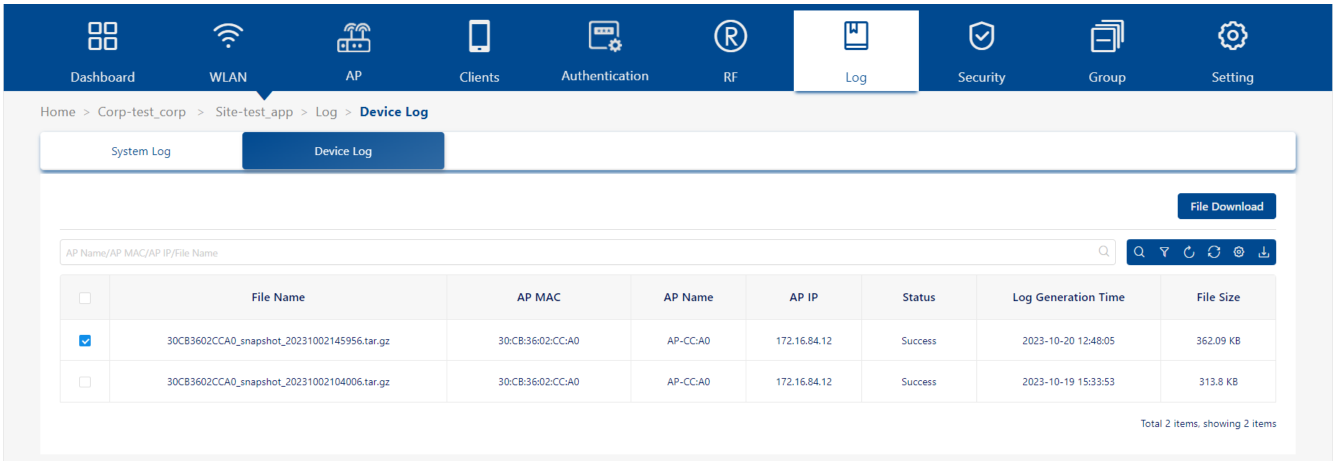
Figure 202: Wireless Authentication

10.2 Device log

After the AP restarts abnormally, it reconnects to the DAC platform. The platform will collect the log files from 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 was generated at this time.
- **File Size:** The file size of this log file.

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



□	File Name	AP MAC	AP Name	AP IP	Status	Log Generation Time	File Size
☑	30CB3602CCA0_snapshot_20231002145956.tar.gz	30:CB:36:02:CC:A0	AP-CC:A0	172.16.84.12	Success	2023-10-20 12:48:05	362.09 KB
□	30CB3602CCA0_snapshot_20231002104006.tar.gz	30:CB:36:02:CC:A0	AP-CC:A0	172.16.84.12	Success	2023-10-19 15:33:53	313.8 KB

Total 2 items, showing 2 items

Figure 203: Device log

11 Security

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

■ WIDS

DAC provides a comprehensive security function to ensure customer wireless cybersecurity. The system identifies rogue APs by following policies and criteria.

- ▶ To detect when APs' signal strength threshold exceeds the value defined by the administrator.
- ▶ To detect if an AP's SSID name is valid according to the system definition.
- ▶ To detect by defined keywords (defined by the administrator) within the SSID name of APs.
- ▶ To detect APs by their defined OUI (Organizational Unique Identifier within the first six digits of the MAC address), refer to the Blacklist mechanism.
- ▶ To detect a defined legal OUI, refer to the Whitelist mechanism. DAC can also detect the 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 disassociation.
  - **Clients:** Valid Client mis-association, Omerta Attack, Unencrypted Valid Clients, 802.11 40 MHz 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

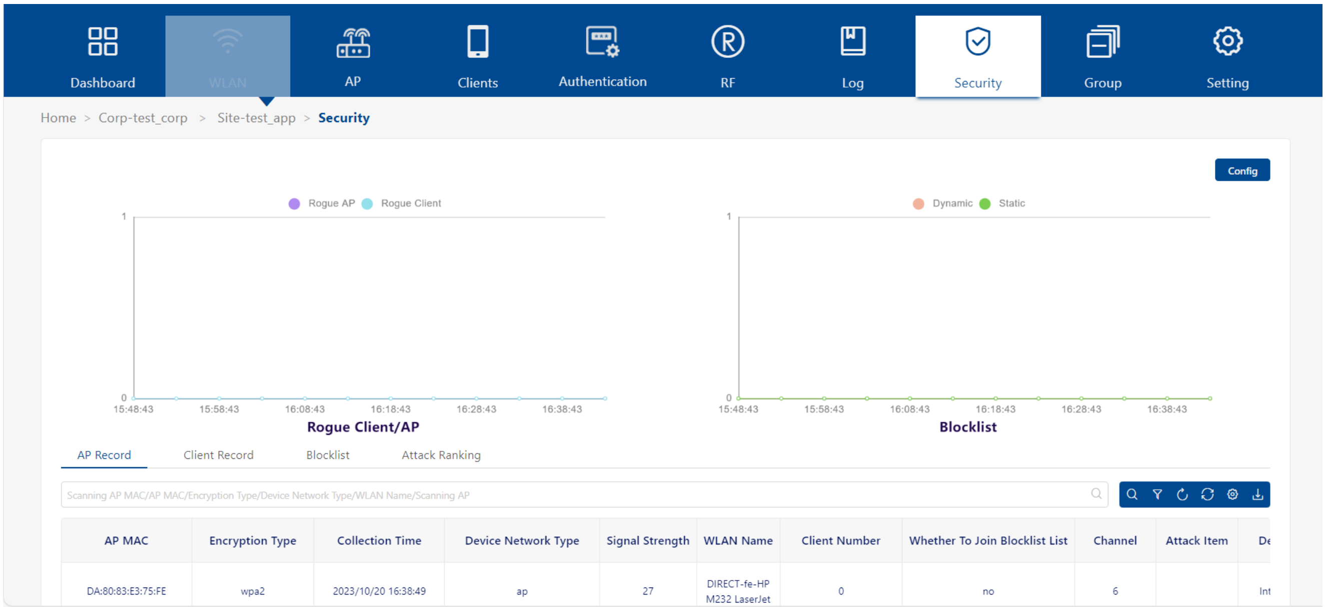
- **WIPS**

In cooperation 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 or passive) to mitigate negative effects by blacklist mechanisms (static or dynamic).
- Security policy to protect legal equipment by providing a whitelist mechanism.

The home page provides 2 charts as shown in Figure 204 to help you understand the current overall situation.

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



AP MAC	Encryption Type	Collection Time	Device Network Type	Signal Strength	WLAN Name	Client Number	Whether To Join Blocklist List	Channel	Attack Item	De
DA:80:83:E3:75:FE	wpa2	2023/10/20 16:38:49	ap	27	DIRECT-fe-HP M232 LaserJet	0	no	6		Int

Figure 204: Security Dashboard

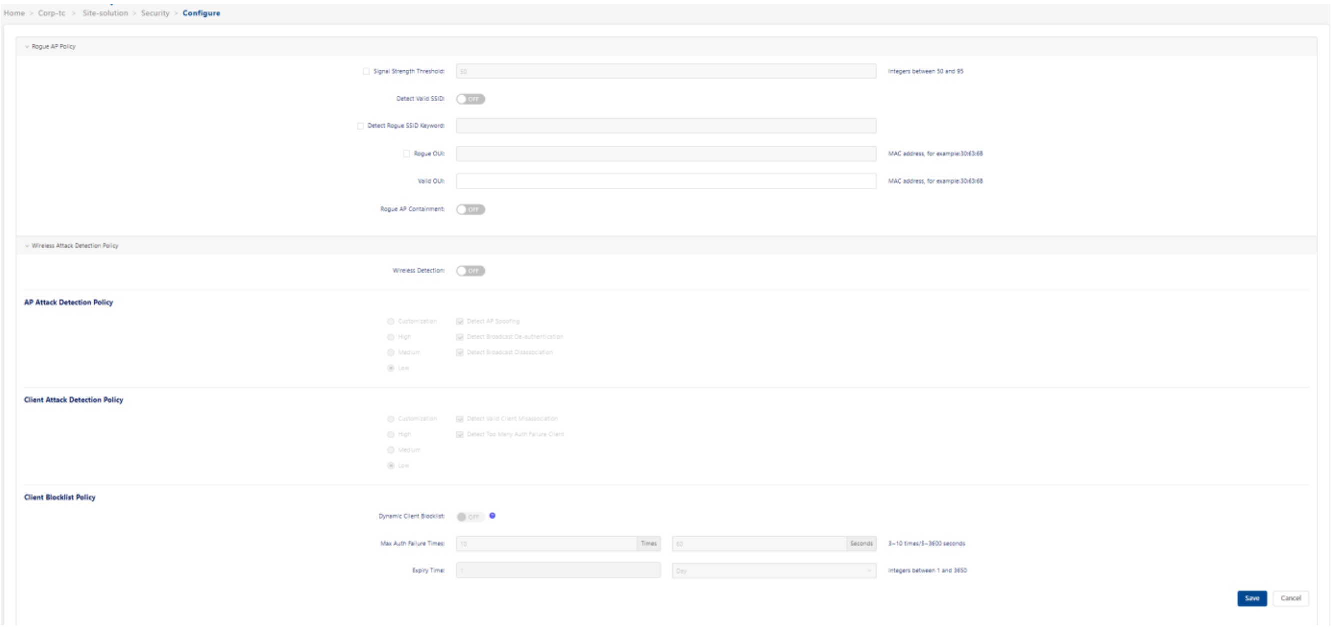
This chapter contains the following topics:

- ▶ Security config
- ▶ AP record
- ▶ Client record
- ▶ Blocklist
- ▶ Attack ranking

11.1 Security config

The Security Config Screen is used to configure policies for Rogue APs 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 the **“Config”** button.
- ☐ Edit the policy as described below.
- ☐ Click the **“Save”** button to activate the policy for the Site wireless network.



Rogue AP Policy

☐ Signal Strength Threshold: 50 Integers between 50 and 95
Detect Valid SSID: OFF
☐ Detect Rogue SSID Keyword:
☐ Rogue OUI: MAC address, for example:30:63:68
Valid OUI: MAC address, for example:30:63:68
Rogue AP Containment: OFF

Wireless Attack Detection Policy

Wireless Detection: OFF

AP Attack Detection Policy

○ Customization ☑ Detect AP Spoofing
○ High ☑ Detect Broadcast De-authentication
○ Medium ☑ Detect Broadcast Disassociation
● Low

Client Attack Detection Policy

○ Customization ☑ Detect Valid Client Misassociation
○ High ☑ Detect Too Many Auth Failure Client
○ Medium
● Low

Client Blocklist Policy

Dynamic Client Blocklist: OFF
Max Auth Failure Times: 10 Times 60 Seconds 3~10 times/5~3600 seconds
Expiry Time: 1 Day Integers between 1 and 3650

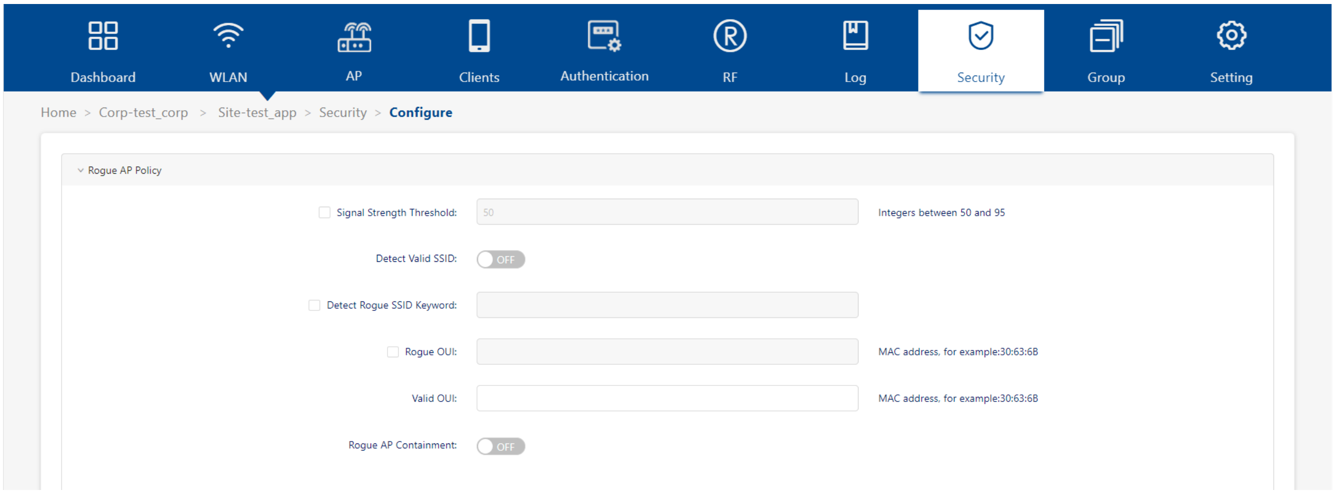
Figure 205: Security Config

11.1.1 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 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, then an interfering AP with a greater RSSI than the setting value will be classified as Rogue AP (Possible values: 50..95). By default, the RSSI matching rule is disabled.

- **Detect Valid SSID:** If enabled, another AP broadcasting the same SSID with valid DAC network SSIDs will be classified as Rogue AP. The Detected Valid SSID rule is disabled by default.
- **Detect Rogue SSID Keyword:** If enabled, an interfering AP broadcasting an SSID that matches the characteristic specified by the user will be classified as Rogue AP. The matching condition can be equal to or contain the SSID of the configured keyword.
- **Rogue OUI:** If enabled, interfering APs matching this MAC OUI will be classified as Rogue AP.
- **Valid OUI:** An AP classified as interfering or Rogue AP 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 not be classified as Rogue AP.
- **Rogue AP Containment:** It is disabled by default. If the Rogue AP Containment is disabled, the impact of the Rogue AP on valid clients reduces.



Home > Corp-test_corp > Site-test_app > Security > **Configure**

Rogue AP Policy

□ Signal Strength Threshold: 50 Integers between 50 and 95

Detect Valid SSID: OFF

□ Detect Rogue SSID Keyword:

□ Rogue OUI: MAC address, for example:30:63:6B

Valid OUI: MAC address, for example:30:63:6B

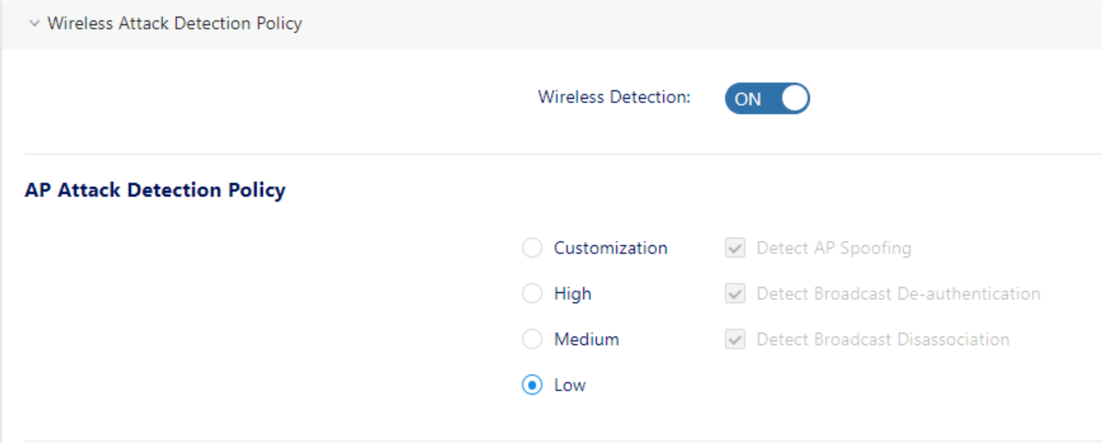
Rogue AP Containment: OFF

Figure 206: Rogue AP Policy

11.1.2 Wireless attack detection policy

A Rogue AP is not the only threat to the wireless network. It can detect other wireless attacks and mitigate them for both APs and Clients. You must enable **Wireless Detection** to create Wireless Attack Policies. 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.

- **Customization:** Enable 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.
- **High:** Enable or disable all applicable detection mechanisms, including all the options of low and medium-level settings.
- **Medium:** Enable specific detection mechanisms. This includes all the options in the low-level settings.
- **Low:** Default. Enable only the most critical detection mechanisms.



Wireless Attack Detection Policy

Wireless Detection: ON

AP Attack Detection Policy

○ Customization ☑ Detect AP Spoofing
○ High ☑ Detect Broadcast De-authentication
○ Medium ☑ Detect Broadcast Disassociation
● Low

Figure 207: Wireless Attack Detection Policy

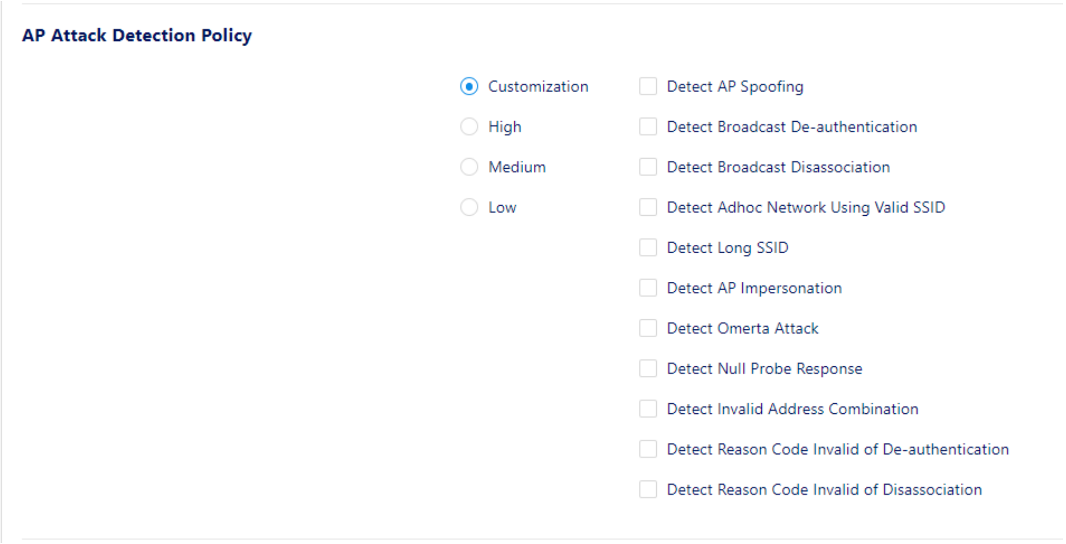
The sections below describe each of the Wireless Attack Policies.

- **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 Network 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:** This feature detects long SSIDs with more than 32 characters in the name.
- **Detect AP Impersonation:** AP impersonation attacks assume the BSSID and ESSID of a valid AP. An AP impersonation attack can be used for man-in-the-middle attacks, a Rogue AP attempting to bypass detection, or a Honeypot attack.
- **Detect Omerta Attack:** Omerta is an 802.11 DoS tool that sends disassociation frames to all stations 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 used under normal circumstances.
- **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 a broadcast or multicast MAC address in the source address field.
- **Detect Reason Code Invalid of De-authentication:** De-authentication packets with an invalid reason code will be classified as an attack.
- **Detect Reason Code Invalid of Disassociation:** Disassociation packets with an invalid reason code will be classified as an attack.



AP Attack Detection Policy

● Customization
○ High
○ Medium
○ Low

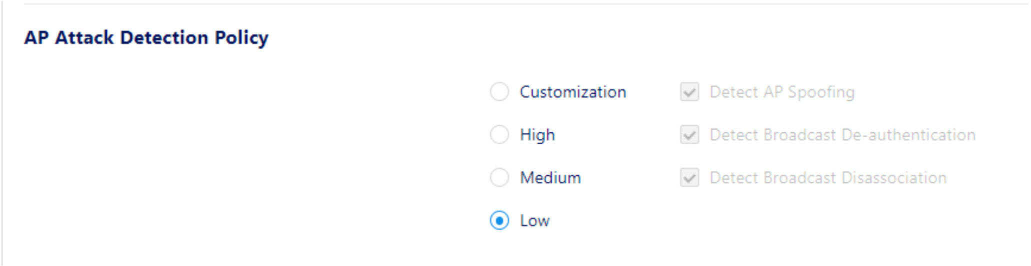
□ Detect AP Spoofing
□ Detect Broadcast De-authentication
□ Detect Broadcast Disassociation
□ Detect Adhoc Network Using Valid SSID
□ Detect Long SSID
□ Detect AP Impersonation
□ Detect Omerta Attack
□ Detect Null Probe Response
□ Detect Invalid Address Combination
□ Detect Reason Code Invalid of De-authentication
□ Detect Reason Code Invalid of Disassociation

Figure 208: AP Attack Detection Policy

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

▶ **Low:**

- Detect AP Spoofing
- Detect Broadcast De-authentication
- Detect Broadcast Disassociation



AP Attack Detection Policy

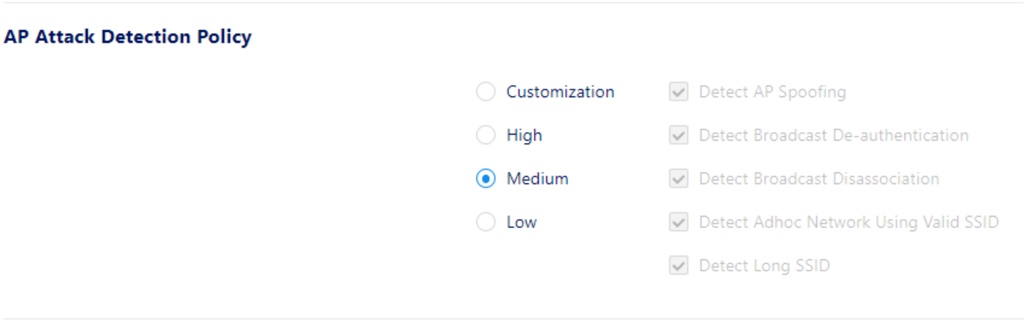
○ Customization
○ High
○ Medium
● Low

☑ Detect AP Spoofing
☑ Detect Broadcast De-authentication
☑ Detect Broadcast Disassociation

Figure 209: AP Attack Detection Policy - Low

▶ **Medium:**

- Detect AP Spoofing
- Detect Broadcast De-authentication
- Detect Broadcast Disassociation
- Detect Adhoc Network Using Valid SSID
- Detect Long SSID



AP Attack Detection Policy

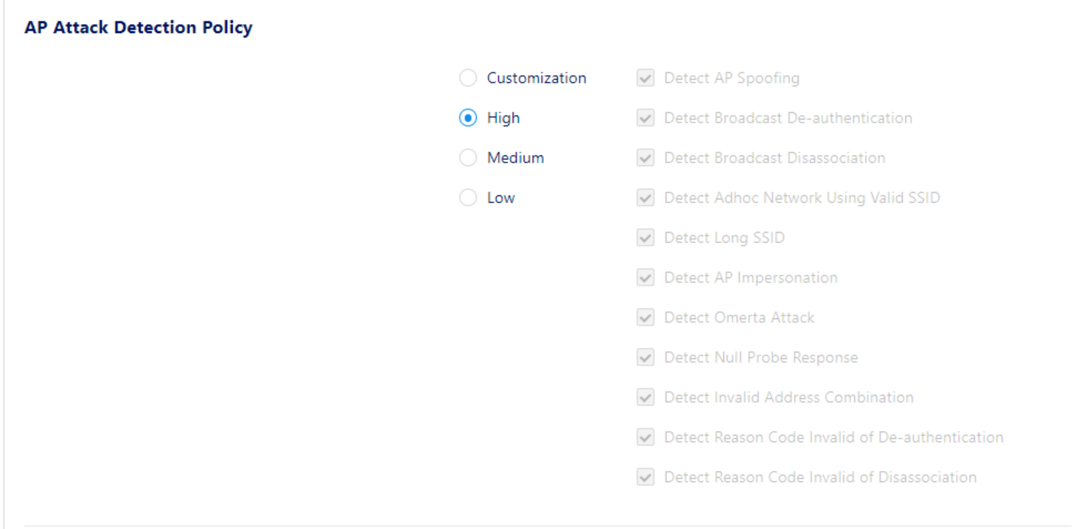
○ Customization
○ High
● Medium
○ Low

☑ Detect AP Spoofing
☑ Detect Broadcast De-authentication
☑ Detect Broadcast Disassociation
☑ Detect Adhoc Network Using Valid SSID
☑ Detect Long SSID

Figure 210: AP Attack Detection Policy - Medium

▶ **High:** The following items will all be used

- Detect AP Spoofing
- Detect Broadcast De-authentication
- Detect Broadcast Disassociation
- Detect Adhoc Network using a 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



AP Attack Detection Policy

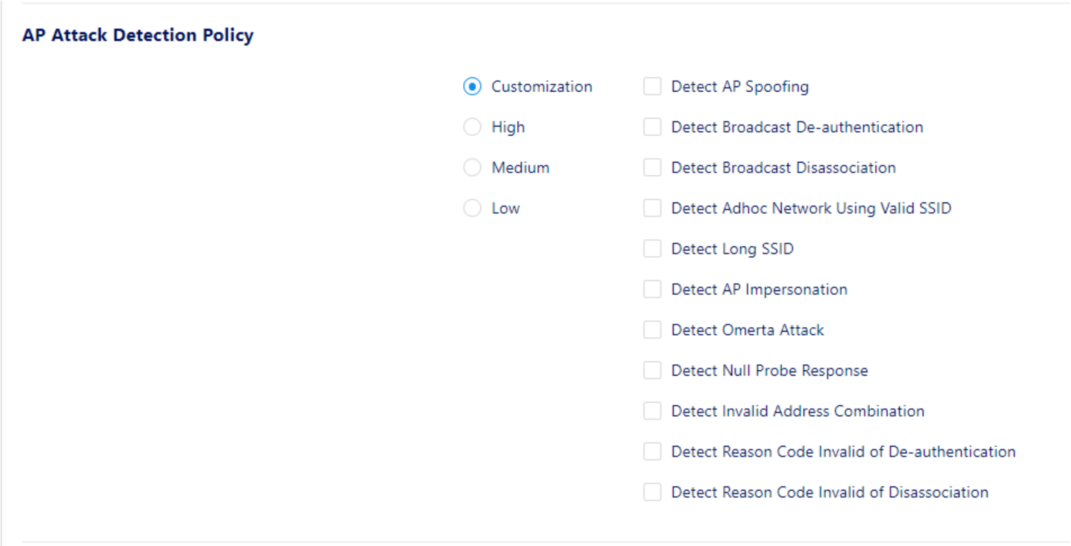
○ Customization
● High
○ Medium
○ Low

☑ 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

Figure 211: AP Attack Detection Policy - High

▶ **Customization:** You can select the attack detection policies that you care about from the following.

- Detect AP Spoofing
- Detect Broadcast De-authentication
- Detect Broadcast Disassociation
- Detect Adhoc Network using a 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



AP Attack Detection Policy

● Customization
○ High
○ Medium
○ Low

□ 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

Figure 212: AP Attack Detection Policy - Customization

■ 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 Client Misassociation:** This feature does not detect attacks but rather monitor valid wireless clients and their associations within the network. Valid client misassociation is potentially dangerous to network security. The 4 types of misassociation monitored are:

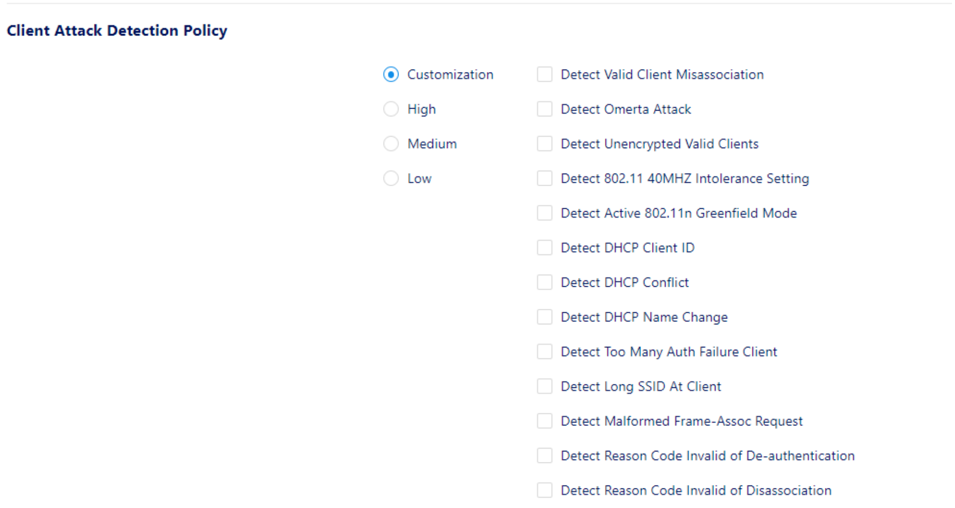
- Valid Client Associated to a Rogue AP: A valid client that is associated to a Rogue AP.

- 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 sending disassociation frames with a reason code of 0x01. This reason code is **“unspecified”** and is not used under normal circumstances.
- **Detect Unencrypted Valid Client:** A valid client that is passing traffic in an 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 40 MHz 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 40 MHz 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 cannot share the same channel as 802.11a/b/g clients. They cannot communicate with legacy devices, and the way they use the transmission medium is different, which would cause collisions, detected errors, and retransmissions.
- **Detect DHCP Client ID:** A client that sends a DHCP DISCOVER packet containing a Client-ID tag (Tag 61) that 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 that receive a DHCP address but continue to use a different IP address may indicate a misconfigured 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 or MAC cloning attack.

- **Detect Too Many Auth Failure Request:** Client that attempts to connect to DAP but fails to pass the authentication too many times indicates an attacking 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 codes will be classified as attacks.
- **Detect Reason Code Invalid of Disassociation:** Disassociation packets with invalid reason codes will be classified as attacks.



Client Attack Detection Policy

● Customization
○ High
○ Medium
○ Low

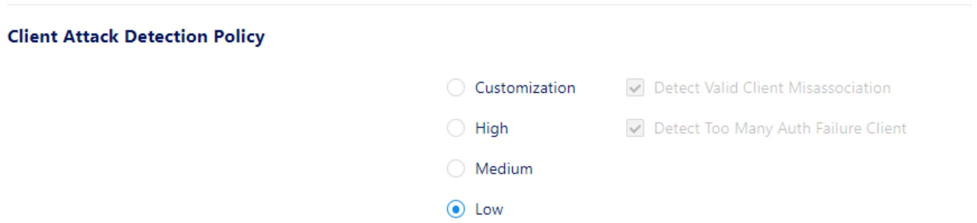
□ Detect Valid Client Misassociation
□ Detect Omerta Attack
□ Detect Unencrypted Valid Clients
□ Detect 802.11 40MHZ Intolerance Setting
□ Detect Active 802.11n Greenfield Mode
□ Detect DHCP Client ID
□ Detect DHCP Conflict
□ Detect DHCP Name Change
□ Detect Too Many Auth Failure Client
□ Detect Long SSID At Client
□ Detect Malformed Frame-Assoc Request
□ Detect Reason Code Invalid of De-authentication
□ Detect Reason Code Invalid of Disassociation

Figure 213: Client Attack Detection Policy - Customization

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



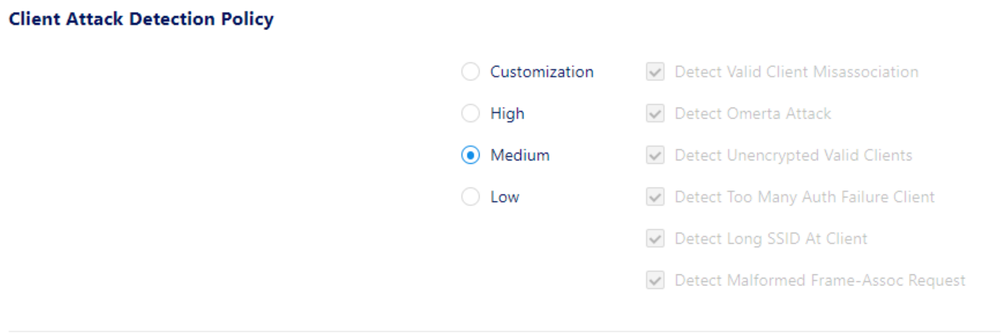
Client Attack Detection Policy

○ Customization ☑ Detect Valid Client Misassociation
○ High ☑ Detect Too Many Auth Failure Client
○ Medium
● Low

Figure 214: Client Attack Detection Policy - Low

▶ **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



Client Attack Detection Policy

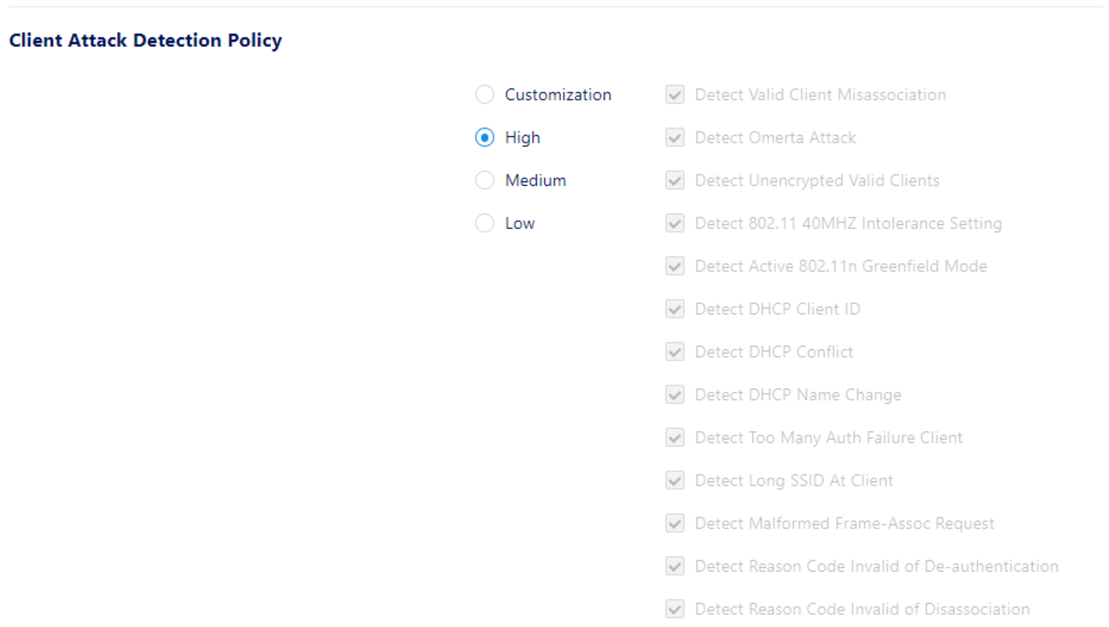
○ Customization ☑ Detect Valid Client Misassociation
○ High ☑ Detect Omerta Attack
● Medium ☑ Detect Unencrypted Valid Clients
○ Low ☑ Detect Too Many Auth Failure Client
☑ Detect Long SSID At Client
☑ Detect Malformed Frame-Assoc Request

Figure 215: Client Attack Detection Policy - Medium

▶ **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



Client Attack Detection Policy

○ Customization
● High
○ Medium
○ Low

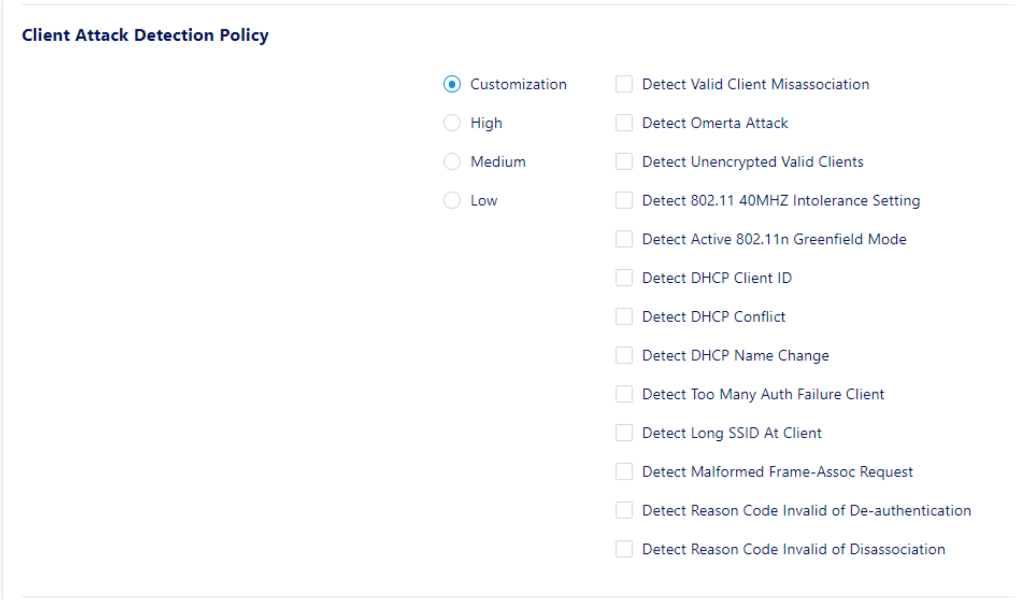
☑ Detect Valid Client Misassociation
☑ Detect Omerta Attack
☑ Detect Unencrypted Valid Clients
☑ Detect 802.11 40MHZ Intolerance Setting
☑ Detect Active 802.11n Greenfield Mode
☑ Detect DHCP Client ID
☑ Detect DHCP Conflict
☑ Detect DHCP Name Change
☑ Detect Too Many Auth Failure Client
☑ Detect Long SSID At Client
☑ Detect Malformed Frame-Assoc Request
☑ Detect Reason Code Invalid of De-authentication
☑ Detect Reason Code Invalid of Disassociation

Figure 216: Client Attack Detection Policy - High

▶ **Customization**:

You can select the attack detection policies that you care about from the following.

- 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 Attack Detection Policy

- ● Customization
- ○ High
- ○ Medium
- ○ Low

- □ 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

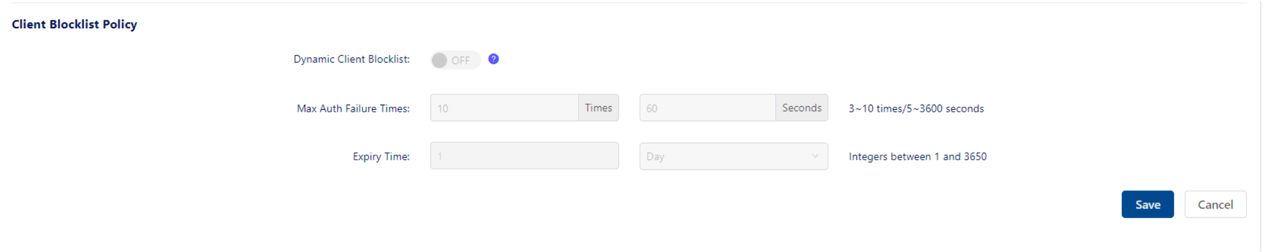
Figure 217: Client Attack Detection Policy - Customization

- **Client blocklist policy**

  There are 2 sources for the Client Blocklist: created manually by user or added dynamically by the system. If the Dynamic Client Blocklist is enabled, then intruders discovered by WIPS are dynamically added to the Client Blocklist and prevented from associating with the network.

  The following detected items are added to the Client Blocklist by the system: List of Client Attack Detection, ad hoc clients, and Clients associated to Rogue AP.

  - **Max Auth Failure Times:** Authentication failure times threshold. When a client fails to pass the authentication too many times in the associated phase within a short period of time, it will be classified as an attack and added into the Client Blocklist. (Possible values: 3~10 times/5~3600 seconds, Default Setting: 10 times/60 seconds).
  - **Expiry Time:** Expiry time for the Client Blocklist. Once expired, a client will be removed from the blocklist and allowed to be associated with the valid network until it is detected as a threat again. (Possible values: 1 hour to 365 days, Default Setting: 1 day).



Client Blocklist Policy

Dynamic Client Blocklist: OFF

Max Auth Failure Times: 10 Times 60 Seconds 3~10 times/5~3600 seconds

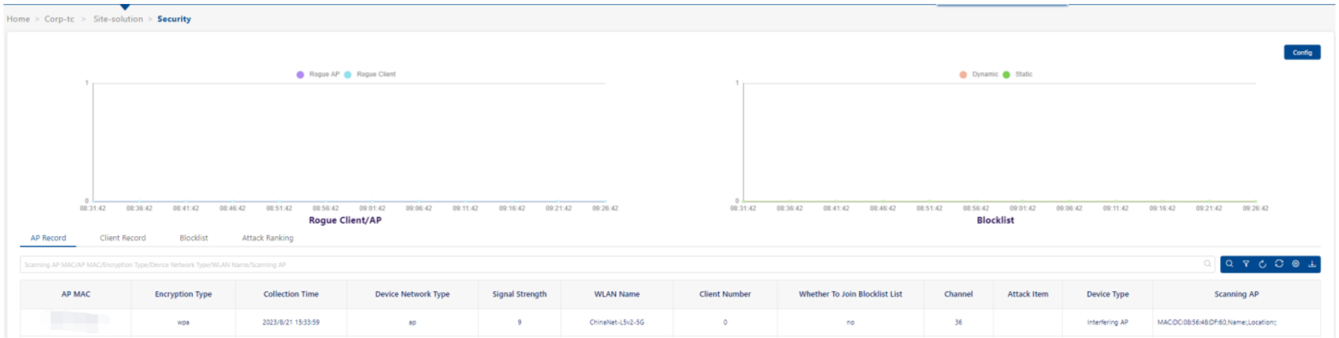
Expiry Time: 1 Day Integers between 1 and 3650

Figure 218: Client blocklist policy

11.2 AP record

The **Security → AP Record** is a list of the scanned APs on the network, including Interfering APs, Rogue APs, and Valid APs.

- **AP MAC:** MAC address of scanned APs.
- **Encryption Type:** Encryption method of the WLAN.
- **Collection Time:** The latest time that the scanned AP was detected.
- **Device Network Type:** The network type of the scanned APs.
- **Signal Strength:** RSSI of the scanned AP.
- **WLAN Name:** SSID of the AP broadcast.
- **Client Number:** The number of clients associated to the scanned AP
- **Whether to Join Blocklist List:** Whether the AP is added to the Blocklist.
- **Channel:** Working channel of the radio frequency on the scanned AP.
- **Attack Item:** The Attack Detection Policy used (e.g., Detect Valid Station Misassociation)
- **Device Type:**
  - Rogue AP: The AP whose MAC matched the **Rouge OUI** is identified as a rouge AP. Setting the **Detect Rogue SSID Keyword** is another way to determine whether the AP is a rogue AP.
  - Valid AP: The AP whose MAC matched the **Valid OUI** is identified as a valid AP.
  - Interfering AP: With the exception of Rouge APs and Valid APs, the rest of APs are considered interfering APs.
- **Scanning AP:** MAC address of the AP that scans the Interfering APs, Rogue APs, and Valid APs.

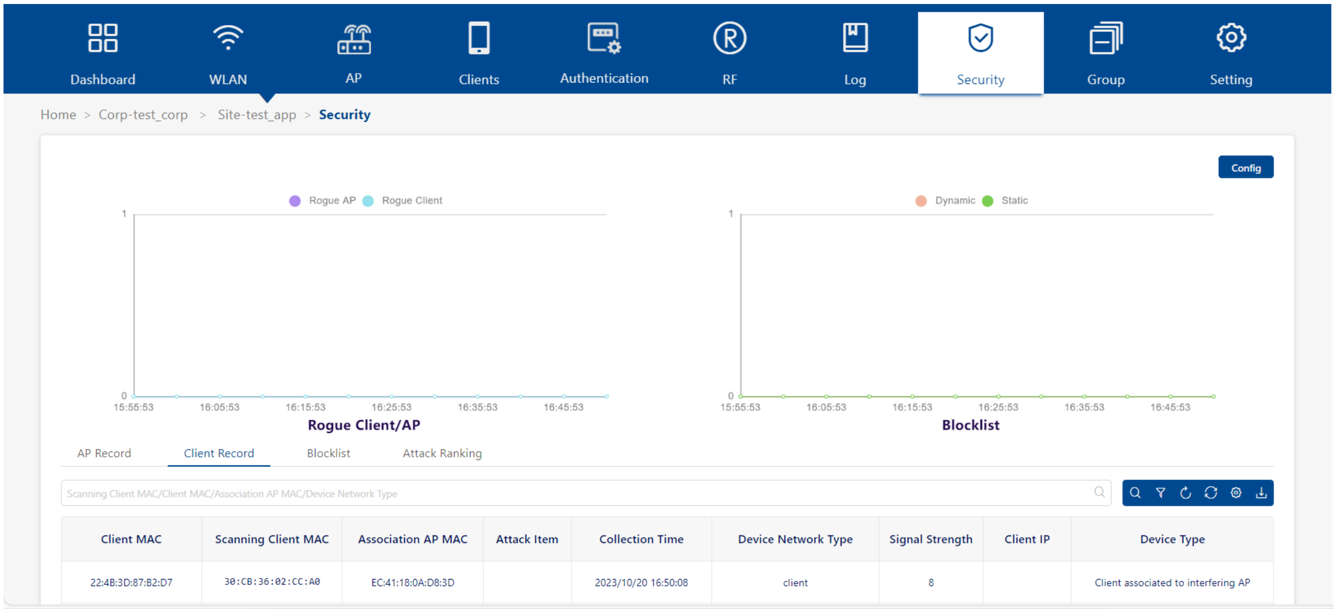


AP MAC	Encryption Type	Collection Time	Device Network Type	Signal Strength	WLAN Name	Client Number	Whether To Join Blocklist List	Channel	Attack Item	Device Type	Scanning AP
[redacted]	wpa	2023/8/21 15:33:59	ap	9	ChinaNet-L5v2-5G	0	no	36		Interfering AP	MAC:DC:08:56:48:DF:60,Name:,Location:;

Figure 219: AP record screen

11.3 Client record

- **Client MAC:** MAC address of the interfering or rogue client.
- **Scanning Client MAC:** MAC address of the scanning client.
- **Association AP MAC:** MAC address of the interfering or rogue AP with 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 or interfering client was scanned.
- **Device Network Type:** The network type of detected clients.
- **Signal Strength:** RSSI of the scanned client.
- **Client IP:** IP address of the scanned client.
- **Device Type:**
  - Clients Associated to a Rogue AP
  - Clients Associated to an Interfering AP



Client MAC	Scanning Client MAC	Association AP MAC	Attack Item	Collection Time	Device Network Type	Signal Strength	Client IP	Device Type
22:4B:3D:87:B2:D7	30:CB:36:02:CC:A0	EC:41:18:0A:D8:3D		2023/10/20 16:50:08	client	8		Client associated to interfering AP

Figure 220: Client Record screen

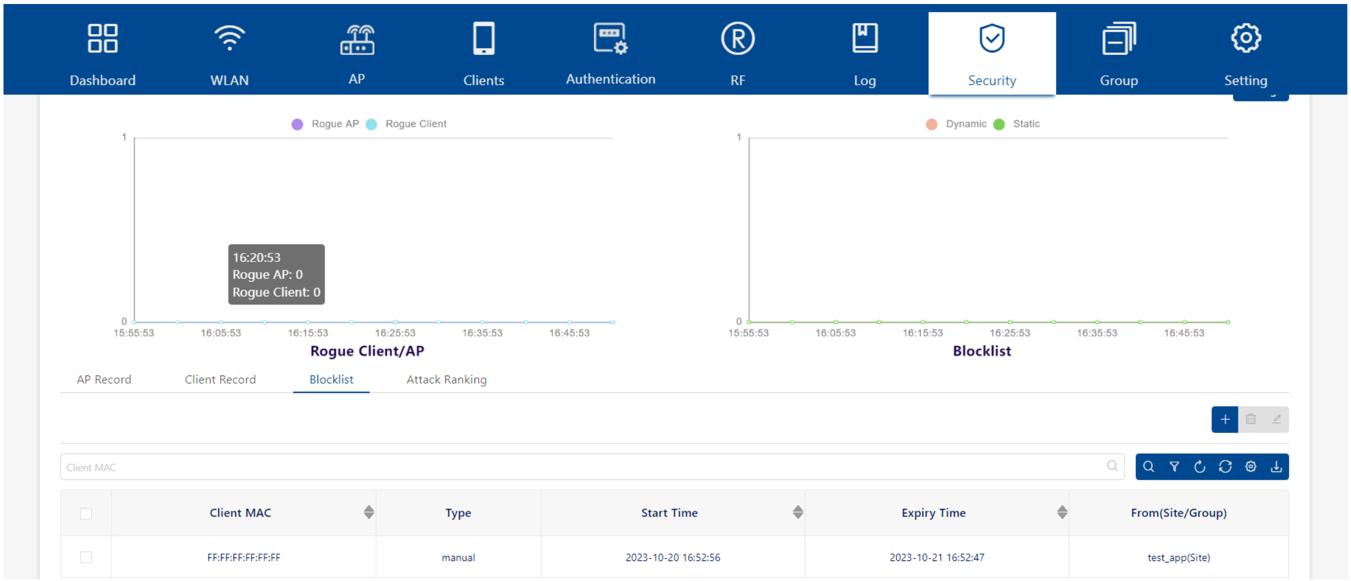
11.4 Blocklist

Blocklist focuses on the basic access control mechanism for users connecting to an SSID based on the client level. Those clients on the Blocklist are denied associating with the DAP. Once a client is on the Blocklist, it cannot connect to any WLAN of any security level (Enterprise, Personal, or Open). You can add or delete the Blocklist based on the client's MAC address.

The Wireless Blocklist Page shows information about all blocked clients. It is also used to manually add clients to the blocklist.

- **Client MAC:** MAC address of the client in the Blocklist.
- **Type:** The way that the client was added to the blocklist.
  - **Manual:** Added to the Blocklist by the user.
  - **Auto:** Dynamically added by the WIPS policy.
- **Start Time:** The starting time for the block.

  During the duration, the client is not allowed to access the wireless network.
- **Expiry time:** The expiration time for the Blocklist.
  The client can access the wireless network after the expiration time.
- **From(Site/Group):** Indicates which site or group the client is from.



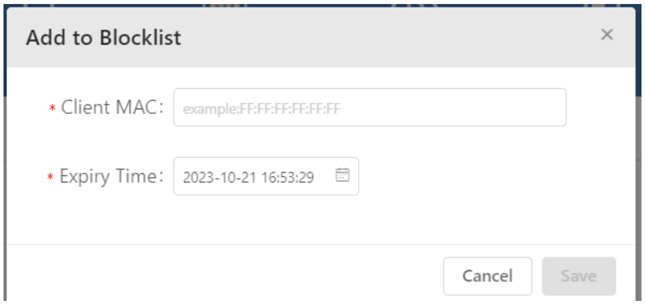
□	Client MAC	Type	Start Time	Expiry Time	From(Site/Group)
□	FF:FF:FF:FF:FF:FF	manual	2023-10-20 16:52:56	2023-10-21 16:52:47	test_app(Site)

Figure 221: Blocklist screen

11.4.1 Adding a client to the blocklist

- ☐ Click the **“+”** icon, and the **“Add to Blocklist”** module opens.
- ☐ Enter the client's **“MAC address”.**
- ☐ Click the **“Save”** button.
- ☐ Repeat to add additional clients.

You should set an Expire time for the client. That means the client can connect to the SSID of this Site again after expiration.



Add to Blocklist

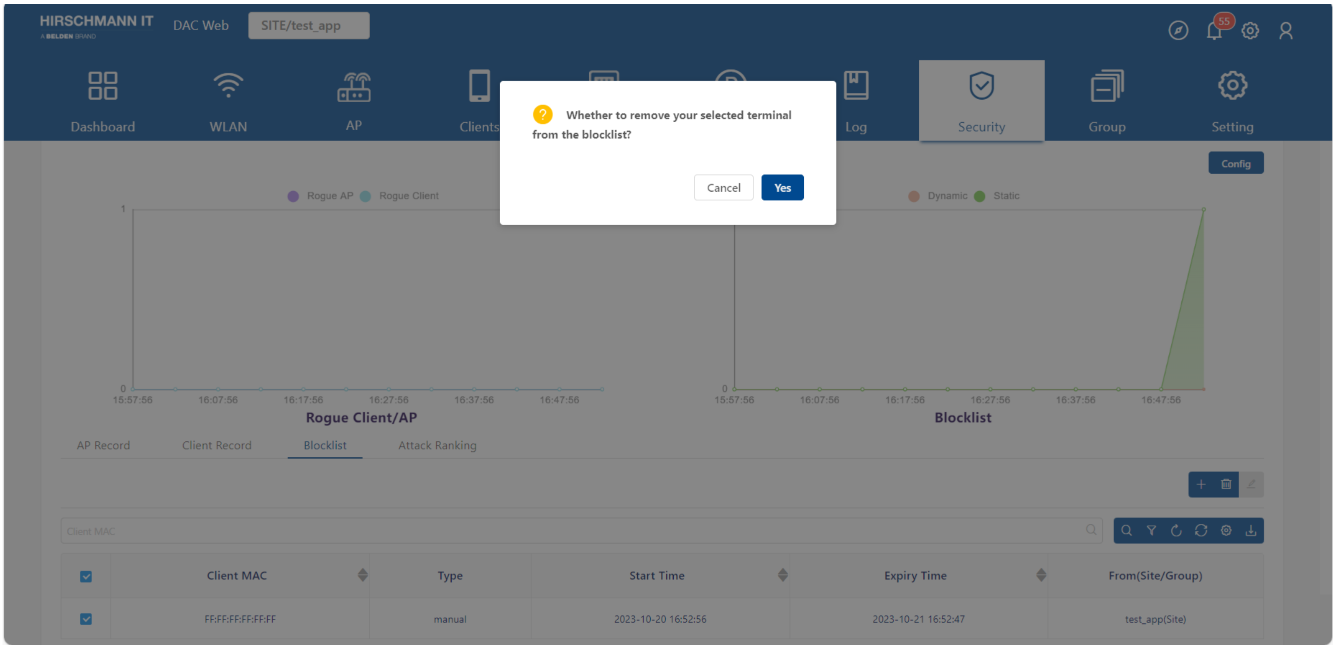
* Client MAC: example:FF:FF:FF:FF:FF:FF

* Expiry Time: 2023-10-21 16:53:29

Figure 222: Adding a client to the blocklist

11.4.2 Deleting a client from the blocklist

- ☐ Select the client(s) in the blocklist.
- ☐ Click the **“Delete”** icon.
- ☐ Click **“Yes”** on the confirmation prompt.



Whether to remove your selected terminal from the blocklist?

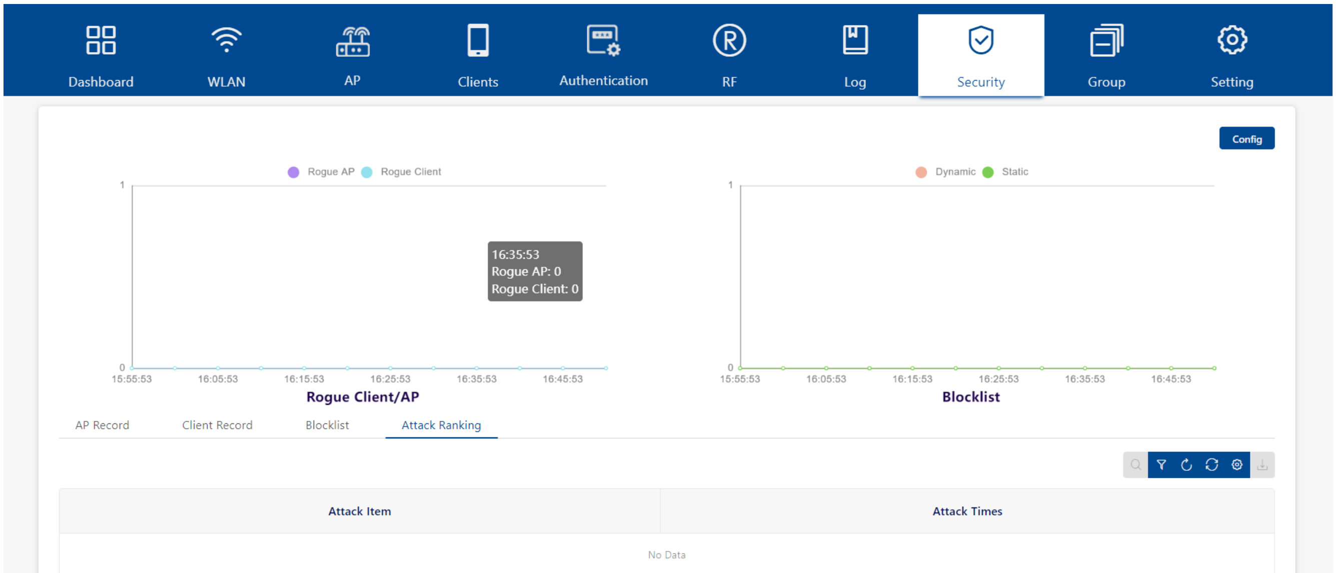
☑	Client MAC	Type	Start Time	Expiry Time	From(Site/Group)
☑	FF:FF:FF:FF:FF:FF	manual	2023-10-20 16:52:56	2023-10-21 16:52:47	test_app(Site)

Figure 223: Deleting a client from the blocklist

11.5 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 the attack item.



Attack Item	Attack Times
No Data	

Figure 224: Attack ranking screen

12 Captive portal

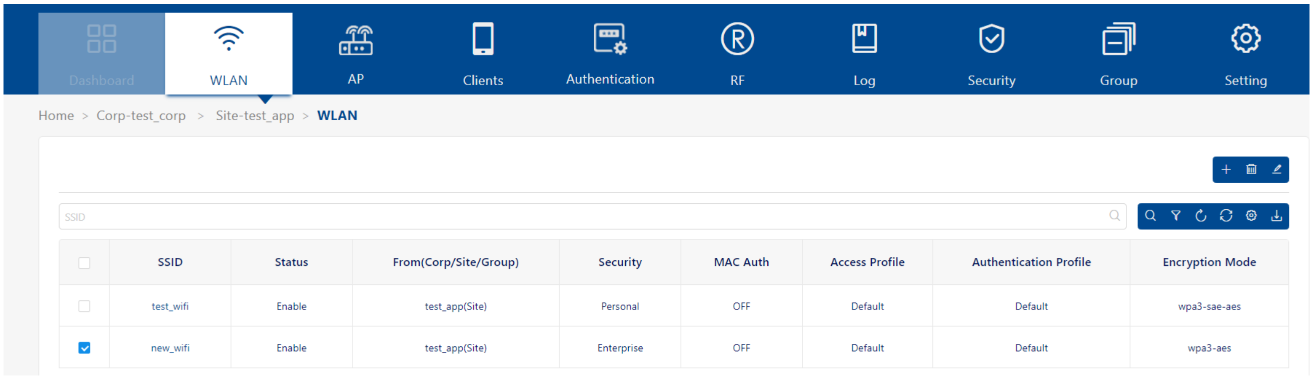
Captive portal authentication is a mechanism for obtaining user credentials through web pages and authenticating them through a RADIUS server. If the authentication is successful, the RADIUS server may return a role (policy list) that applies to traffic from the user device. Captive Portal provides a secondary level of authentication that applies a new role (QoS policy list) to the user. The employee feature provides an external, guest Captive Portal authentication mechanism.

This chapter contains the following topics:

- Entry to portal page editor
- Portal editor view
- Select template
- Page selector
- Page view
- Component attributes

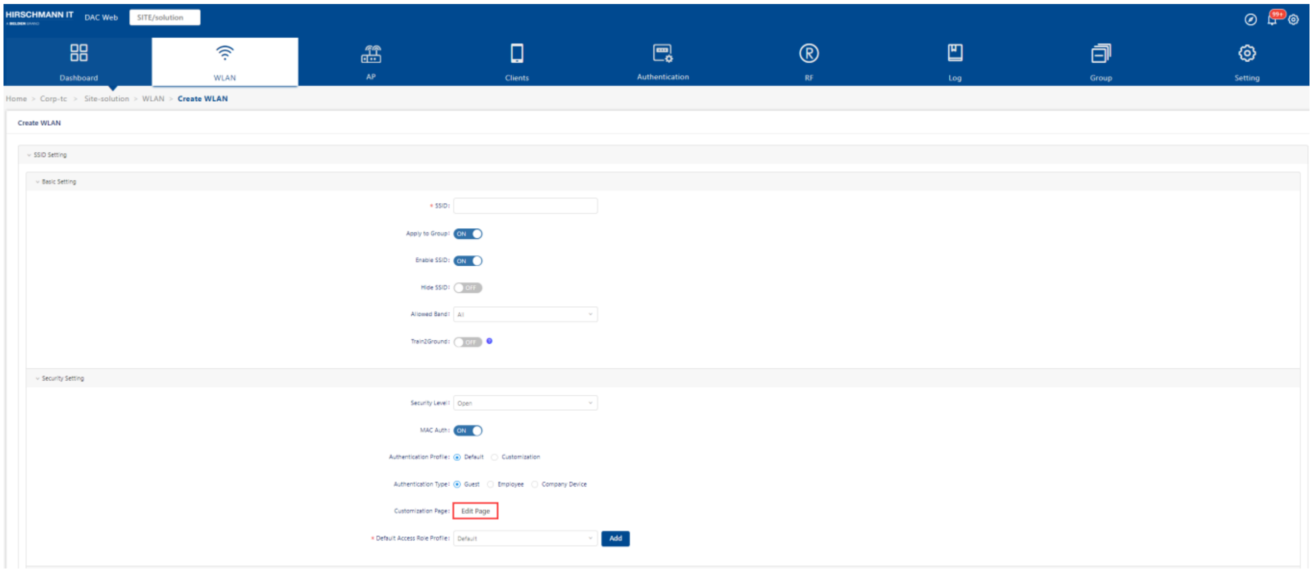
12.1 Entry to portal page editor

- Portal page is binding to **Guest Access Strategy** or **Employee Access Strategy**.
- To use Portal authentication, you should enable **“MAC Auth”** and disable **“Train2Groud”** on the WLAN page.
- When you select **“Default”** for Authentication Profile, you can enter the portal editor by clicking the **“Edit page”** button.



Home > Corp-test_corp > Site-test_app > **WLAN**

	SSID	Status	From(Corp/Site/Group)	Security	MAC Auth	Access Profile	Authentication Profile	Encryption Mode
☐	test_wifi	Enable	test_app(Site)	Personal	OFF	Default	Default	wpa3-sae-aes
☑	new_wifi	Enable	test_app(Site)	Enterprise	OFF	Default	Default	wpa3-aes



Home > Corp-tc > Site-solution > WLAN > **Create WLAN**

Create WLAN

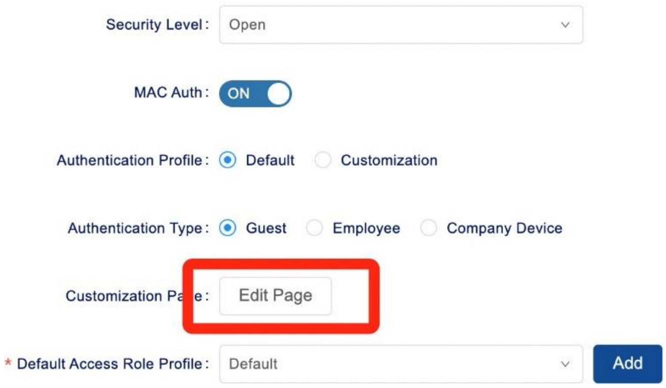
SSID Setting

Basic Setting

* SSID:
Apply to Group: ON
Enable SSID: ON
Hide SSID: OFF
Allowed Band: All
Train2Ground: OFF

Security Setting

Security Level: Open
MAC Auth: ON
Authentication Profile: ● Default ○ Customization
Authentication Type: ● Guest ○ Employee ○ Company Device
Customization Page: Edit Page
* Default Access Role Profile: Default



Security Level: Open

MAC Auth: ON

Authentication Profile: ● Default ○ Customization

Authentication Type: ● Guest ○ Employee ○ Company Device

Customization Pa e: Edit Page

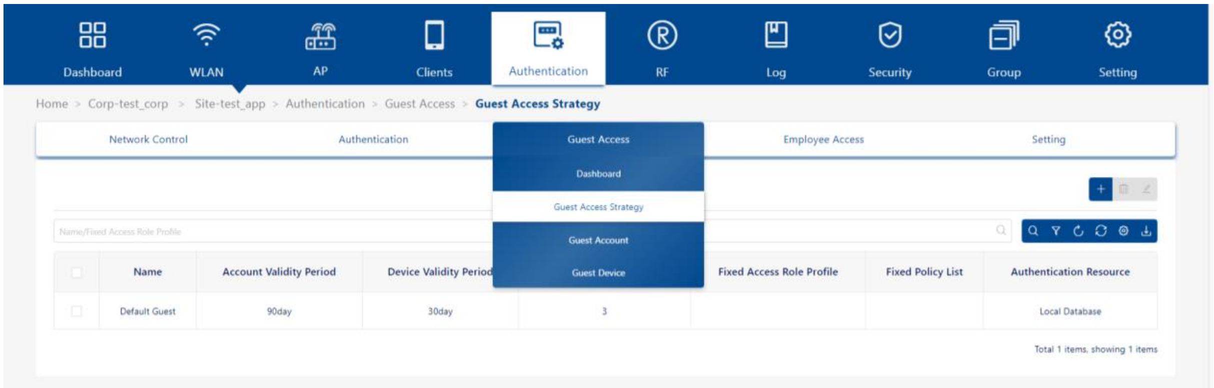
* Default Access Role Profile: Default Add

Figure 225: Edit portal page

- □ If you select **“Customization”** for **“Authentication Profile”**, you can find the entrance of Portal editor in the page of Guest Access Strategy or Employee Access Strategy.

  - ▶ Guest Access Strategy

    Authentication → Guest Access → Guest Access Strategy



Home > Corp-test_corp > Site-test_app > Authentication > Guest Access > **Guest Access Strategy**

Name/Fixed Access Role Profile

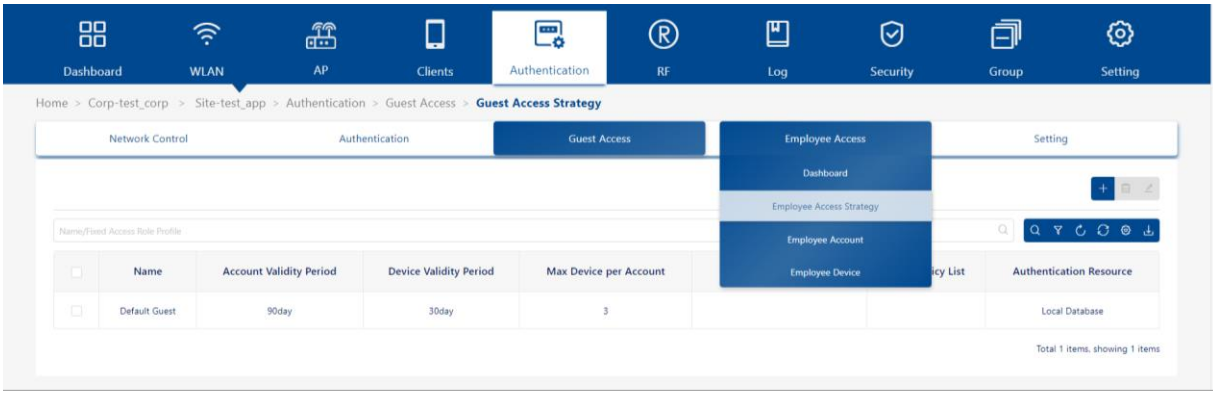
	Name	Account Validity Period	Device Validity Period		Fixed Access Role Profile	Fixed Policy List	Authentication Resource
□	Default Guest	90day	30day	3			Local Database

Total 1 items, showing 1 items

Figure 226: Entry to portal page editor - Guest

  - ▶ Employee Access Strategy

    Authentication → Employee Access → Employee Access Strategy



□	Name	Account Validity Period	Device Validity Period	Max Device per Account		icy List	Authentication Resource
□	Default Guest	90day	30day	3			Local Database

Total 1 items, showing 1 items

Figure 227: Entry to portal page editor - Employee

12.2 Portal editor view

The layout of portal customized page is shown in the below figure. The Portal Page is divided into the following functional blocks:

- **Page selector**

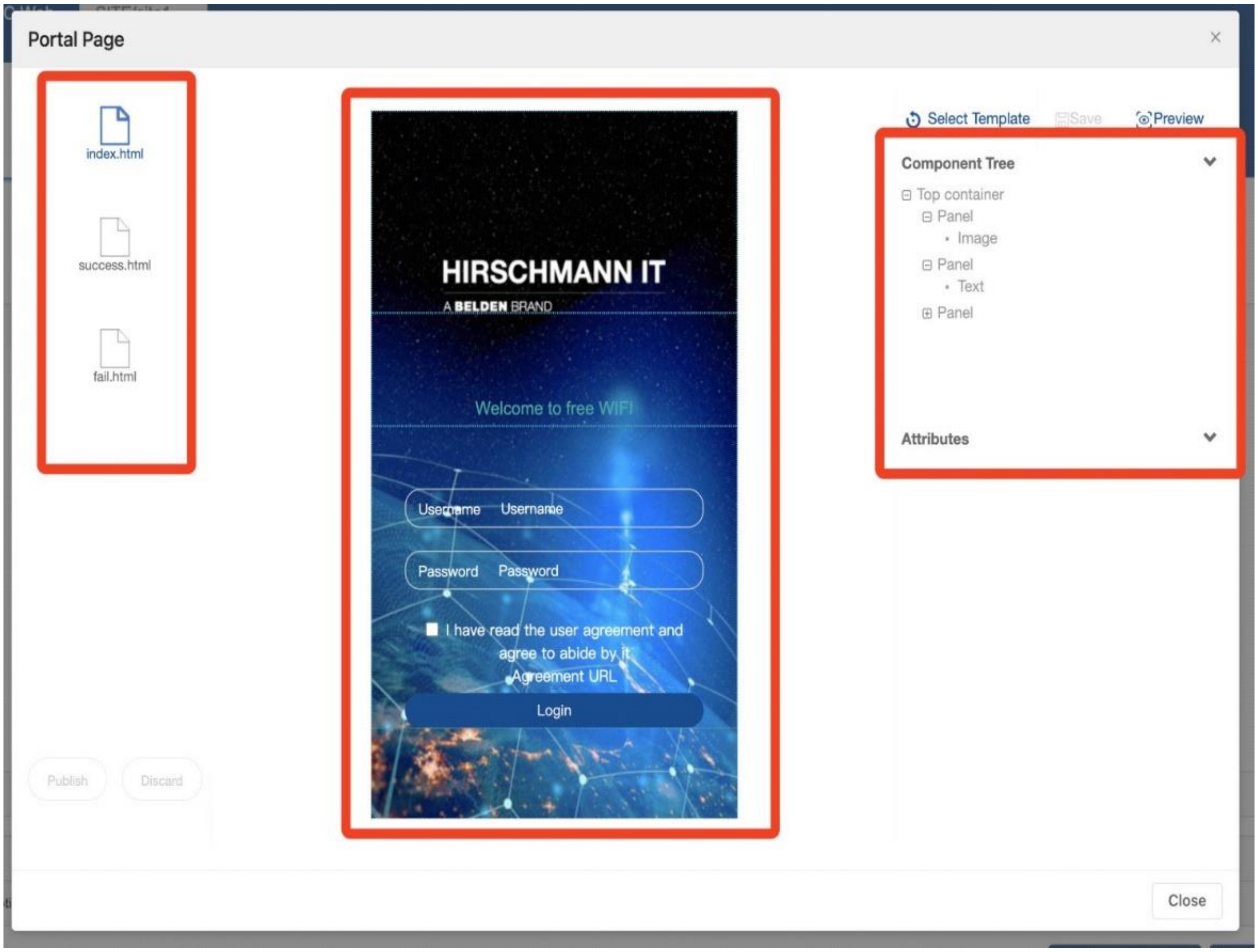
  It usually includes 3 HTML pages: index, success, and fail. You can select one of them to edit.

- **Page view**

  Dynamic display of the 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 an HTML Component.

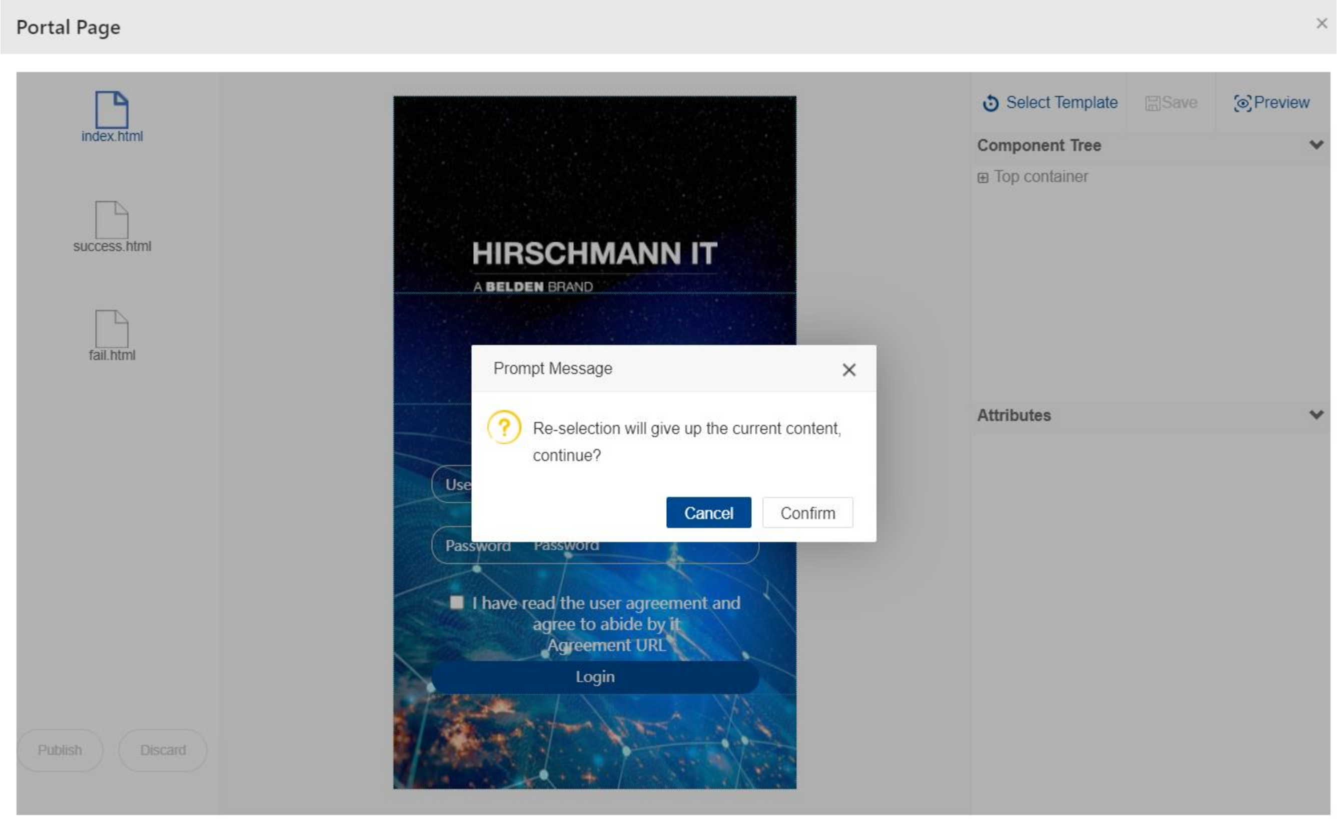


□ I have read the user agreement and agree to abide by it
Agreement URL

Figure 228: Portal editor view

12.3 Select template

- □ Click the **“Select Template”** button, which is at the top of the page attributes view.
- □ On the **“Prompt Message”** window, click the **“Confirm”** button.



Portal Page

Prompt Message

Re-selection will give up the current content, continue?

Figure 229: Select template

- □ There are 4 templates that you can select:
  - ▶ **Login by Account:** From this Portal template, the user can log in 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.

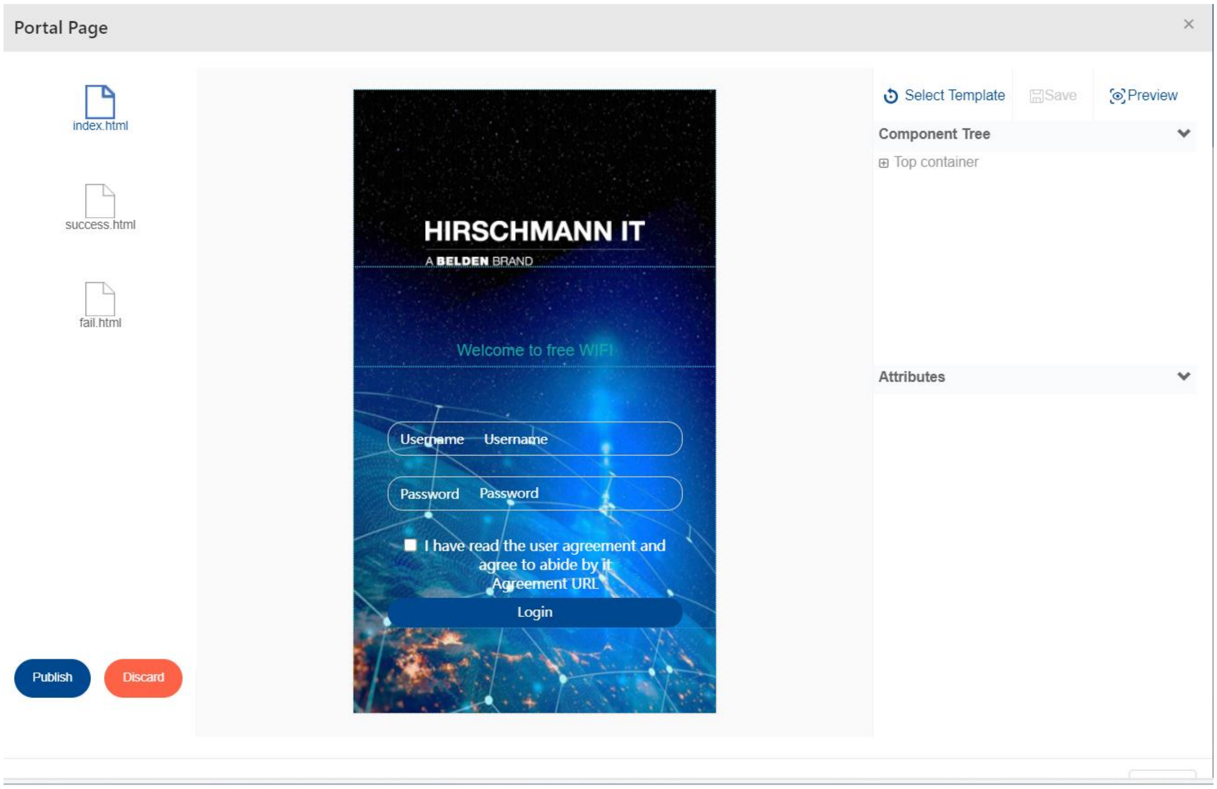


Figure 230: Select template - Login by Account

- **Access Code:** This Portal is used for guest access. An Access Code can be added at the **"Create Guest Account"** page. Select **"Access Code"** as the Guest Type.

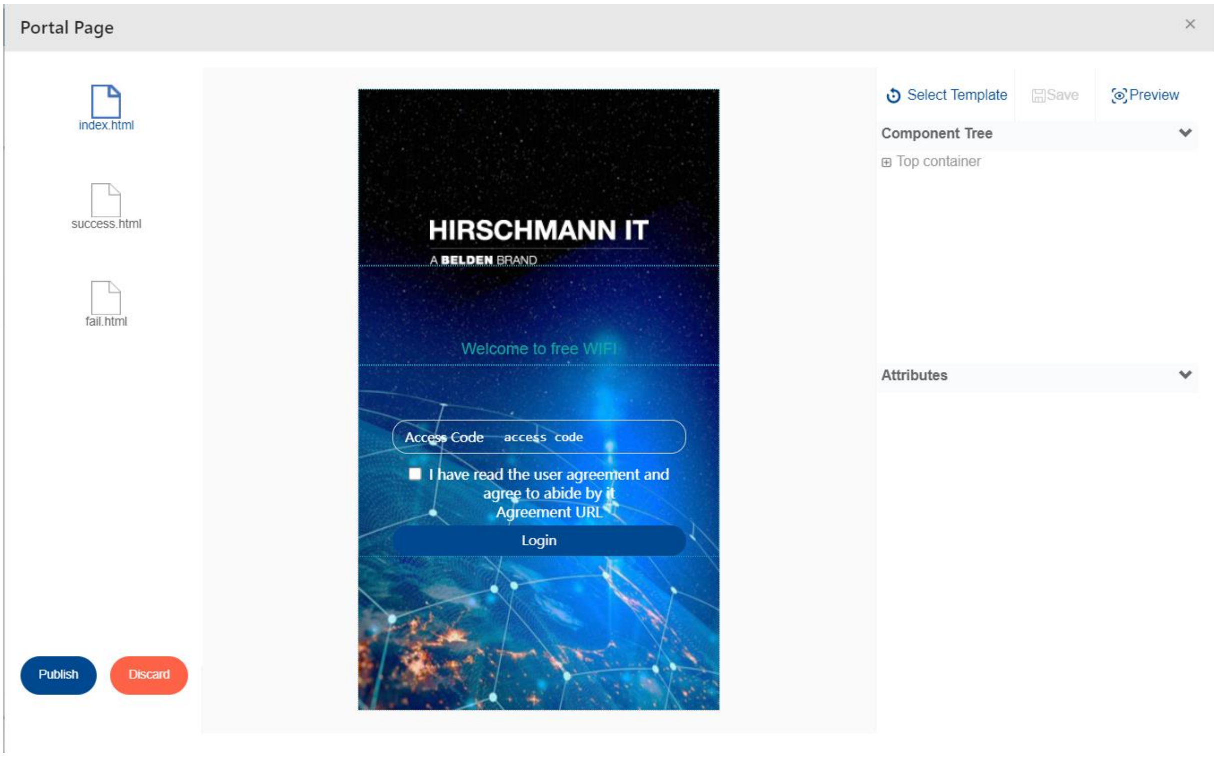


Figure 231: Select template - Access code

- **Scan QRCode by Employee:** This Portal is used for guest access. When the guest is associated with the WLAN using this template, they will get a portal page containing a QR code. Any employee can scan the QR code with the user certified mobile phone to authorize the guest.

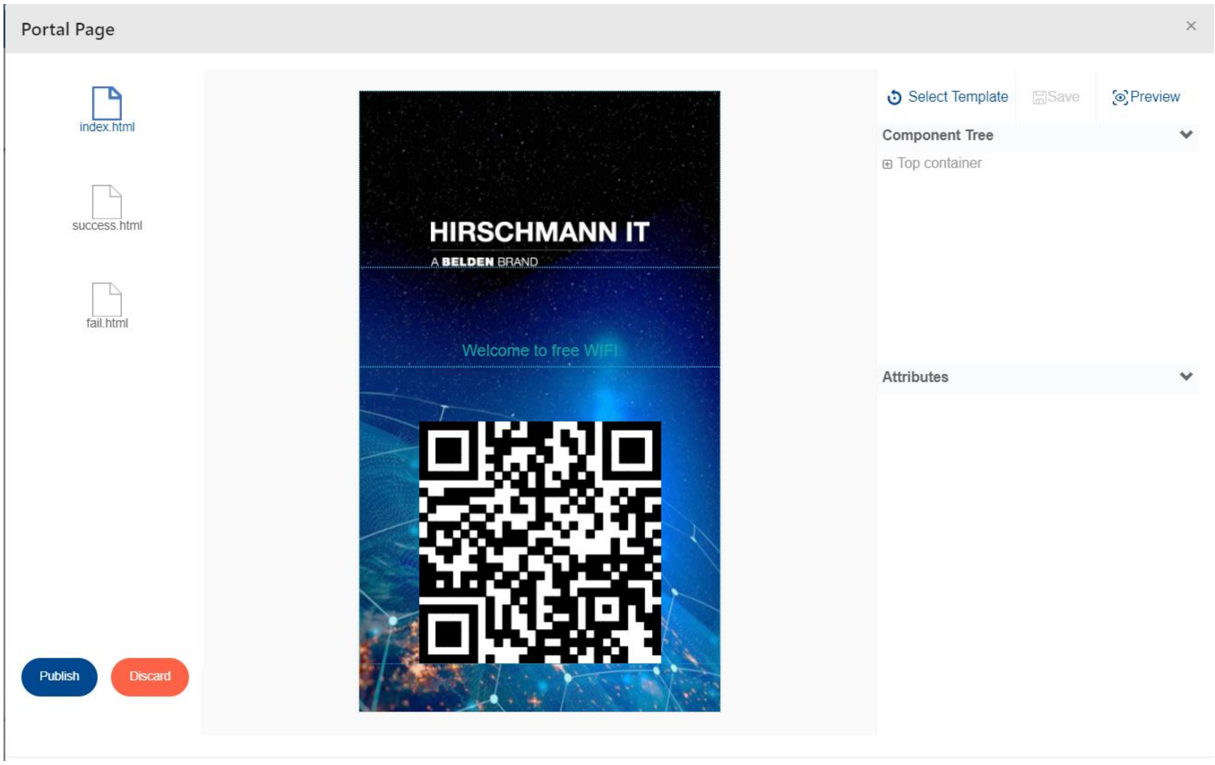


Figure 232: Select template - Scan QRcode by Employee

- **SMS Login:** From this Portal template, the user can log in with a mobile number.

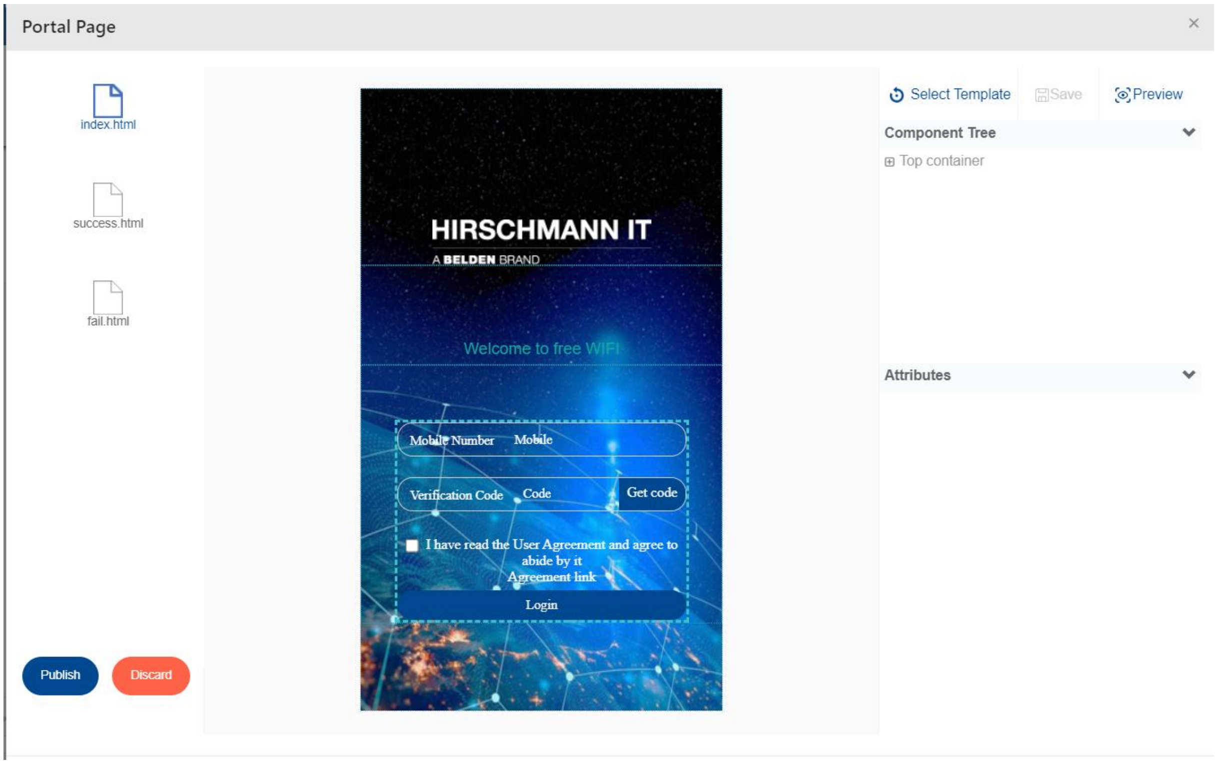
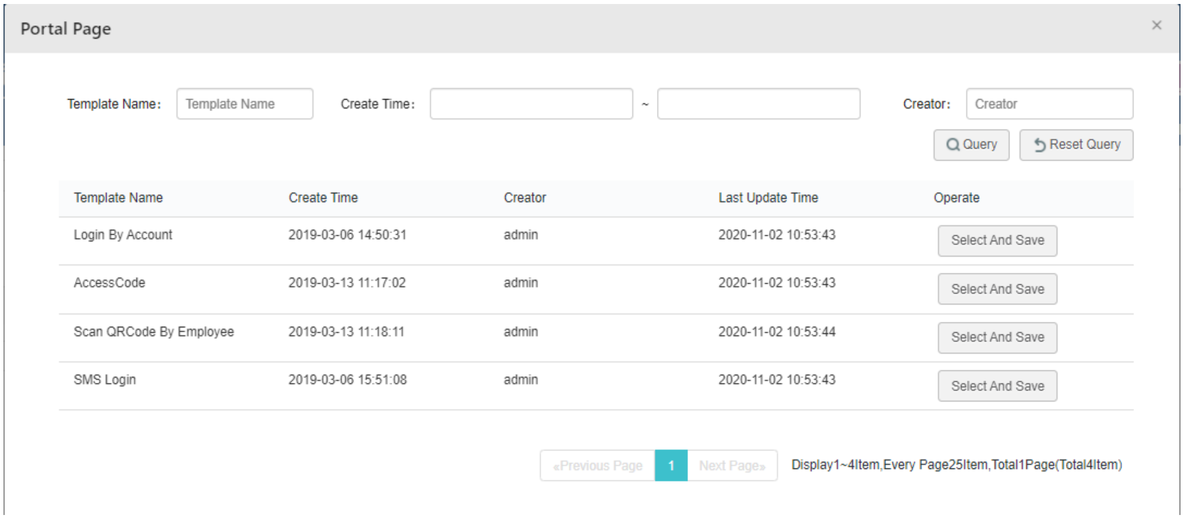


Figure 233: Select template – SMS Login


Portal Page

Template Name: Template Name Create Time: ~ Creator: Creator

Query Reset Query

Template Name	Create Time	Creator	Last Update Time	Operate
Login By Account	2019-03-06 14:50:31	admin	2020-11-02 10:53:43	Select And Save
AccessCode	2019-03-13 11:17:02	admin	2020-11-02 10:53:43	Select And Save
Scan QRCode By Employee	2019-03-13 11:18:11	admin	2020-11-02 10:53:44	Select And Save
SMS Login	2019-03-06 15:51:08	admin	2020-11-02 10:53:43	Select And Save

«Previous Page 1 Next Page» Display1~4Item,Every Page25Item,Total1Page(Total4Item)

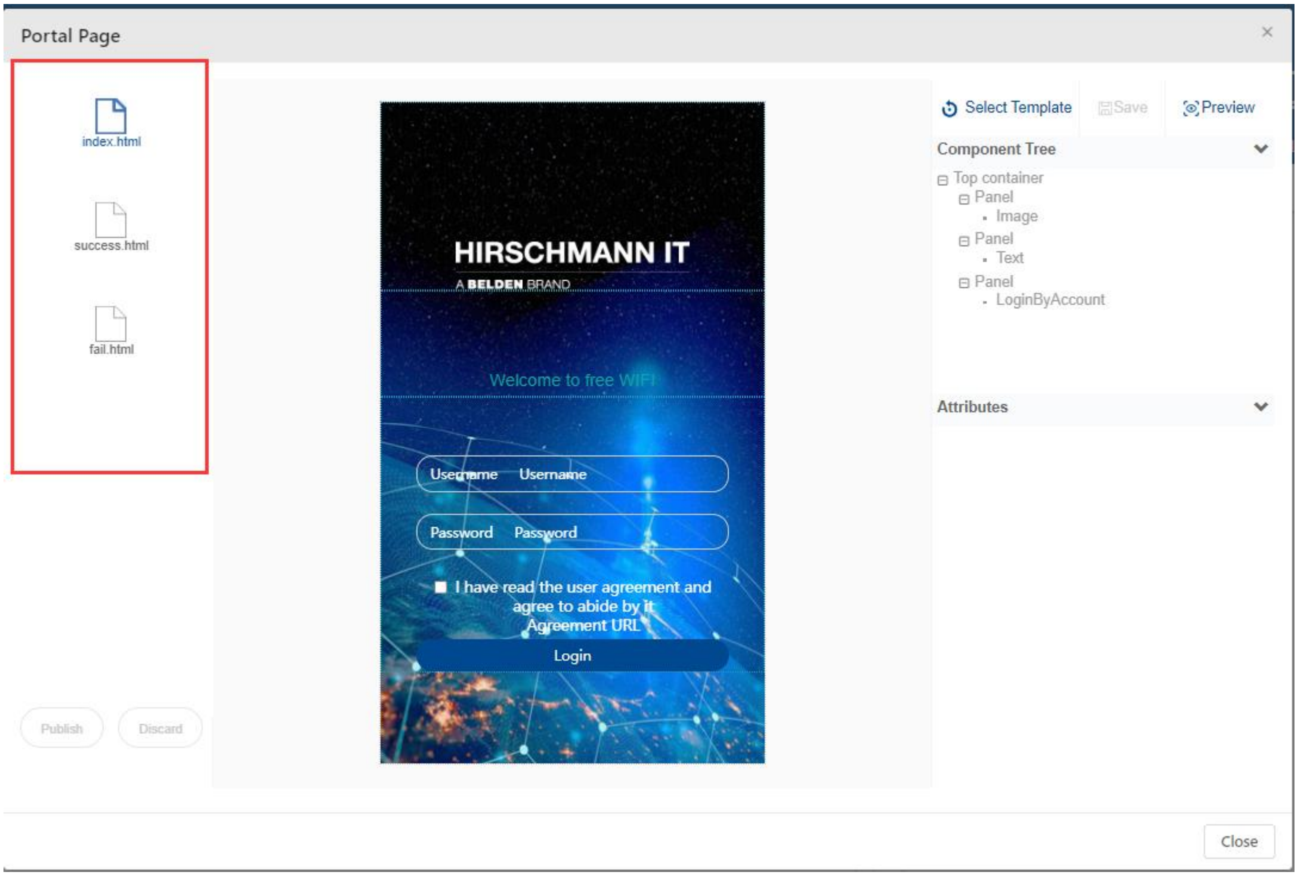
Figure 234: Portal page

12.4 Page selector

Each portal template usually contains 3 pages:

- Index
- Success
- Failed

The index page contains the login form. The user will see the success page when they log in successfully. When the user is unable to log in, they will see the failed page.
Click the page, and then you can edit it.

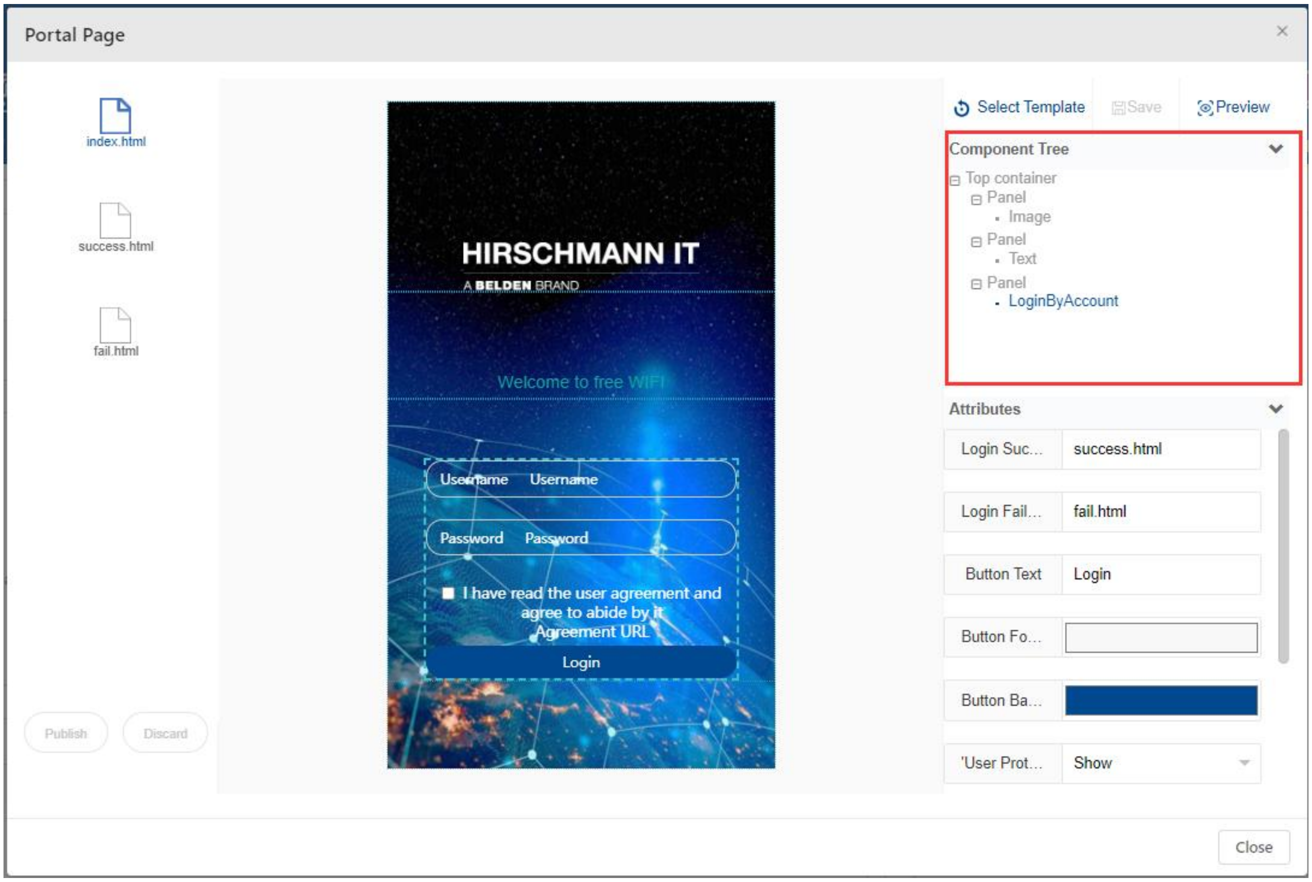


□ I have read the user agreement and agree to abide by it
Agreement URL

Figure 235: Page selector

12.5 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. To change the display content and visual effect of the page.



Component Tree

- Top container
  - Panel
    - Image
  - Panel
    - Text
  - Panel
    - LoginByAccount

Attributes

Login Suc...	success.html
Login Fail...	fail.html
Button Text	Login
Button Fo...	▭
Button Ba...	■
'User Prot...	Show

Figure 236: Component tree

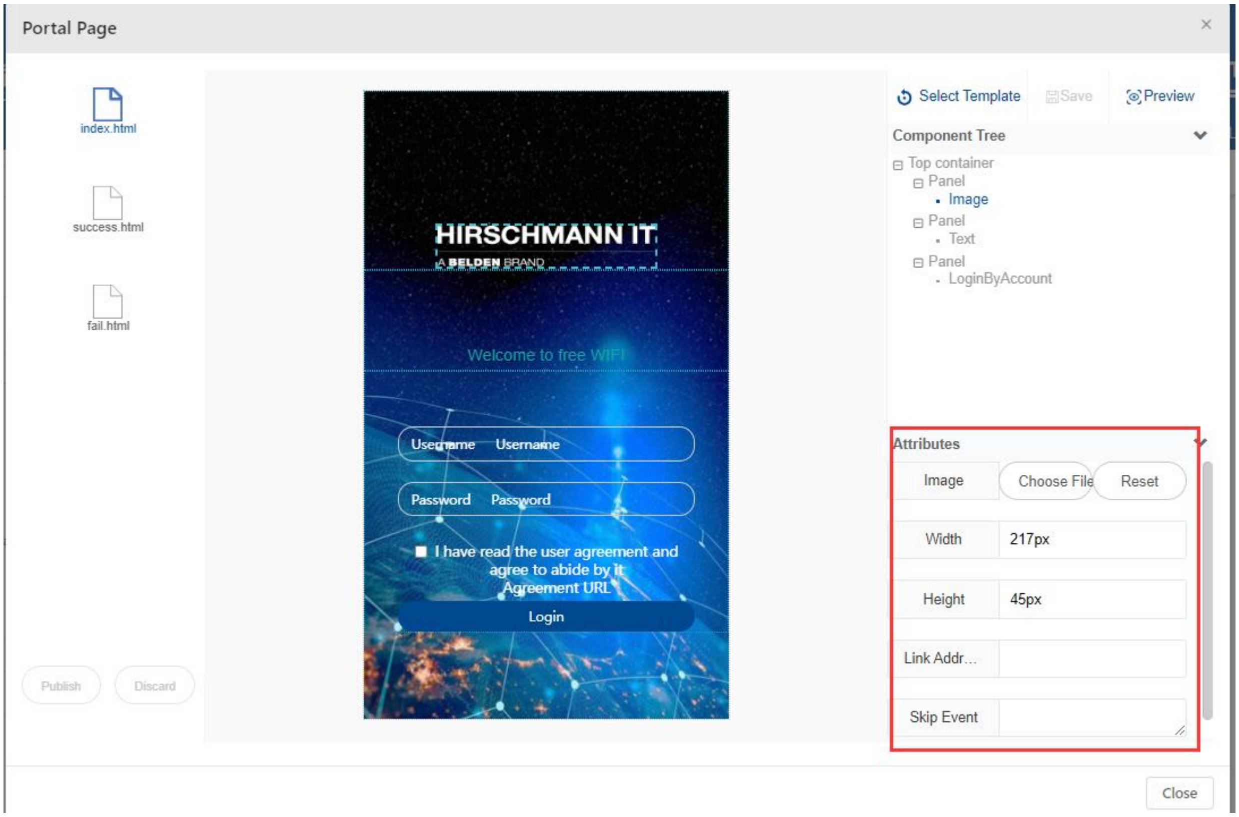
12.6 Component attributes

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

12.6.1 Image component

Below are listed several attributes of the 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 verify that the IP address of the hyperlink is in the allowed IP.
- **Skip Event:** The event specified by the user to jump after clicking on the picture.



Image

Width 217px

Height 45px

Link Addr...

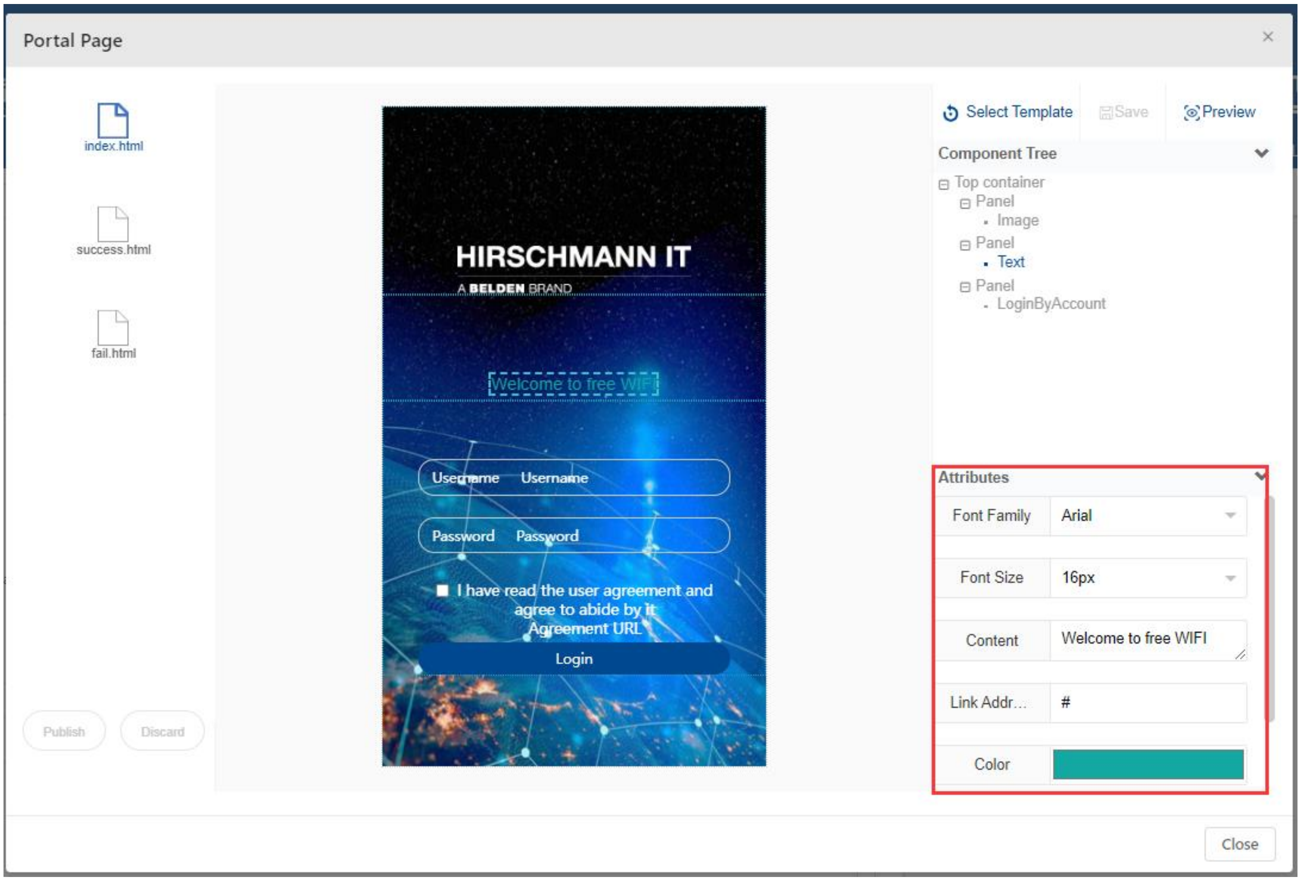
Skip Event

Figure 237: Image component attributes

12.6.2 Text component

Below are listed several attributes of text components:

- **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 you click the text, open the URL. If the current page is not a successful page, you need to verify that the IP address of this URL is in the allowed IP.
- **Color:** The font color of the text.
- **Action:** The action of clicking the text. It can be one of the following values: none, back, or forward. If the link address is configured, then it should not work here.



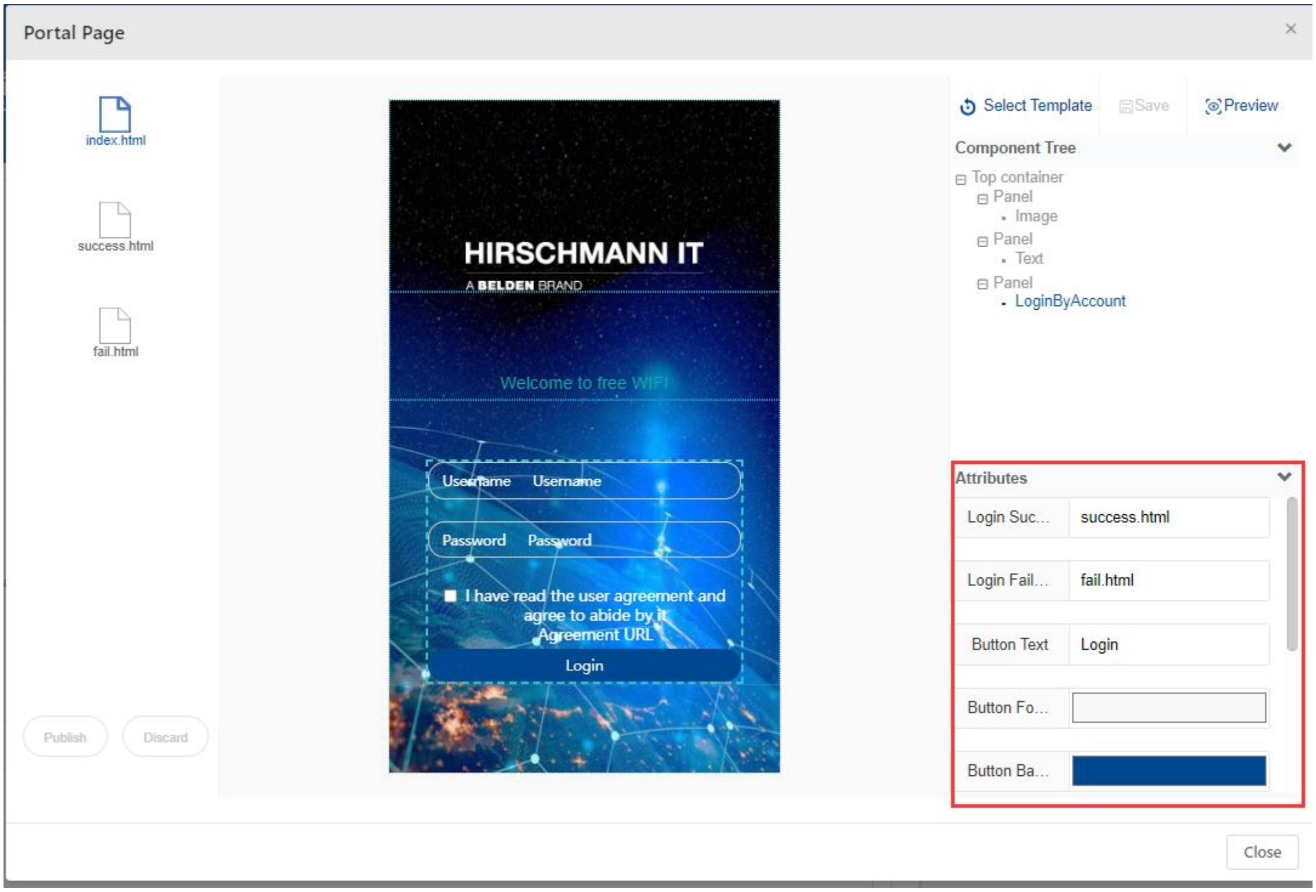
Font Family	Arial
Font Size	16px
Content	Welcome to free WIFI
Link Addr...	#
Color	🟩

Figure 238: Text component attributes

12.6.3 Form component

Below are listed several attributes of form components:

- **Login Success Redirect URL:** Redirect to this URL when login is 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:** Redirect to this URL when login is unsuccessful. This means that the failed page in the template will not be used. You need to verify that there is a prompt for **"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 an allowed IP.
- **Button Text:** Text content on the button.
- **Button Font Color:** Color of the text on the button.
- **Button Background Color:** Color of the Button.
- **"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.
- **Material Width:** Only appears in scan QR-Code by employee template. The width of a QR-Code can be the number of pixels or percent.



Attributes

Login Suc...	success.html
Login Fail...	fail.html
Button Text	Login
Button Fo...	
Button Ba...	

Figure 239: Form component attributes

13 Glossary

A	
AAA	Authentication, authorization, accounting
ACL	Access Control List
ACS	Automatic Channel Selection
APC	Automatic Power Control
ARP	Address Resolution Protocol
B	
BLE	Bluetooth Low Energy
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
C	
CLI	Command-Line Interface
D	
DAC	Dragonfly Access Controller
DAP	Dragonfly Access Point
DCM	Dynamic Client Management
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DRM	Dynamic Radio Management: automatically manages the DAP working channel and transmitting power.
DSCP	Differentiated Services Code Point
E	
EAP	Extensible Authentication Protocol
ESSID	Extended Service Set Identifier
F	
FQDN	Fully Qualified Domain Name
G	
GUI	Graphical User Interface
I	
IDS	Intrusion Detection System
IG	Installation Guide
IGMP	Internet Group Management Protocol
L	
LDAP	Lightweight Directory Access Protocol
M	
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
N	

NAT	Network Address Translation
NTP	Network Time Protocol
O	
OKC	Opportunistic Key Caching
OUI	Organizationally unique identifier
P	
PHY	Port Physical Layer
PMD	Post Mortem Dump
PMF	Protected Management Frames
PNAC	Port-based Network Access Control
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.
Q	
QoS	Quality of Service
QSG	Quick Start Guide
R	
RADIUS	Remote Access Dial-In User Service
RF	Radio Frequency
RSSI	Received Signal Strength Indicator
S	
SLB	Smart Load Balance
SNMP	Simple Network Management Protocol
SNR	Signal-to-noise ratio
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 issue, the SVM will automatically upgrade to act as the PVM.
T	
TCM	Three-Color Marking
TCP	Transmission Control Protocol
TLS	Transport Layer Security
U	
UDP	User Datagram Protocol
UNP	User Network Profile
V	
VLAN	Virtual Local Area Network
W	
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

A Further support

Technical questions

For technical questions, please contact any Hirschmann IT dealer in your area or Hirschmann IT directly.

A list of local telephone numbers and email addresses for technical support directly from Hirschmann IT is available at

https://hirschmann-it-support.belden.com

This Site also includes a free of charge knowledge base and a software download section.

HIRSCHMANN IT

A BELDEN BRAND